ESCUELA SUPERIOR POLITÉCNICA AGROPECUARIA DE MANABÍ MANUEL FÉLIX LÓPEZ

DIRECCIÓN DE POSGRADO Y FORMACIÓN CONTINUA

INFORME DE TRABAJO DE TITULACIÓN

PREVIA LA OBTENCIÓN DEL TÍTULO DE MAGISTER EN TECNOLOGÍAS DE LA INFORMACIÓN MENCIÓN EN REDES Y SISTEMAS DISTRIBUIDOS

MODALIDAD: PROYECTO DE INVESTIGACIÓN Y DESARROLLO

TEMA:

COMPARATIVA ENTRE HERRAMIENTAS DE MONITOREO DE RED DE COMPUTADORAS APLICADAS A LA EMPRESA PUERTO ATÚN

AUTOR:
MILTON LUYELY INTRIAGO CEDEÑO

TUTOR:
Mgtr. RAMÓN JOFFRE MOREIRA PICO

CALCETA, SEPTIEMBRE 2019

DERECHOS DE AUTORÍA

MILTON LUYELY INTRIAGO CEDEÑO, declaro bajo juramento que el trabajo aquí descrito es de mi autoría, que no ha sido previamente presentado para ningún grado o calificación profesional, y que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo los derechos de propiedad intelectual a la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López, según lo establecido por la Ley de Propiedad Intelectual y su Reglamento.

_____

MILTON LUYELY INTRIAGO CEDEÑO

CERTIFICACIÓN DE TUTOR

Mgtr. RAMON JOFFRE MOREIRA PICO, certifica haber tutelado el Trabajo de Titulación **COMPARATIVA ENTRE HERRAMIENTAS DE MONITOREO DE RED DE COMPUTADORAS APLICADAS A LA EMPRESA PUERTO ATÚN**, que ha sido desarrollado por **MILTON LUYELY INTRIAGO CEDEÑO**, previa la obtención del título de Magister en Tecnologías de la Información, mención Redes y Sistemas Distribuidos de acuerdo con el **REGLAMENTO DE LA UNIDAD DE TITULACIÓN DE LOS PROGRAMAS DE POSGRADO** de la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López**.**

_____

Mgtr. RAMÓN JOFFRE MOREIRA PICO

APROBACIÓN DEL TRIBUNAL

Los suscritos integrantes del tribunal correspondiente, declaramos que hemos **APROBADO** el trabajo de titulación **COMPARATIVA ENTRE HERRAMIENTAS DE MONITOREO DE RED DE COMPUTADORAS APLICADAS A LA EMPRESA PUERTO ATÚN**, que ha sido desarrollado por **MILTON LUYELY INTRIAGO CEDEÑO**, previa la obtención del título de Magister en Tecnologías de la Información, mención Redes y Sistemas Distribuidos de acuerdo con el **REGLAMENTO DE LA UNIDAD DE TITULACIÓN DE LOS PROGRAMAS DE POSGRADO** de la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López.

_____ _____

DR. INF. JORGE PÁRRAGA ÁLAVA
MIEMBRO

DR. INF. JORGE HERRERA TAPIA
MIEMBRO

_____

MGTR. JÉSSICA MORALES CARILLO
PRESIDENTE

AGRADECIMIENTO

Mis agradecimientos, van dirigidos en primer lugar, a Dios, por ser el principal guía y así poder finalizar esta importante etapa de nuestras vidas.

A esta prestigiosa ESPAM MFL, que me acogió y me permitió ser parte de ella para forjar un futuro dentro de sus instalaciones.

A mi tutor el Mgtr. Joffre Moreira Pico, quien con sus conocimientos y orientaciones me ayudó en el desarrollo del proyecto de titulación y culminarlo satisfactoriamente.

De manera muy especial agradezco a la empresa Puerto Atún quien fue de gran ayuda para poner en práctica la ejecución del proyecto y así poder culminarlo.

A mis profesores y amigos quienes me acompañaron en esta gran etapa y que de una u otra forma me brindaron su apoyo.

MILTON LUYELY INTRIAGO CEDEÑO

DEDICATORIA

Quiero dedicar de manera muy especial este trabajo principalmente a Dios, quien deposito en mí la fuerza de voluntad para culminar mi carrera.

A mis padres quienes siempre estuvieron a mi lado brindándome su apoyo incondicional, siendo mi principal fuente motivacional para mi superación.

A mis hermanos y amigos que de una u otra manera siempre estuvieron presentes y apoyándome en la etapa de preparación.

MILTON LUYELY INTRIAGO CEDEÑO

CONTENIDO GENERAL

CONTENIDO DE CUADROS, FIGURAS, IMÁGENES Y GRÁFICOS

RESUMEN

Las infraestructuras tecnológicas representan para las empresas actuales un activo de vital importancia para manipular información, comunicarse con los proveedores, brindar servicios a sus clientes y otras actividades. En este sentido la empresa Puerto Atún tiene una importante cantidad y variedad de dispositivos tecnológicos en los cuales sustenta varias de sus actividades cotidianas, así mismo esta entidad no cuenta con una herramienta de monitoreo de redes y aplicaciones, por tal motivo el objetivo de este trabajo es comparar varias soluciones de monitoreo para obtener la que mejores prestaciones brinde a la empresa en términos de adaptabilidad y funcionalidades. Para el desarrollo de este proyecto se evaluaron siete herramientas ya establecidas en el mercado de las cuales se escogieron cuatro para pruebas de implementación, luego se instalaron por periodos de cinco días cada una de las aplicaciones escogidas para determinar su nivel de cumplimiento con base en parámetros obtenidos de varios estudios similares. La herramienta Nagios fue la que presentó mejores prestaciones según los criterios evaluados, adicionalmente los sistemas de monitoreo pudieron detectar apagones de varios equipos y niveles elevados de consumo de los recursos de hardware en otros. Como resultado de la comparativa de herramientas para el monitoreo de la red y los servicios de la entidad, se estableció un plan de mejoras con estrategias para la optimización de la red de datos.

Palabras clave: Redes, monitoreo, Nagios, Zabbix, PRTG, Pandora FMS

ABSTRACT

Technological infrastructures represent a vital asset for current companies to manipulate information, communicate with suppliers, provide services to their customers and other activities. In this sense, the Puerto Tuna company has an important amount and variety of technological devices in which it supports several of its daily activities, likewise this entity does not have a network and application monitoring tool, for this reason the objective of this work is to compare several monitoring solutions to obtain the best performance provided to the company in terms of adaptability and functionalities. For the development of this project, seven tools already established in the market were evaluated, of which four were chosen for implementation tests, then each of the applications chosen were installed for periods of five days to determine their level of compliance based on parameters obtained from several similar studies. The Nagios tool was the one that presented the best performance according to the evaluated criteria, additionally the monitoring systems were able to detect blackouts of several equipment and high levels of consumption of hardware resources in others. As a result of the comparison of tools for monitoring the network and services of the entity, an improvement plan was established with strategies for optimizing the data network.

Keywords: Networks, monitoring, Nagios, Zabbix, PRTG, Pandora FMS.

CAPÍTULO I. ANTECEDENTES

1.1 PLANTEAMIENTO Y FORMULACIÓN DEL PROBLEMA

Como resultado del vertiginoso progreso tecnológico, áreas como la radio, la televisión y la computación están convergiendo con rapidez en el siglo XXI, y las diferencias entre recolectar, transportar, almacenar y procesar información están desapareciendo rápidamente. Las organizaciones con cientos de oficinas esparcidas sobre una amplia área geográfica dan por sentado como algo rutinario a la capacidad de examinar el estado actual, aun de su oficina más remota, con sólo presionar un botón (Wetherall, 2012).

A medida que aumenta nuestra habilidad para recopilar, procesar y distribuir la información, la demanda de procesamiento de los datos aumenta rápidamente. La industria de la informática es considerada joven, pero si se compara con otras (como la automotriz y la de transporte aéreo), esta ha progresado de manera impresionante en un periodo muy breve (Wetherall, 2012).

Las redes de computadoras están basadas en los estándares IEEE 802.3 y 802.11 los cuales determinan su naturaleza, es decir pueden ser cableadas o inalámbricas. Los elementos que conforman estas redes son *routers*, *switches* puntos de acceso, servidores, entre otros, todo este conjunto de elementos funcionando de manera idónea garantizan servicios eficientes (Bayas, 2015).

Según el análisis de Fava (2016), estaban constituidas por mainframes como únicos actores en la década de los 70, además se caracterizaban por bajas velocidades y transmisiones asíncronas. Ya en los 80 proliferaron las redes de área local (LAN) con la llegada de los microprocesadores y el aumento de la velocidad.

Actualmente las redes constituyen un elemento determinante en el éxito de una empresa, al producirse una falla en esta los empleados y usuarios quedan incomunicados, de forma que es imposible acceder a información vital para la empresa. Siendo así, que el monitoreo resulta fundamental para la prevención

y resolución de incidentes con la red de computadoras de una organización, así como también en el éxito de muchos de sus procesos (Gallego, 2015).

Puesto que Sánchez (2017), hace mención a que el tráfico IP se multiplico por 13 entre 2011 al 2016 en España, teniendo como resultado 258 millones de dispositivos conectados con un aproximado de 5.1 conexiones por habitante, de la cual el aumento de usuarios y dispositivos conectados en internet, el tráfico de información a nivel global se incrementa exponencialmente y por ende el congestionamiento de la red.

Donde Romero y Padua (2018), manifiestan la importancia de detectar de manera oportuna las fallas mediante el monitoreo red, de manera que se identifiquen las fallas posibilita el catalogar un comportamiento o estado mediante el análisis y recolección de tráfico.

Un caso muy particular es la Universidad Politécnica Salesiana sede Guayaquil donde Pilozo y Zambrano (2013) efectuaron la implementación de un sistema de monitoreo, que después de la instalación de cada software de monitoreo, mostraron cambios positivos en la administración y tiempo de respuestas a problemas por parte del personal de Sistemas, tendiendo con resultado la información de datos estadísticos del estado de los servidores, alertas vía correo, identificar problemas en los servidores y el consumo del ancho de banda.

Sin embargo, en la empresa industrial “Puerto atún” de la ciudad de Jaramijó, no cuenta con un sistema de monitoreo de redes que le permita identificar el estado de sus servicios y dispositivos en el caso que se amerite alguna alerta en caso de incidentes en la comunicación de la red, dado que monitorear los servicios y equipos de una red de computadoras es una actividad importante para el control de las redes y asegurar la continuidad de las actividades empresariales.

Considerando los aspectos mencionados en párrafos anteriores el autor de esta investigación se planteó la interrogante: **¿De qué manera determinar el**

análisis de amenazas y compontes defectuosos en las redes de computadoras de la empresa Puerto Atún?

1.2 JUSTIFICACIÓN

La monitorización de las redes de computadoras recoge los datos relacionados con los eventos suscitados en la infraestructura de red permitiendo alertar a los administradores del sistema y sirviendo de sustento en la ejecución de las medidas correctivas y/o preventivas. Con estos antecedentes el autor de este trabajo se enfoca en la necesidad de realizar la comparativa de herramientas de monitoreo con el fin de determinar cuál cumple con el mayor porcentaje del análisis y notificación de eventos de la red de la empresa Puerto Atún.

La disponibilidad de los recursos tecnológicos en las diferentes entidades se ha convertido en una prioridad para la atención a los clientes, la comunicación con los proveedores, medios publicitarios, agilidad en las actividades contables, entre otras funciones. En este sentido se categoriza a la infraestructura tecnológica como el nexo sociedad-institución que le permite estar presente en múltiples plataformas para ofertar sus productos (Bayas 2015).

Es importante tener en consideración el aspecto legal al momento de elegir la herramienta de monitoreo de red, ya que, dichas soluciones se encuentran distribuidas en términos de acuerdos de licencia, y aunque varias de estas se encasillan como software libre u open source es importante tener claro que opciones nos brindan cada una de las herramientas (Bayas 2015).

En el aspecto ambiental el monitoreo de los elementos de la red tiene su impacto, ya que, como hace mención Pérez (2013) el auge de las redes de telecomunicaciones ha generado la coexistencia de múltiples marcas que desarrollan sus productos de manera variada considerando los componentes y capacidades, el control de estos equipos aporta a escoger soluciones más robustas y amigables con el medio ambiente.

El control de la infraestructura tecnológica en una organización representa una inversión de recursos que a mediano y largo plazo se justifica a través de la

respuesta inmediata a problemas identificados en los dispositivos y servicios, así como también con la implementación de medidas preventivas que respalden el buen funcionamiento de la red Velasco y Cagua (2017).

1.3 OBJETIVOS

1.3.1 OBJETIVO GENERAL

Comparar herramientas de monitoreo de red, para el análisis de amenazas y componentes defectuosos en la red de la empresa Puerto Atún.

1.3.2 OBJETIVOS ESPECÍFICOS

- Determinar el conjunto de herramientas para el monitoreo de las redes de computadoras.
- Diseñar la estrategia de monitoreo de la red de computadoras.
- Implementar las herramientas de monitoreo en la infraestructura de red.
- Categorizar las herramientas de monitoreo a partir de los resultados obtenidos por estas.
- Generar un plan de mejoras para la optimización de la red de datos basados en los resultados obtenidos de las herramientas de monitoreo.

1.4 IDEA A DEFENDER

La comparativa de herramientas de monitoreo de red en la empresa Puerto Atún, permitirá la selección de la mejor herramienta para identificar las amenazas y componentes defectuosos que pueden ocasionar fallas en los servicios, sistemas y dispositivos en la red.

CAPÍTULO II. REVISIÓN BIBLIOGRÁFICA

2.1 MONITOREO DE REDES DE COMPUTADORAS EN LAS EMPRESAS

La obra de White (2015) hace mención a que el mundo de los negocios modernos no podría funcionar sin la comunicación y las redes de computadoras, por motivo que la mayoría de las personas hacen uso indirecto o interactúan con dichas redes. En el pasado este campo de estudio no pasaba de ser competencia de los ingenieros y personal técnico, pero en la actualidad se encuentran involucrados los gerentes administrativos, usuarios finales y, cualquier persona que utilice un teléfono inteligente o una computadora.

Así mismo Wu y Irwin (2016), consideran el enfoque de las redes de computadoras como un conjunto variado de subredes (redes empresariales, de hogar y personales) que convergen en lo que conocemos como internet para lograr transparentar la comunicación entre todos los sectores involucrados.

Existen muchas razones prácticas por las cuales es importante el estudio de la estructura de la red de internet, Newman (2018) define como la función principal de internet a la transmisión de datos entre computadoras y demás dispositivos en diferentes partes del mundo.

Es necesario ejercer control sobre la infraestructura tecnológica para asegurar el funcionamiento adecuado de los sistemas y prevenir fallos en los equipos de comunicaciones, estas medidas fomentan la optimización de la red a través de información detallada del estado de sus recursos. El monitoreo puede realizarse a través de soluciones basadas en hardware o en software buscando siempre óptimos niveles de supervisión y notificación Gavilares (2016).

La dependencia de contar con una infraestructura computacional en las empresas modernas conlleva un intrínseco control sobre dicha infraestructura, en el trabajo de Tobar (2015), se define como sistema de monitorización y gestión de redes al conjunto de sistemas, normativas y protocolos de gestión que facilitan las actividades de monitoreo y mantenimiento de la red.

La disponibilidad en internet de los servicios empresariales se ha convertido en un aspecto de vital importancia para el desarrollo de estas y su interacción con los usuarios. Para mantener siempre activos estos servicios Gavilares (2016) considera necesario un monitoreo constante de la infraestructura computacional, además enfatiza la automatización de este procedimiento para notificar a los administradores sobre las advertencias y problemas encontrados.

El crecimiento continuo y rápido de las redes basadas en el protocolo IP junto a la dependencia que se genera en torno a estas redes hace que su administración y mantenerlas todo el tiempo operativas resulte una tarea complicada, una de las propuestas que plantea Qadir y Adnan (2010), es la supervisión continua para minimizar el tiempo de inactividad, proceso que se puede realizar con el uso de soluciones comerciales de alto costo al igual que mediante aplicaciones de código abierto como Nagios y OpenNMS.

La gestión integrada de dispositivos de múltiples proveedores es un activo clave para todo negocio referente a las telecomunicaciones ya sea de manera directa o indirecta, en este sentido Nagios es una plataforma abierta, adaptable y de bajo costo (o nulo según la versión) que admite la administración de fallas para redes de próxima generación Kora y Soidridine (2012).

2.1.1 HERRAMIENTAS DE MONITOREO PARA REDES DE DATOS

Según Pérez (2013), la selección de las herramientas de monitoreo se debe realizar de acuerdo a las necesidades y la topología existente. Además, considera que la utilización de un agente de monitoreo favorece la supervisión de las computadoras, el determinar el estado de los componentes de los sistemas supervisados y la presentación de informes al servidor de monitoreo.

En el trabajo de Issariyapat *et al.* (2012), hacen referencia a **Nagios** como una de las herramientas que han sido ampliamente utilizadas por administradores de red, debido a su arquitectura modular flexible que permite a los usuarios desarrollar módulos personalizados que se adapten a las características de cada escenario.

Entre los autores que apoyan la implementación de **Pandora FMS** se mencionan a Alava y Guerrero (2018), quienes catalogan esta aplicación como una herramienta que detecta los problemas físicos en los equipos de la infraestructura, así mismo Silva (2013), indica que Pandora FMS implementa protocolos de gestión y consulta sobre los equipos con el objetivo de ser flexible para monitorear infraestructuras variadas sin invertir demasiado tiempo, recurso humano y dinero, además esta solución permite escoger entre su versión comercial y de software libre, para las cuales se consideran las funcionalidades y el soporte que brinda la empresa.

Como menciona en su obra Dalle (2015), **Zabbix** se ha mostrado como una potente y efectiva solución de código abierto para el monitoreo de redes, la cual puede ser descargada desde el sitio oficial para diversas plataformas. Un concepto interesante es el que mencionan Dalle y Kewan (2015), los cuales sostienen que no consideran a Zabbix como la herramienta capaz de solucionar todos los problemas de administración y monitoreo de redes, pero afirman que es una herramienta poderosa que puede ser personalizada para ajustarse a necesidades específicas brindando capacidades de medición para gran variedad de componentes y un sistema de alertas efectivo.

La herramienta de monitoreo **PRTG Network Monitor** básicamente se encarga de identificar y prevenir los problemas que ocurren en la red, según Deokule, y otros (2016), una de sus ventajas es el autodescubrimiento de la red, además de proveer seguridad y alertas efectivas. La versión libre de este software brinda soporte para cien sensores que son suficientes para los servicios más comunes en las redes tales como: HTTP, SMTP/POP3, FTP, SSH, entre otros.

Según Qadir y Adnan (2010), el objetivo de monitorear la red es obvio, es decir, ayudar a mantener la red en un nivel operativo óptimo. A nivel de funcionalidad el sistema de monitoreo de redes (Network Monitoring System - NMS) adquiere la información actualizada de cada uno de los dispositivos bajo su supervisión y dicha información es almacenada y analizada por el administrador de la red.

Los datos que recibe el NMS pueden variar entre estadísticas sobre el tráfico de red, consumo de los recursos de los dispositivos pertenecientes a la infraestructura computacional, estado de los enlaces, entre otros Gallego (2015), manifiesta los datos obtenidos se pueden presentar de diferentes formas según la configuración establecida, por ejemplo:

- **Datos estadísticos del uso de los recursos. –** Según Fava (2016), para este caso se pueden mencionar el consumo del CPU, la utilización del ancho de banda, la tasa de acceso a servicios y equipos determinados en un tiempo específicoEstos informes no son de tipo críticos y por ende de manera general se muestran en la estación de monitoreo.
- **Alertas. -** Este tipo de mensaje es enviado por el NMS cuando se requiere atención inmediata por parte de un servicio o dispositivo.

El sistema de notificaciones que brinde cada NMS va a depender de su funcionalidad y características, entre las opciones más comunes se pueden encontrar: mensajes con niveles de criticidad en la consola del sistema de monitoreo, notificaciones por correo electrónico, mensajes de telefonía móvil celular, entre otros.

2.1.2 SNMP (SIMPLE NETWORK MANAGMENT PROTOCOL)

El Protocolo Simple de Administración de Red o SNMP trabaja en la capa de aplicación del modelo OSI y es el que permite intercambiar información entre los dispositivos de la red, desde que fue definido el protocolo siempre se consideró inseguro, para compensar dicho problema desde las últimas versiones hasta la actualidad se han logrado implementar cierto grado de seguridad denominado SNMPsec, siendo su principal características la identificación unívoca de las entidades que participan (Gavilares, 2016).

Este protocolo permite a los administradores de redes supervisar el desempeño, buscar y resolver problemas y planear su expansión, para obtener información de los equipos administrados. Silva (2013), menciona que SNMP utiliza dos modalidades; la primera es realizando un sondeo cada determinado tiempo sobre los elementos administrados para conocer su estado y el segundo

método se basa en la captura de alertas provenientes de los equipos monitoreados las cuales se lanzan cuando suceden alguna de las siguientes acciones:

- Caída en la interfaz del equipo.
- Se estropea el ventilador de un router o switch.
- Se llena el *filesystem* de un servidor.
- Un UPS cambia de estado.

Para Fava (2016), SNMP es un protocolo que ha tenido amplia aceptación porque brinda una interface no propietaria para administrar dispositivos de múltiples vendedores independientes de sus características y tecnologías de redes. Por tal razón, provee un gerenciamiento a nivel macro, es decir, en ocasiones no brinda detalles requeridos para solventar problemas específicos.

2.2 SISTEMA DE MONITOREO EN UNA INFRAESTRUCTURA DE TI

Quispe (2018), Menciona que el uso apropiado para la gestión de redes, incrementa la satisfacción de los usuarios finales, garantizándoles mayores niveles de disponibilidad independientemente de la complejidad, escalabilidad o modificaciones en la red. Además, concluye que un sistema de monitoreo es una herramienta de apoyo para la gestión de los dispositivos críticos en la red.

El sistema de monitoreo permite a los administradores de red mejorar su desempeño y asegurar por mayor tiempo la disponibilidad de los servicios de TI, basado en la supervisión continua que permitirá identificar las causas de las fallas y brindar soluciones en menor tiempo, estas acciones optimizan el trabajo del personal de TI permitiéndoles realizar otras funciones (Quispe, 2018).

La idea de supervisión constante de los activos en las organizaciones supone una inversión de recursos que en ocasiones puede ser importante, la cual se justifica considerando los beneficios que prestan los sistemas de monitoreo, en este documento se exponen dichas bondades, de las cuales se citan varios ejemplos a continuación:

- La detección y solución de los problemas se lleva a cabo de manera más eficiente, enfocándose en fallas específicas.

- Los datos de los hábitos de consumo, ayudan a establecer políticas de calidad de servicios (QoS) que garanticen la cuota necesaria de recursos para los servicios prioritarios (Saavedra, 2018).
- Optimización de recursos en la solución de problemas en la red.
- El conocimiento del estado de los dispositivos y servicios de la red, permitirá a los administradores planificar mantenimientos preventivos y correctivos de la infraestructura de TI (Sánchez, 2017).

2.2.1. CONTROL DE SERVICIOS Y EQUIPOS

Los sistemas de monitoreo actualmente tienden a trabajar bajo el paradigma conocido como gestor-agente, el cual tiene como principio fundamental el intercambio de información entre el o los nodos gestores y los nodos en los que se instaló el agente (Pérez, 2013). Una función interesante de este paradigma es que los agentes sin necesidad de ser invocados pueden emitir notificaciones por eventos o comportamientos anómalos registrados en alguno de los componentes del dispositivo en el que se encuentra implementado.

Según Tobar (2015), la funcion de configuracion de dispositivos se encuentra relacionada con la verificacion y deteccion de cambios en la configuracion de los dispositivos que conforman la red. Así mismo, este aspecto se refiere a la recopilacion de informacion concerniente a cambios de versiones, actualizaciones y demas acciones tanto de hardware como de software que se realicen en la infraestructura. El mismo Tobar (2015), expresa la importancia de conocer el grado de utilizacion de los recursos de la red para poder priorizar a los sectores críticos de las instituciones y brindar respuesta de forma efectiva a las posibles caidas de servicios o daños de equipos.

Freire y Sánchez (2016), mencionan lo importante que es para las empresas garantizar a sus clientes calidad y disponibilidad de sus servicios, en este sentido hacen enfasis en la necesidad de contar con una herramienta de control que les permita conocer el estado de sus servicos y equipos de una forma centralizada y automaática para obtener los datos necesarios que solventen la infraestructura.

CAPÍTULO III. DESARROLLO METODOLÓGICO

El presente trabajo es una investigación de campo que se fundamentó en los métodos comparativo y experimental para su desarrollo, se realizó un comparativo referente a la funcionalidad y adaptabilidad de varios sistemas de monitoreo de redes para su posterior aplicación. En el ámbito experimental se puede mencionar que en la empresa Puerto Atún no se han realizado estudios de este tipo que fortalezcan el control de su infraestructura tecnológica. La metodología que se utilizó para el desarrollo de esta investigación es la consecución de objetivos (Anexo 2), lo que permitió obtener los resultados de manera organizada.

3.1. DETERMINACIÓN DEL CONJUNTO DE HERRAMIENTAS PARA EL MONITOREO DE LAS REDES DE COMPUTADORAS

En la elección de las soluciones de monitoreo a evaluar se realizó de manera previa la revisión bibliográfica de diversas fuentes que sustentaron la elección de una u otra herramienta (Opsview, 2019) (González, 2011) (Nagios, 2016). Con dicha base se escogieron 7 herramientas: Nagios, Zabbix, Pandora FMS, PRTG network monitor, Open NMS, Opsview y Zenoss, que fueron valoradas con parámetros generales, además se tuvo como sustento evaluaciones encontradas en sitios específicos y otros artículos relacionados.

Sin embargo, estas herramientas de monitoreo de redes de computadoras se basan a varios estudios que sustentan su aplicabilidad, en los niveles de popularidad de estas soluciones y sus características generales y en su mayoría fueron consideradas herramientas de software libre.

Dichas soluciones fueron escogidas mediante una evaluación de cumplimiento de parámetros y trabajos de comparativas de sistemas de monitoreo, quedando seleccionadas para el estudio las herramientas Zabbix, Nagios, PGTR Network Monitor y Pandora FMS.

3.2 DISEÑO DE LA ESTRATEGIA DE MONITOREO DE LA RED DE COMPUTADORAS

Para el cumplimiento de este apartado se identificaron los equipos que componen la infraestructura de red de la empresa Puerto Atún, con el propósito de plasmar la mejor estrategia de red mediante una topología óptima, permitiendo así indicar la cantidad de routers, switches, puntos de acceso inalámbricos y demás dispositivos tecnológicos que conforman la misma.

Luego de conocer el entorno, fue necesario definir qué equipos y servicios se iban a monitorizar en la red. Entre los servicios definidos tenemos: el servidor web, el servidor de correo, entre otros, mientras que entre los dispositivos se encontraban los switches, el *router* principal, antenas, cámaras de seguridad y cualquier otro equipo que facilitó la comunicación en prestación de servicios en la empresa.

3.3 IMPLEMENTACIÓN DE LAS HERRAMIENTAS DE MONITOREO EN LA INFRAESTRUCTURA DE RED

La implementación de las herramientas se realizó de manera nativa en un computador de escritorio con las características de hardware necesarias requeridas para instalar cada uno de los sistemas de monitoreo. Antes de realizar las instalaciones de las aplicaciones de monitoreo se formateó la computadora para que no contara con registros o información de los demás sistemas.

Puesto que propuesta toma en consideración que la mayoría de los sistemas de monitoreo tienen un agente el cual responde a las solicitudes de acción que envía el servidor de monitoreo, analizando esta actividad se entiende que en su medida genera tráfico extra en la red y al implementar cuatro sistemas al mismo tiempo generaría sobrecarga a la red y resultaría perjudicial en la obtención de los resultados.

Cada una de las soluciones de monitoreo fueron implementadas por un periodo de cinco días, registrando todos los eventos que se suscitaron en ese lapso, a las soluciones que no tenían activo el auto reconocimiento de dispositivos se procedió a activar dicha función para agilizar el trabajo.

3.4 CATEGORIZACIÓN DE LAS HERRAMIENTAS DE MONITOREO A PARTIR DE LOS RESULTADOS OBTENIDOS POR ESTAS

Para realizar la categorización de las herramientas de monitoreo de redes y aplicaciones fue necesario establecer una serie de parámetros que permitiesen valorar cada una de las soluciones implementadas, todos los puntos definidos para la evaluación fueron divididos en cinco categorías generales: requerimientos del sistema, seguridad, soporte, facilidad de uso y administración.

De acuerdo con estas categorías se efectuó el análisis comparativo entre las herramientas de monitoreo basados al trabajo de González (2011), en el que la autora compara cinco soluciones de monitoreo asignando tres posibles valores según el nivel de cumplimiento de cada característica. Asigna el valor de 1 al parámetro que se cumpla totalmente, el valor de 0.5 es asignado a las características que se cumplan a medias y el valor de 0 para los parámetros que no se cumplen. Adicionalmente se agregaron medidas cualitativas que consideró importante el autor de este trabajo en este proceso de desarrollo (Anexo 4).

3.5 ELABORACIÓN DE UN PLAN DE MEJORAS PARA LA OPTIMIZACIÓN DE LA RED DE DATOS BASADOS EN LOS RESULTADOS OBTENIDOS DE LAS HERRAMIENTAS DE MONITOREO

En este punto se procedió al análisis de los resultados basándose en los eventos registrados por cada una de las soluciones, estos detalles fueron

considerados para el desarrollo del plan de mejoras del rendimiento de la infraestructura.

Posteriormente a la elaboración y aprobación del plan, se hace la entrega al departamento de sistemas de la empresa Puerto Atún, el mismo que contiene puntos específicos sobre las acciones a realizar para garantizar el funcionamiento adecuado de la red.

CAPÍTULO IV. RESULTADOS Y DISCUSIÓN

En este capítulo se menciona el esquema de trabajo para realizar el monitoreo de la infraestructura de red de la empresa Puerto Atún (Anexo 1), así como también se encuentran el diseño topológico de la red, la comparativa entre varios sistemas de monitoreo.

Los resultados obtenidos por cada herramienta de monitoreo, la representación estadística y gráfica del nivel de cumplimiento de las soluciones implementas y varias ideas para el desarrollo del plan de mejoras en cuanto a la gestión y rendimiento de la infraestructura tecnológica de la institución.

Se obtuvieron los siguientes resultados de acuerdo con los objetivos planteados y desarrollados en la ejecución de la investigación:

4.1 DETERMINACIÓN DEL CONJUNTO DE HERRAMIENTAS PARA EL MONITOREO DE LAS REDES DE COMPUTADORAS

En el Cuadro 1 se realizó la selección de las herramientas mediante una comparativa entre varias soluciones de monitoreo de redes de computadoras considerando las soluciones de software libre en su mayoría, ya que en ocasiones las empresas no dan la importancia que merece el monitoreo de su infraestructura tecnológica, aun así se consideró para esta comparativa la versión shareware del sistema PRTG teniendo en cuenta que es uno de los más populares en el mercado y que el tiempo que está activa la prueba brinda casi todas sus funcionalidades. Esta selección se realizó marcando una **X** a las características que tiene cada herramienta y de esta manera escoger una de ellas, que cumpla con las necesidades que requiere el monitoreo de la red de datos.

Cuadro 1. Comparativa de las características que presentan las herramientas de monitoreo de red de datos.

HERRAMIENTAS / CARACTERÍSTICAS	NAGIOS	ZABBIX	PANDORA FMS	PRTG NETWORK MONITOR	OPENNMS	OPSVIEW	ZENOSS
Monitoreo de red	X	X	X	X	X	X	X
Monitoreo en la nube	X	X	X	X		X	
Monitoreo de aplicaciones	X	X	X	X		X	X
Monitoreo de servidores	X	X	X	X	X	X	X
Monitoreo web o remoto	X	X	X	X			
Dispositivos de almacenamiento	X	X	X				
Monitoreo de máquinas virtuales	X	X	X	X	X	X	X
Aplicaciones java		X			X		
Monitoreo de bases de datos	X	X	X	X	X	X	X
KPI/SLA		X	X				
Telefonía	X	X	X	X	X	X	X
Monitoreo de seguridad	X	X		X	X	X	
Temperatura de un servidor	X	X	X	X	X	X	X
Temperatura de un sistema	X	X	X	X	X	X	X
Monitoreo de sistema operativo	X	X	X	X	X	X	X
Herramienta tolerante a fallos (servidor de respaldo)				X			
Monitoreo de rendimiento de un computador	X					X	
Monitoreo de correo electrónico	X	X	X	X	X	X	X
Linux	X	X	X		X	X	X
Windows	X		X	X	X	X	

Elaboración: El Autor

4.2 DISEÑO DE LA ESTRATEGIA DE MONITOREO DE LA RED DE COMPUTADORAS

Una vez recolectado los datos sobre la arquitectura de red de la empresa y haber definido cada uno de los elementos que iban a ser monitorizados, se determinó que la empresa cuenta con una topología de red de estrella extendida y entre las tecnologías que tiene en su infraestructura se mencionan las siguientes categorías: central telefónica, teléfonos IP, computadores, routers, switches, cámaras PTZ, Grabadores DVR, Grabador NVR, lector biométrico, enlaces inalámbricos punto a punto y puntos de acceso inalámbricos. Varios detalles correspondientes a las marcas, modelos, diseños topológicos lógicos de la red, cantidad y diversidad de productos tecnológicos con que cuenta la entidad, entre otros aspectos no se muestran en este documento por cuestiones de confidencialidad y seguridad solicitadas por la empresa. A continuación, en la Figura 1 se puede observar el diseño de la topología física de la red de la Empresa Puerto Atún.

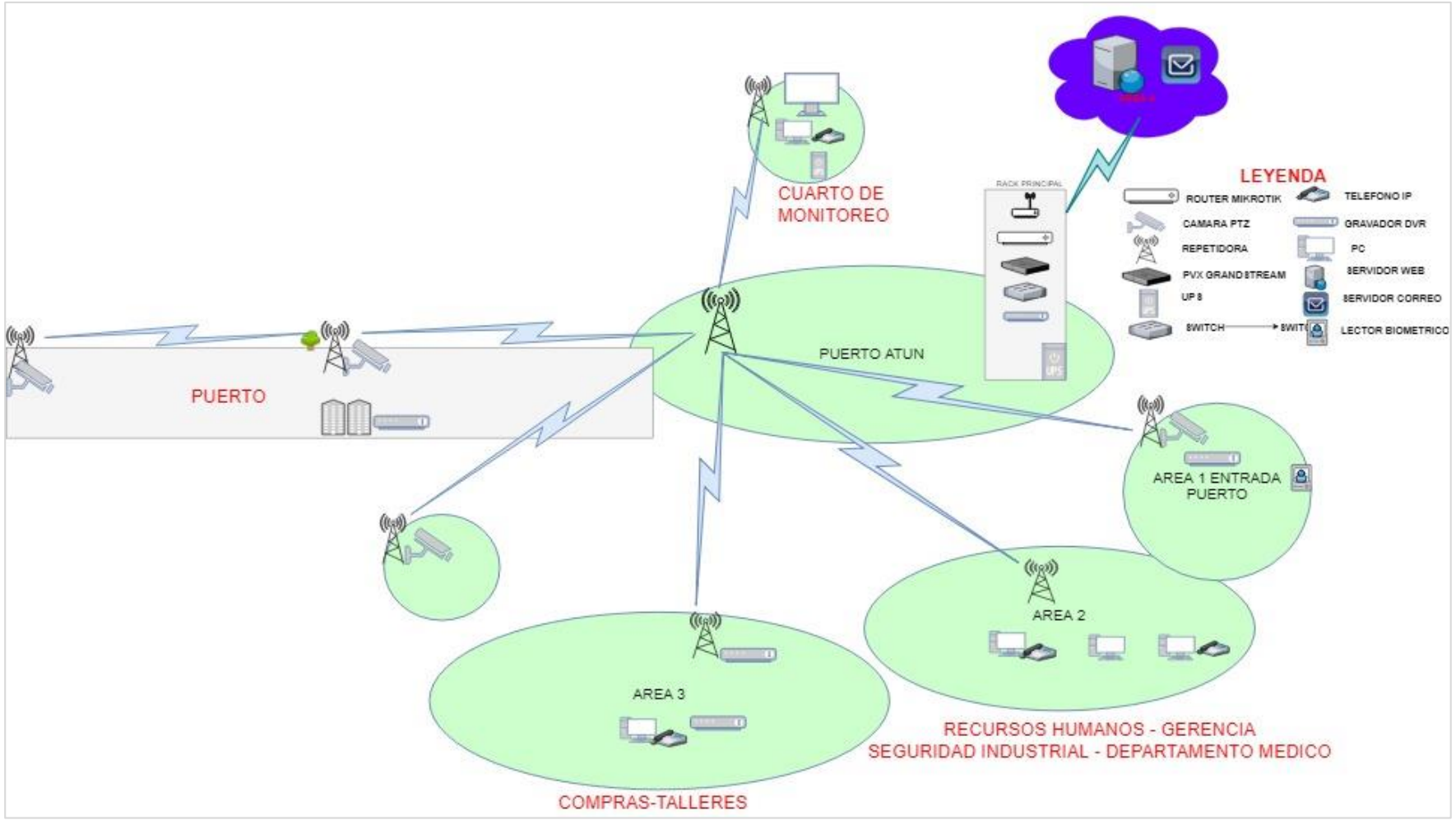


Figura 1. Topología física de la red de la empresa “Puerto Atún”
Elaboración: El Autor

4.3 IMPLEMENTACIÓN DE LAS HERRAMIENTAS DE MONITOREO EN LA INFRAESTRUCTURA DE RED

El procedimiento detallado de la instalación de los sistemas de monitoreo se puede encontrar en el Anexo 3, de este documento, a continuación, se muestran las capturas de pantalla obtenidas de las herramientas de monitoreo posterior a su instalación y configuración para realizar la monitorización de la infraestructura tecnológica de la empresa Puerto Atún.

4.3.1 ZABBIX

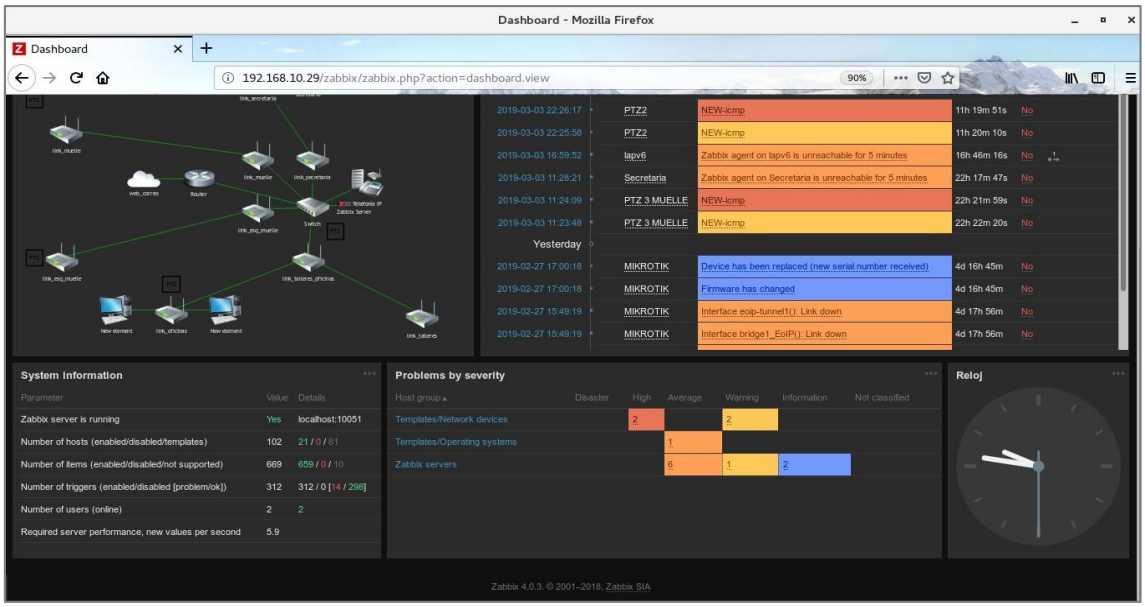


Imagen 1. Monitoreo de red con Zabbix
Elaboración: El Autor

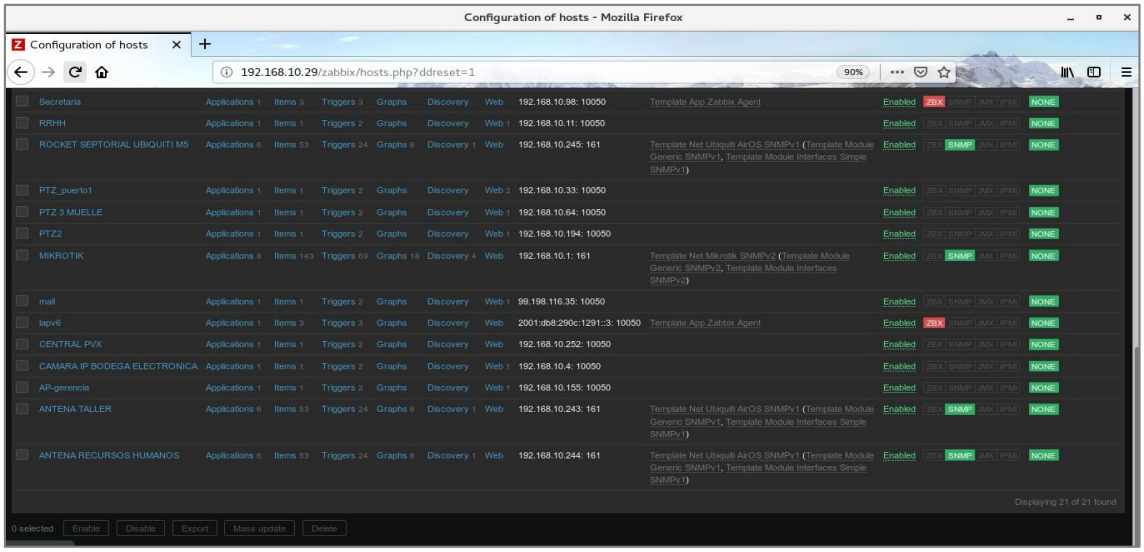


Imagen 2. Monitoreo de servidores con Zabbix.
Elaboración: El Autor

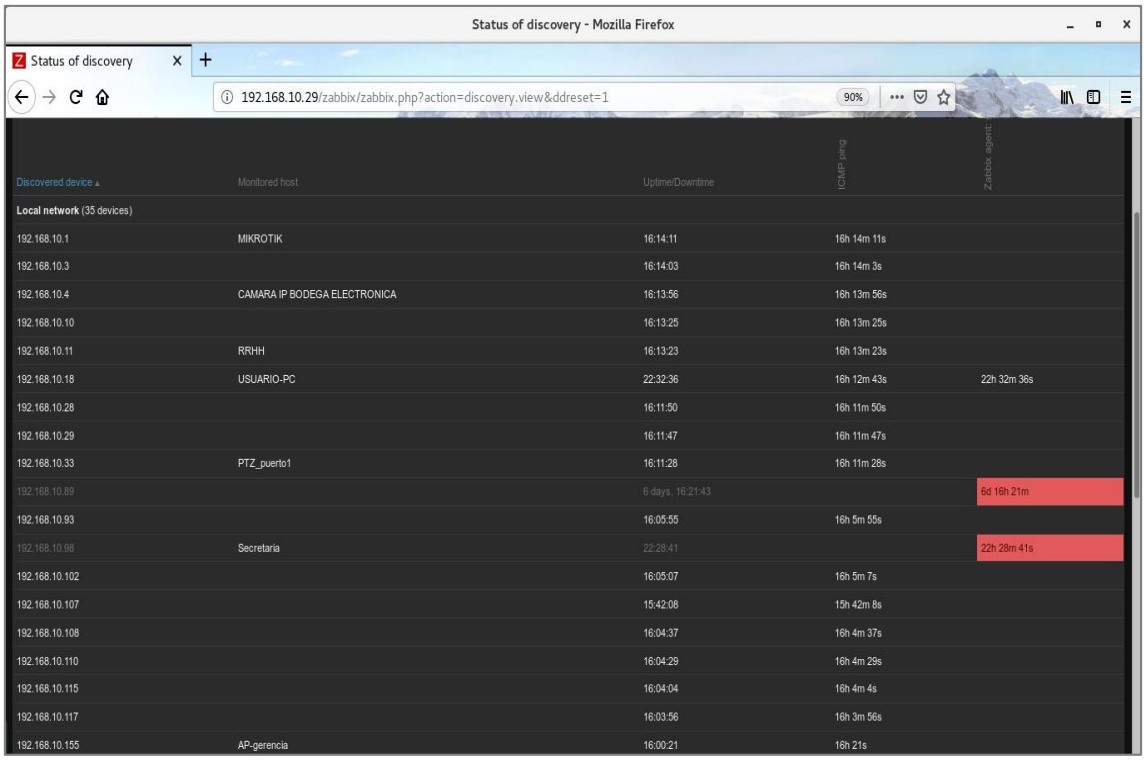


Imagen 3. Hosts encontrados por auto-descubrimiento con Zabbix
Elaboración: El Autor

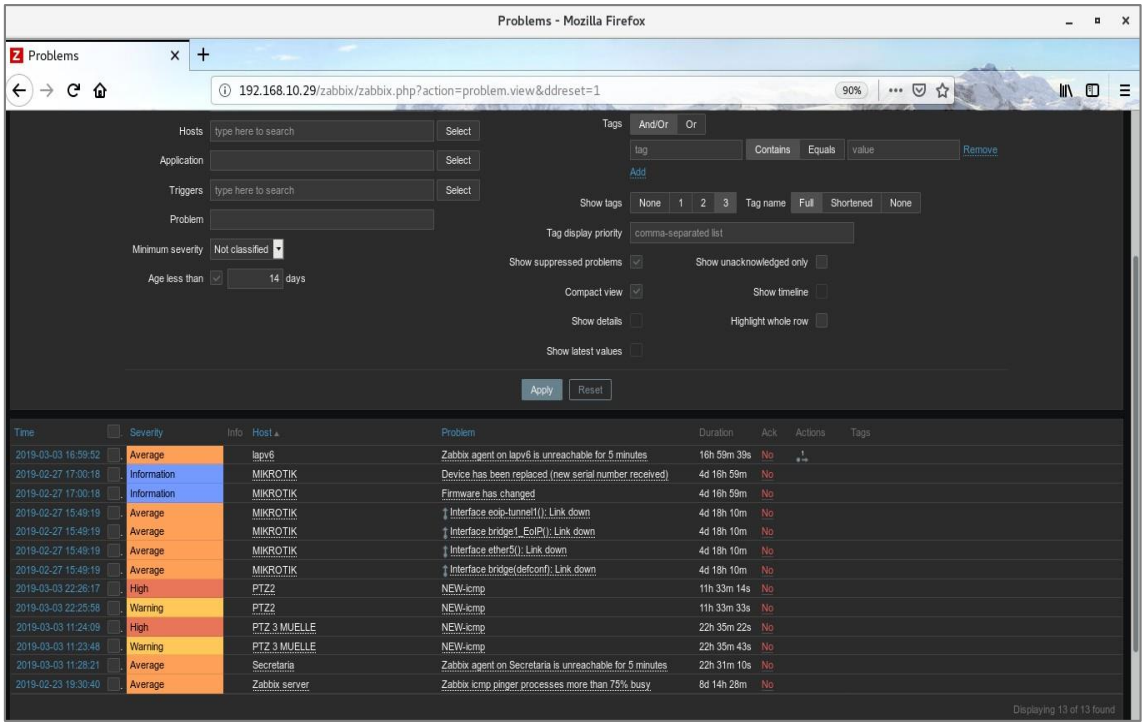


Imagen 4. Problemas y eventos reportados por Zabbix
Elaboración: El Autor

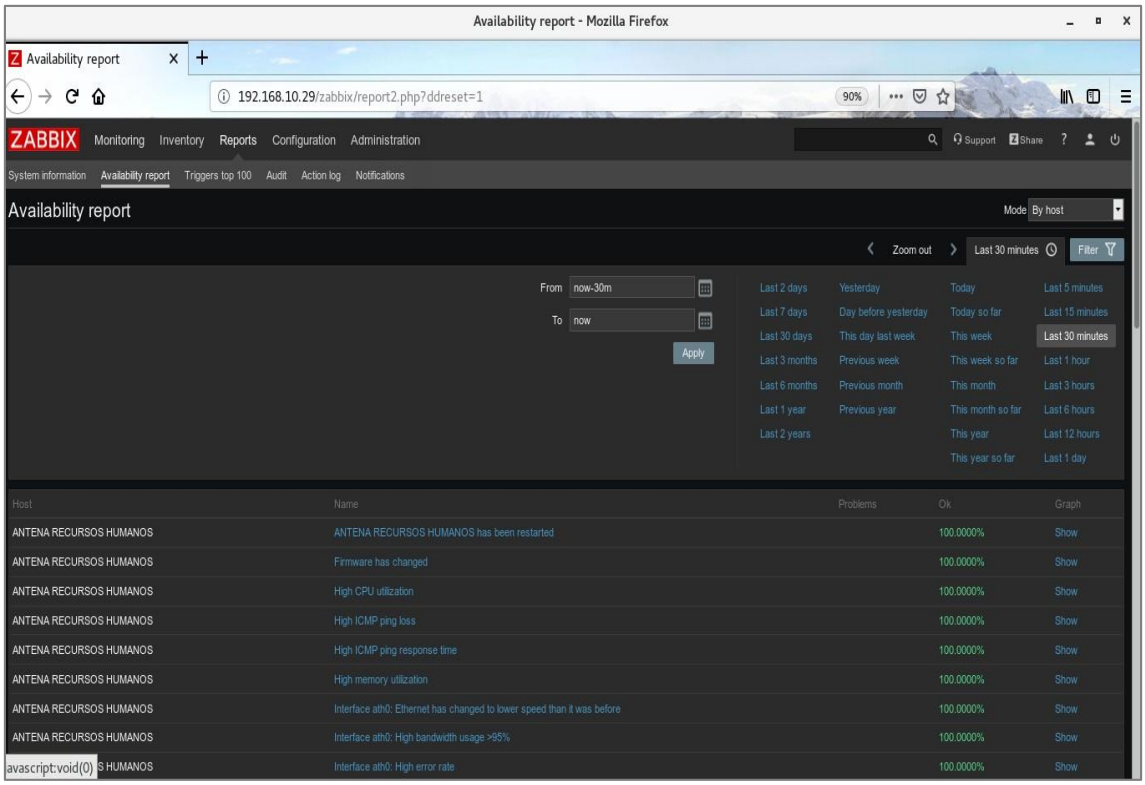


Imagen 5. Reportes generados por Zabbix
Elaboración: El Autor

4.3.2 NAGIOS

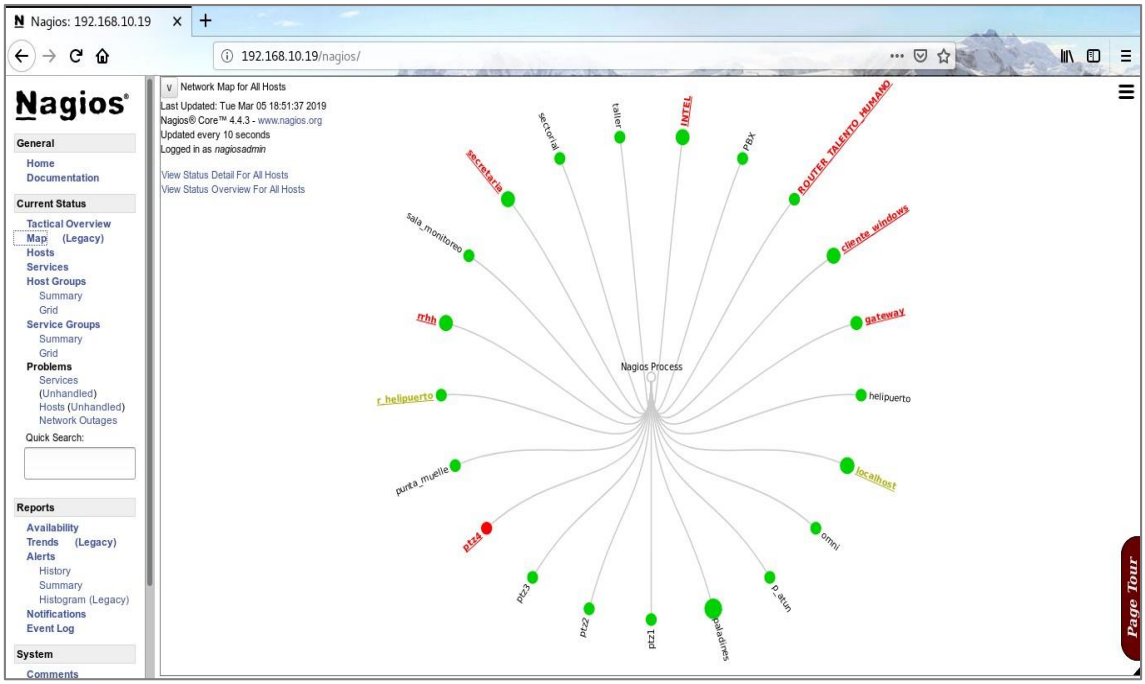


Imagen 6. Diagrama automático de los equipos agregados en Nagios
Elaboración: El Autor

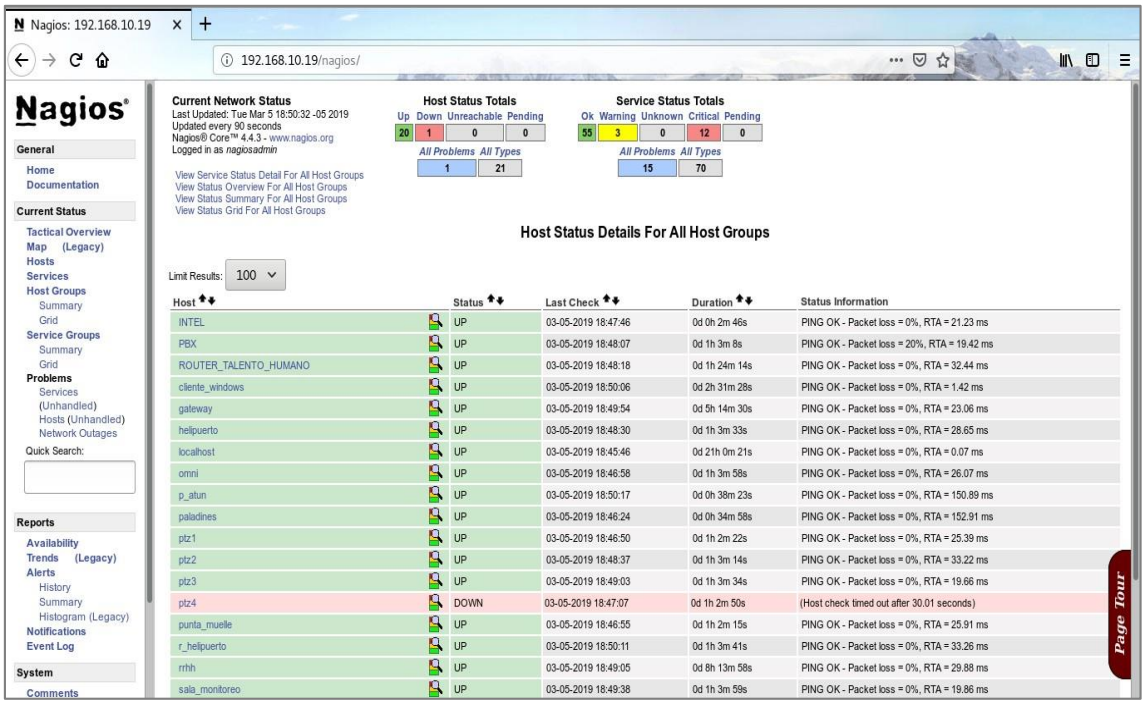


Imagen 7. Reportes del estado de los grupos de Host generados por Nagios
Elaboración: El Autor

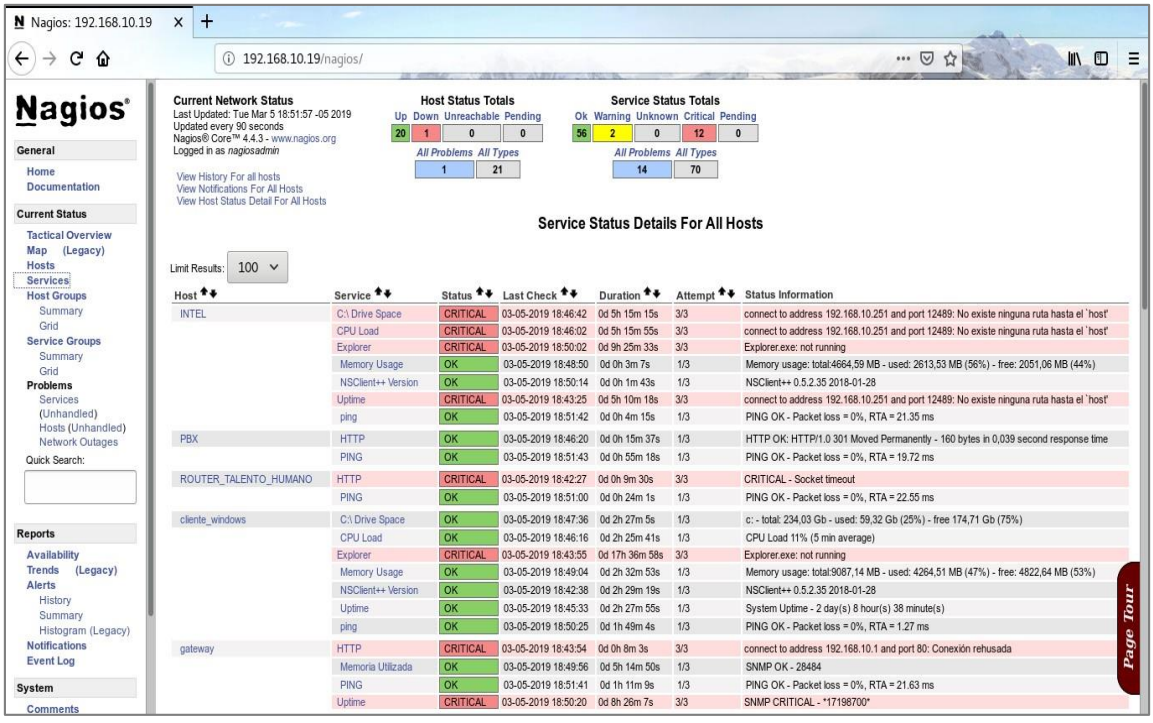


Imagen 8. Reportes del estado de los servicios de todos los Host con Nagios
Elaboración: El Autor

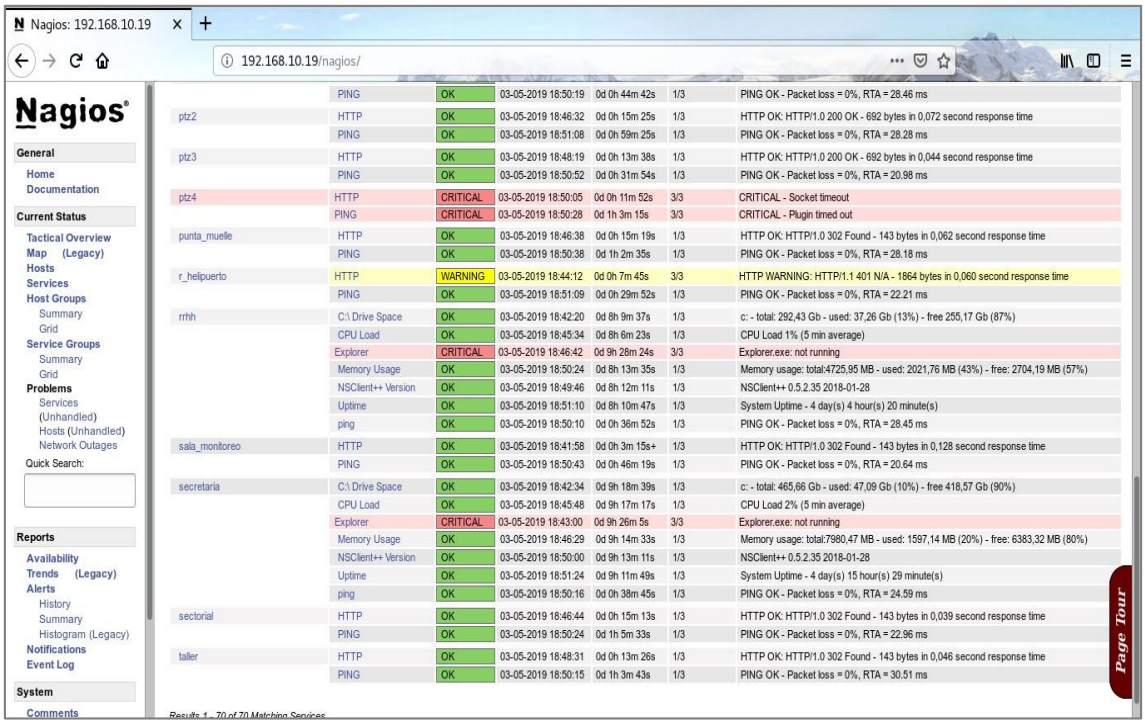


Imagen 9. Reportes del estado de los servicios en los departamentos de la empresa con Nagios
Elaboración: El Autor

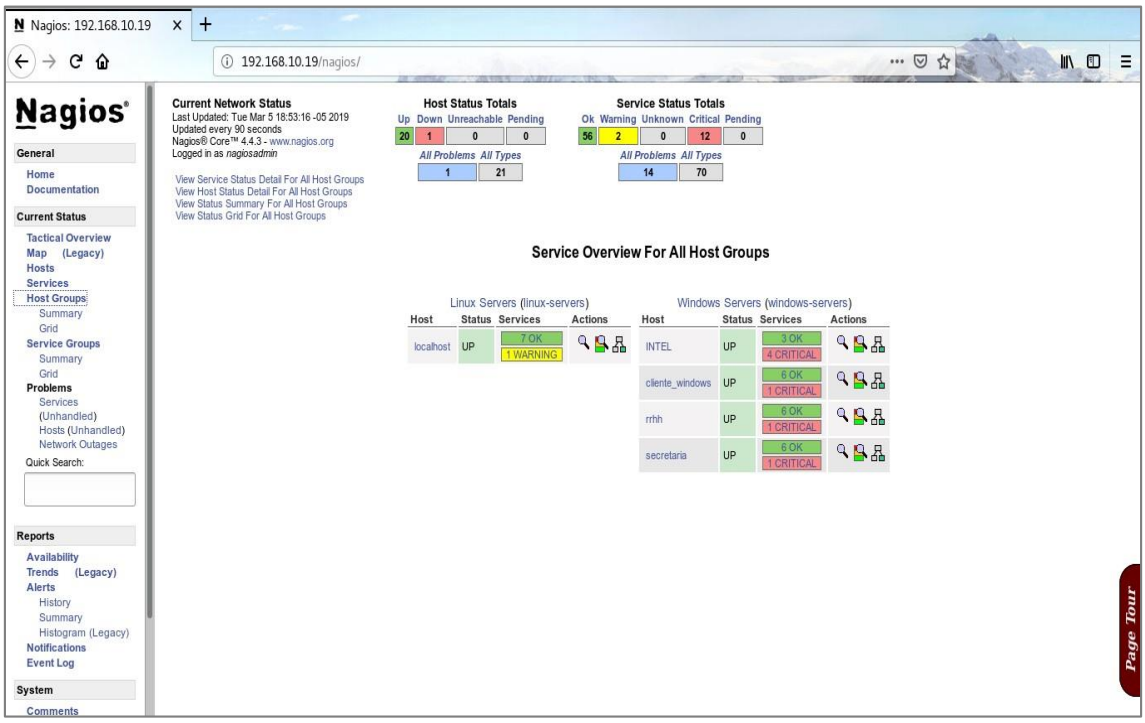


Imagen 10. Reportes del estado actual de los servicios de los grupos de Hosts con Nagios
Elaboración: El Autor

4.3.3 PRTG

Imagen 11. Panel principal de PRTG
Elaboración: El Autor

4.3.4 PANDORA FMS

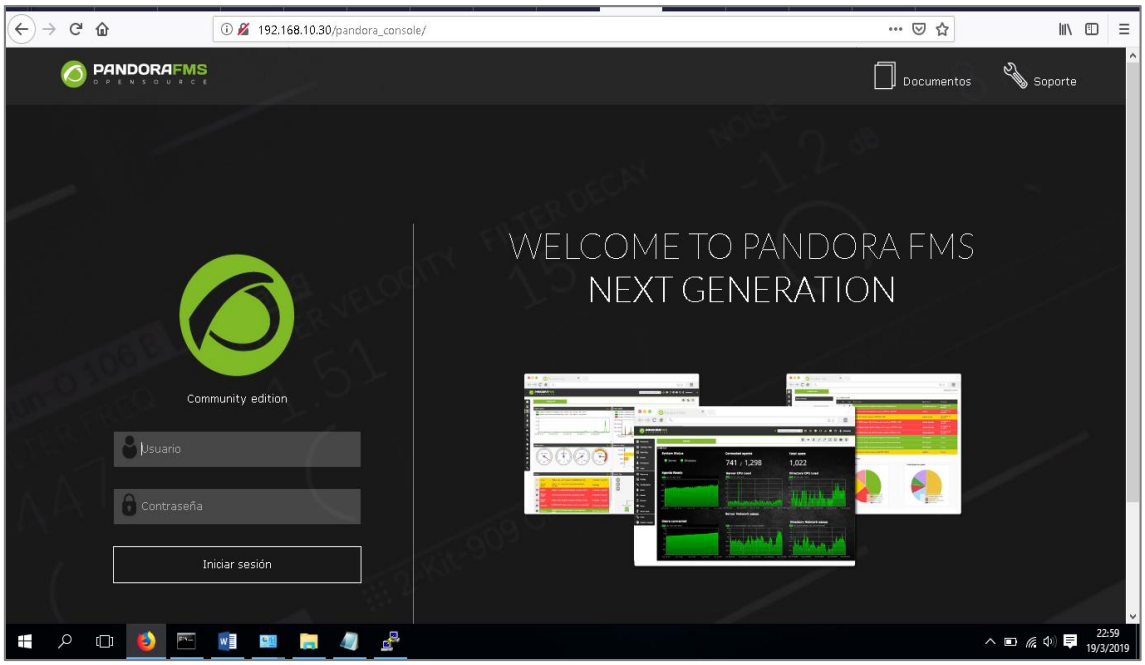


Imagen 12. Página de acceso de Pandora FMS
Elaboración: El Autor

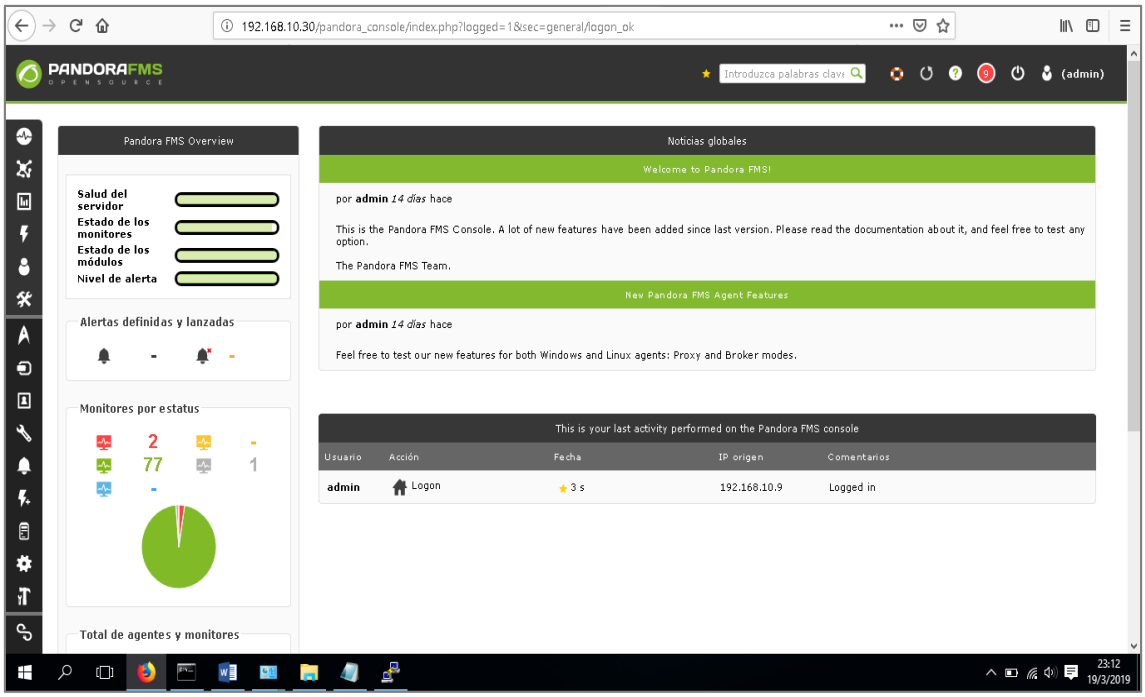


Imagen 13. Panel principal de Pandora FMS
Elaboración: El Autor

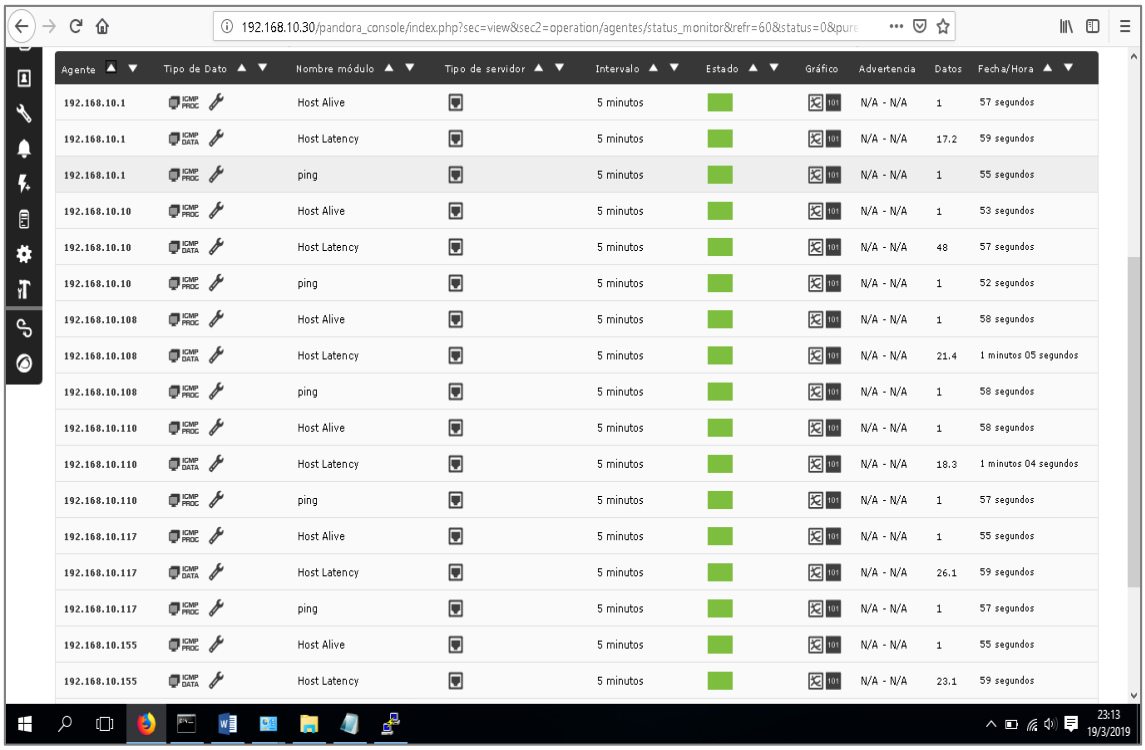


Imagen 14. Monitoreo del estado, latencia y ping hacia los equipos monitorizados por Pandora FMS
Elaboración: El Autor

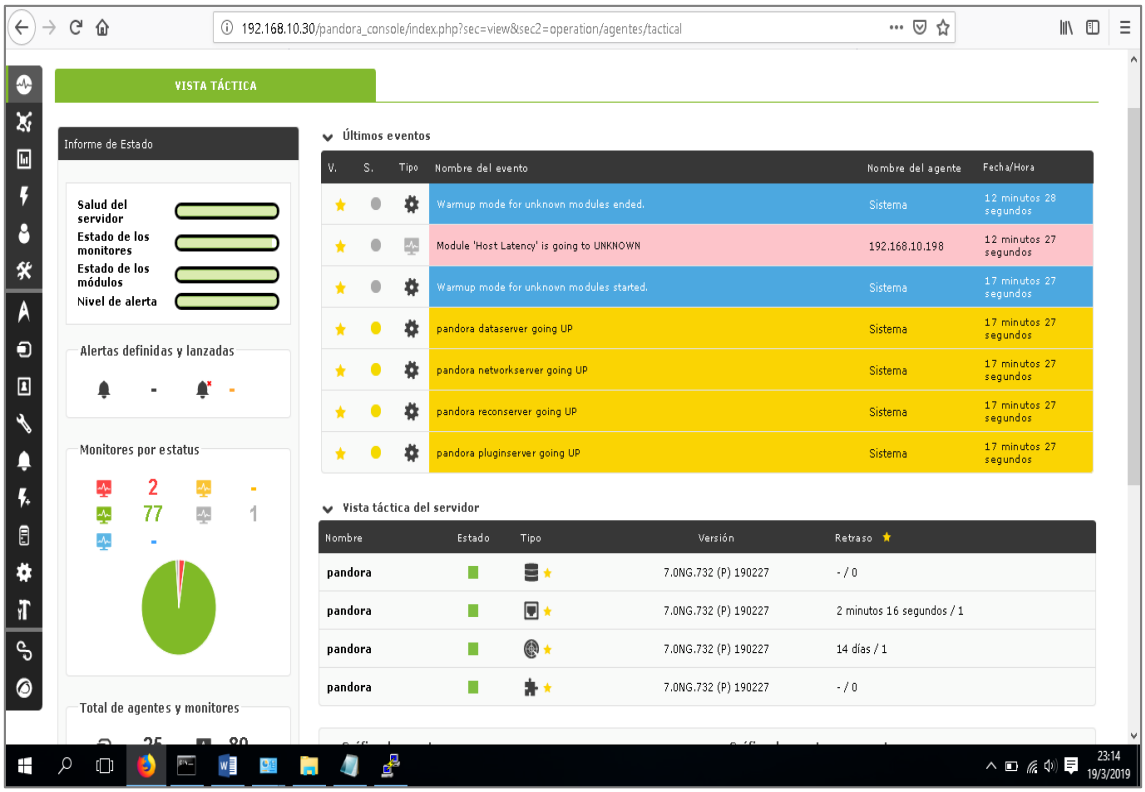


Imagen 15. Reporte de incidentes por Pandora FMS
Elaboración: El Autor

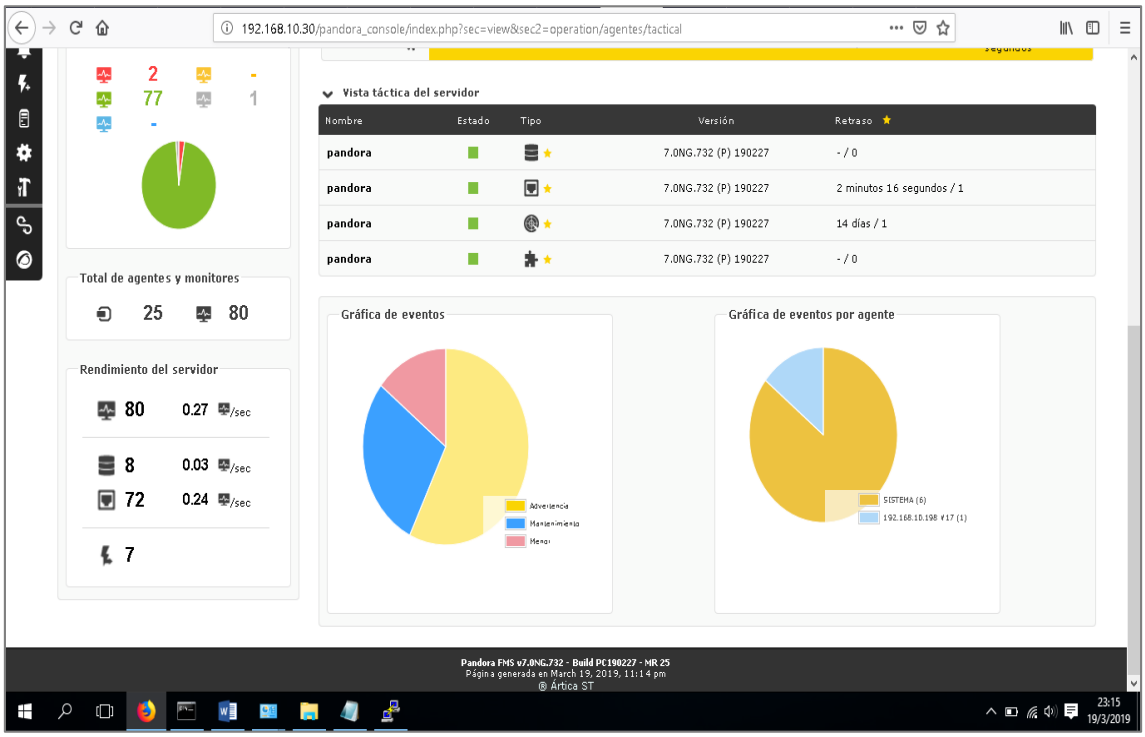


Imagen 16. Gráficas estadísticas de los eventos detectados por Pandora FMS
Elaboración: El Autor

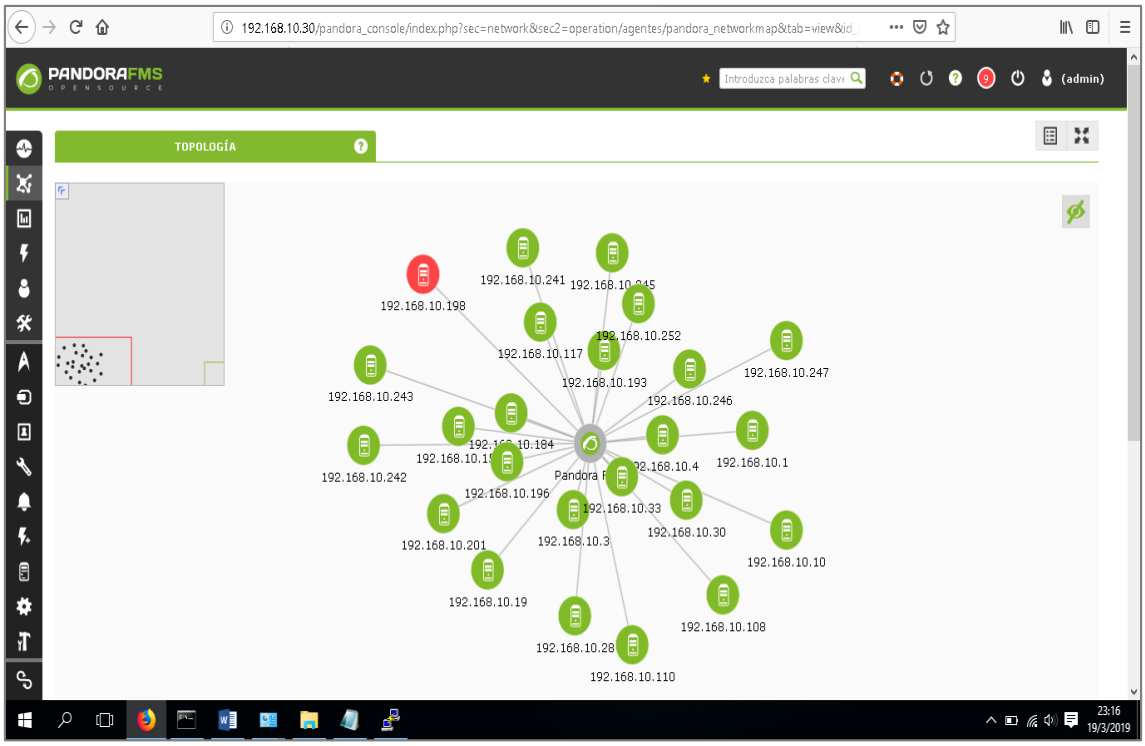


Imagen 17. Mapa de las IPs asignadas en Puerto Atún detectadas con Pandora FMS
Elaboración: El Autor

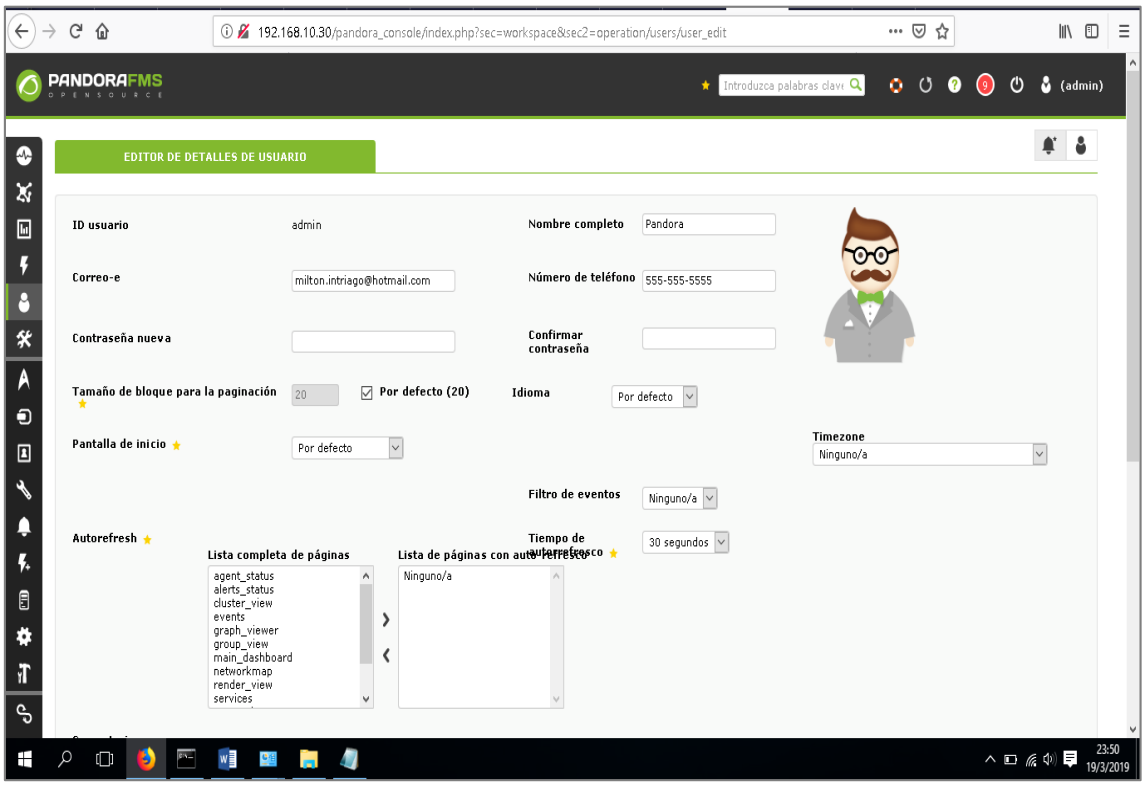


Imagen 18. Administración y configuración de usuarios en Pandora FMS
Elaboración: El Autor

4.4 CATEGORIZACIÓN DE LAS HERRAMIENTAS DE MONITOREO A PARTIR DE LOS RESULTADOS OBTENIDOS POR ESTAS

Antes de hacer el análisis comparativo de las características que presentan las herramientas, se obtuvieron eventos o actividades que reportaron los sistemas de monitoreo como el apagado de ciertos equipos en la red, la sobrecarga de otros, en las diferentes IP como se muestra en el Cuadro 3. Los colores asignados (Cuadro 2) es para identificar la herramienta que detectó el evento.

Cuadro 2. Etiqueta de color para la herramienta de monitoreo de red

HERRAMIENTA	COLOR
PRTG	
ZABBIX	
PANDORA FMS	
NAGIOS	

Elaboración: El Autor

Cuadro 3. Registro de eventos o actividades en las herramientas de monitoreo de red

HERRAMIENTAS / EVENTOS	PRTG	ZABBIX	PANDORA	NAGIOS	IP
NO SE DETECTO PING DETECCIÓN EN TIEMPO REAL					192.168.10.244
DETECTÓ TODO LOS HOST CAÍDOS DETECCIÓN POR CORREO ELECTRÓNICO					192.168.10.0/24
FIREWIRE A SIDO ACTUALIZADO					192.168.10.1
USO DE ANCHO DE BANDA					192.168.10.1
SOBRECARGA DEL CPU					192.168.10.1
SOBRE CARGA EN DISCO DURO + 90% DETECCIÓN DE TIEMPO REAL					192.168.10.252
SOBRE CARGA CPU DEL COMPUTADOR, DETECCIÓN EN TIEMPO REAL					192.168.10.93
APAGADO DE CENTRAL TELEFÓNICA DETECCIÓN POR CORREO ELECTRÓNICO					19.168.10.252

Elaboración: El Autor

En el Gráfico 1 se puede observar que en cuanto al cumplimiento de los requisitos de los sistemas operativos Linux y Windows, la herramienta Nagios es la de mayor porcentaje de cumplimiento con un valor de 4,5/5 mientras que PRTG es la aplicación de menor satisfacción con un valor de 2,5/5.

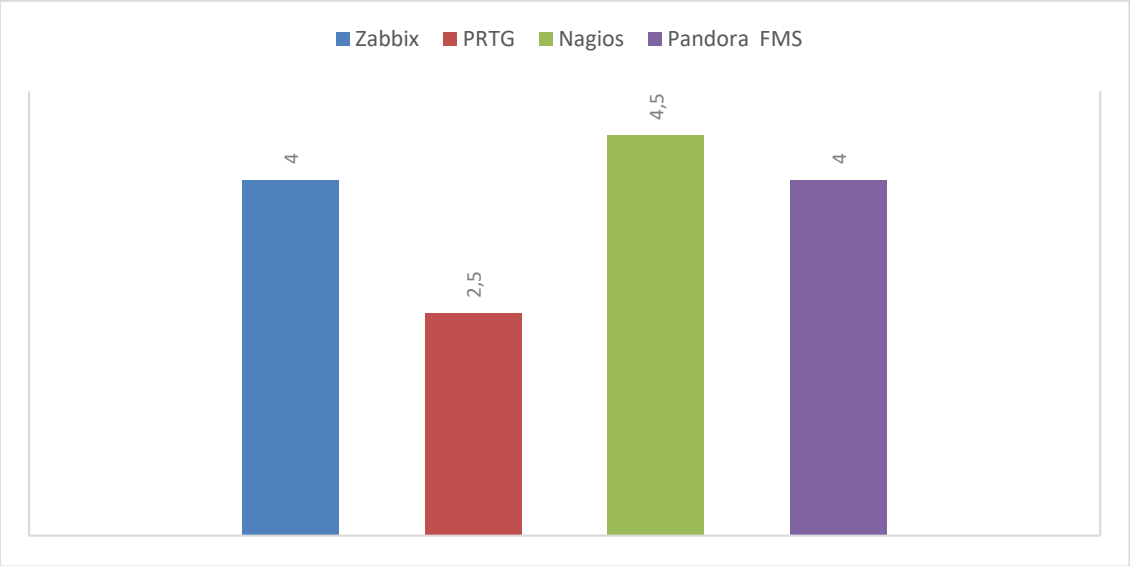


Gráfico 1. Cumplimiento de requisitos del sistema operativo Linux y Windows
Elaboración: El Autor

En el Gráfico 2 se observa que Pandora FMS es la solución con más altos estándares de seguridad con un valor de 3,5/5 mientras que Zabbix, PRTG y Nagios comparten un valor de 2/5.

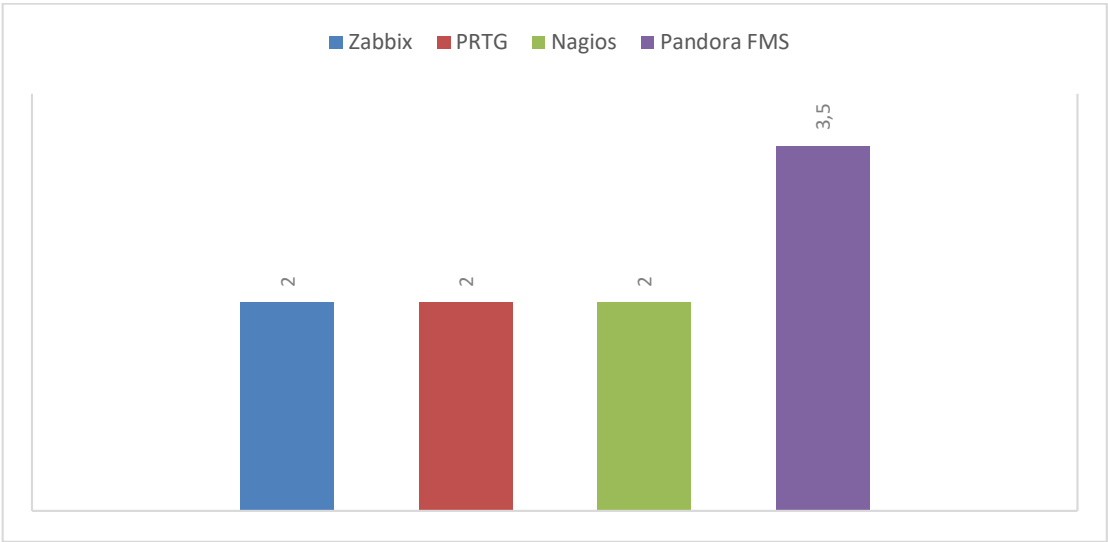


Gráfico 2. Parámetros de seguridad de las herramientas de monitoreo de red
Elaboración: El Autor

En el Gráfico 3 se puede observar que Nagios y Zabbix brindan mayores facultades de soporte con un valor de 4,5/5 mientras que la aplicación de

menores prestaciones en este aspecto es PRTG con un valor de 3/5 y Pandora FMS está valorada con 3,5/5.

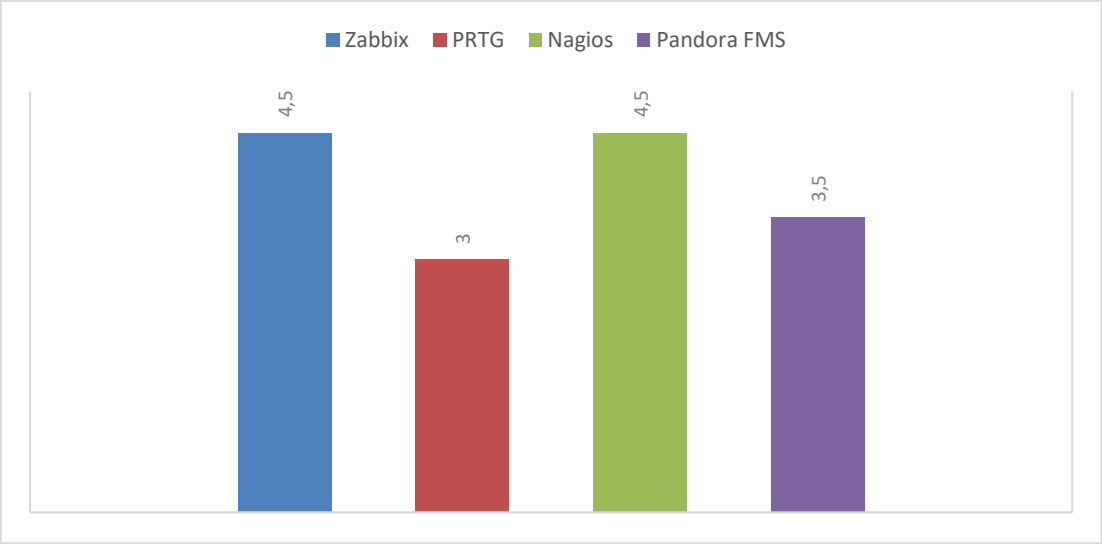


Gráfico 3. Prestaciones de soporte de las herramientas
Elaboración: El Autor

En el Gráfico 4 se puede observar que los sistemas de monitoreo Zabbix, PRTG y Pandora FMS están valorados con 7,5/8 respecto a la facilidad de uso, así mismo Nagios es la herramienta con más baja puntuación con un valor de 7/8.

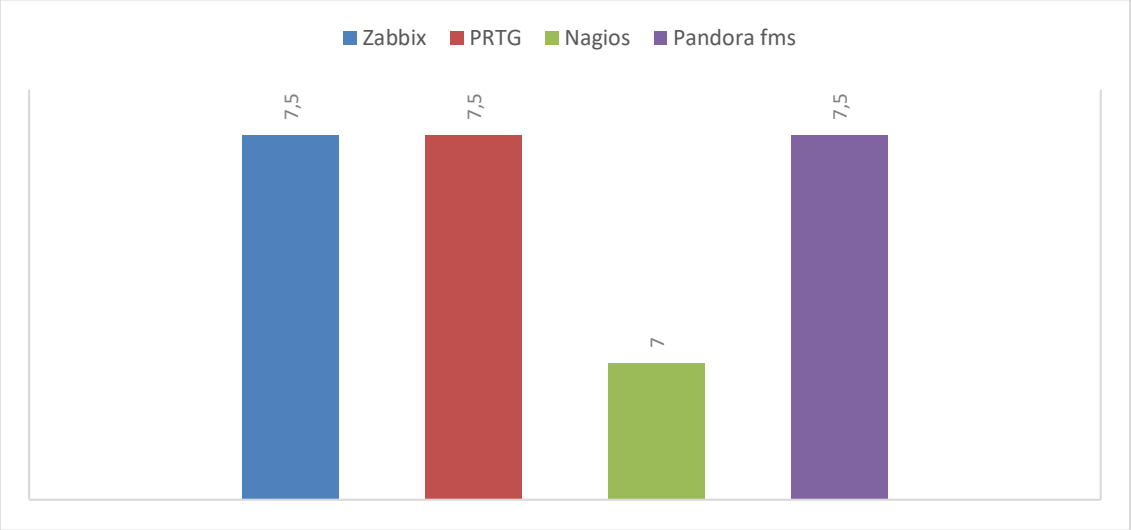


Gráfico 4. Facilidad de uso de las herramientas de monitoreo
Elaboración: El Autor

En el Gráfico 5 se observa que en respuesta al parámetro de administración Nagios cumple con 14/14 de los criterios valorados en este aspecto, PRTG tiene un valor de 11/14, a este lo sigue Pandora FMS con un valor de 10,5/14 y por último Zabbix tiene un valor de 10/14.

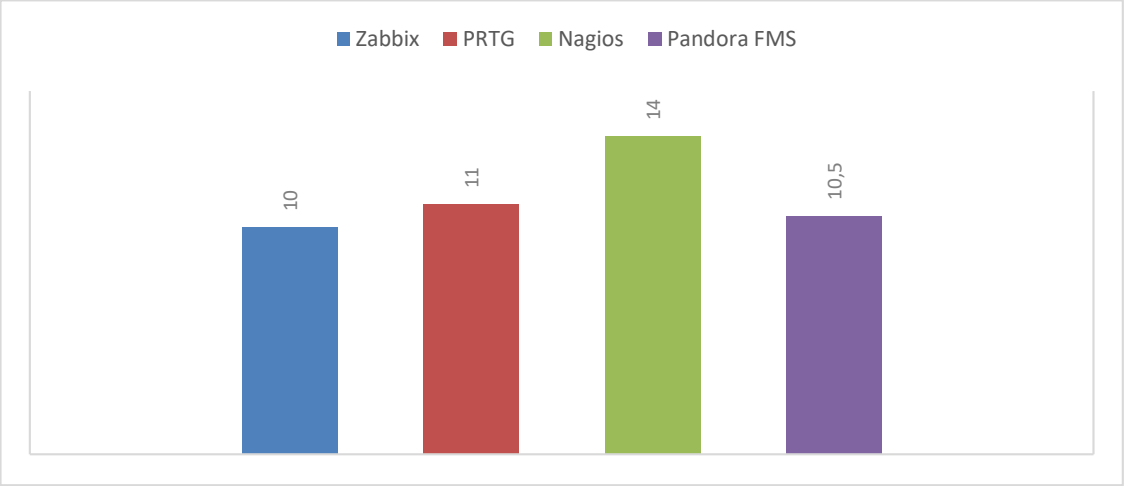


Gráfico 5. Parámetros de administración de las herramientas
Elaboración: El Autor

En el Gráfico 6 se observa la evaluación de las herramientas, verificando que el sistema de monitoreo con mejores prestaciones es Nagios con un valor de 32/38, seguidamente, se ubica Pandora FMS con un total de 29/38, en tercer puesto se encuentra Zabbix con un valor de 28/38 y la aplicación con menores prestaciones es PRTG con un valor de 26/38.

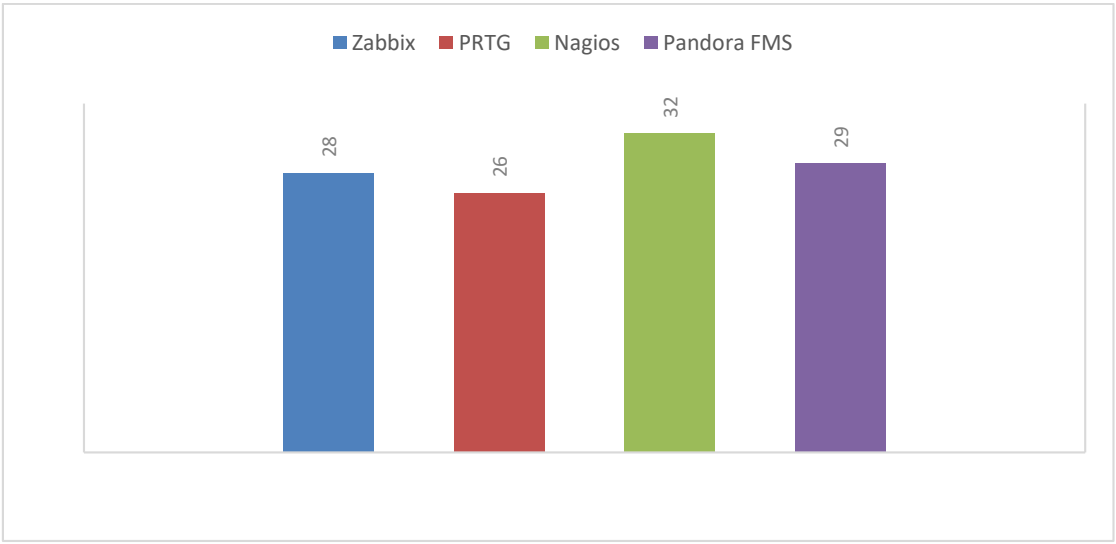


Gráfico 6. Evaluación total de las herramientas
Elaboración: El Autor

Una vez obtenido el registro de actividades, en el Cuadro 4 se realizó la comparativa en cuanto al cumplimiento de actividades y funcionalidades que tienen las herramientas de monitoreo analizadas, estos datos fueron obtenidos luego de implementar cada una de las soluciones y dejarlas en ejecución durante cinco días.

Cuadro 4. Ponderación de las características de las herramientas de monitoreo de red de datos.

HERRAMIENTAS / CARACTERÍSTICAS	ZABBIX 4.0	PRTG NETWORK MONITOR 19.1.48.239	NAGIOS CORE 4.4.3	PANDORA FMS 7.0 NG 732
REQUERIMIENTOS DEL SISTEMA (5)	**4**	**2.5**	**4.5**	**4**
Dificultad de instalación	**Baja (1)**	**Baja (1)**	**Media (0.5)**	**Media (0.5)**
Instalación en Linux	**1**	**0**	**1**	**1**
Instalación en Windows	**0**	**1**	**1**	**1**
Licencias	**1**	**0.5**	**1**	**1**
Bases de datos	**1**	**0**	**1**	**0.5**
SEGURIDAD (5)	**2**	**2**	**2**	**3.5**
Control de versión	**0.5**	**0.5**	**0.5**	**0.5**
Seguimiento de auditoria	**0**	**0**	**0**	**0**
Gestión de sesiones	**0**	**0**	**0**	**1**
Verificación de correo electrónico	**1**	**1**	**1**	**1**
Acceso remoto	**0.5**	**0.5**	**0.5**	**1**
SOPORTE (6)	**4.5**	**3**	**4.5**	**3.5**
Soporte comercial	**1**	**1**	**0.5**	**0.5**
Foro público	**1**	**0**	**1**	**0**
Manuales comerciales	**0.5**	**0**	**0.5**	**0.5**
Ayuda en línea	**0.5**	**1**	**1**	**1**
Desarrollo de terceros	**0.5**	**0**	**1**	**1**
Aprendizaje comercial	**1**	**1**	**0.5**	**0.5**
FACILIDAD DE USO (8)	**7.5**	**7.5**	**7**	**7.5**
Auto descubrimiento	**1**	**1**	**0.5**	**1**
Perfiles de usuario	**1**	**1**	**1**	**1**
Gráficas	**1**	**1**	**1**	**1**
Informes	**1**	**1**	**1**	**1**
Mapas	**0.5**	**0.5**	**1**	**0.5**
Aplicación web	**1**	**1**	**1**	**1**
Informar cumplimiento SLA´s	**1**	**1**	**1**	**1**
Complejidad para administrar nodos	**Baja (1)**	**Baja (1)**	**Media (0.5)**	**Baja (1)**

ADMNISTRACIÓN (14)	10	11	14	10,5
SNMP	1	1	1	1
Plugins o sensores	0.5	1	1	0.5
Estadísticas	1	1	1	1
Soporte para IPv6	1	1	1	1
Aplicación móvil	1	1	1	1
Alertas	1	1	1	1
Notificaciones vía mail	1	1	1	1
Notificaciones vía sms	1	1	1	1
Notificaciones por mensajería instantánea	0	0	1	0
Mapas	0.5	1	1	1
Monitorización distribuida	1	1	1	1
Scripts externos	0	0	1	0
Creación de complementos	0	0	1	0
Registro de Logs	1	1	1	1

Elaboración: El Autor

4.5 ELABORACIÓN DE UN PLAN DE MEJORAS PARA LA OPTIMIZACIÓN DE LA RED DE COMPUTADORAS BASADOS EN LOS RESULTADOS OBTENIDOS DE LAS HERRAMIENTAS DE MONITOREO

Mediante los resultados obtenidos en los diferentes objetivos que se plasmaron y determinaron en esta investigación, se elaboró el plan de mejoras para la optimización de la red de computadoras (Anexo 5), el mismo que brinda una serie de pautas para la implementación de soluciones de monitoreo de red con estrategias de uso y aplicabilidad.

4.6. DISCUSIÓN

Luego de la obtención de los resultados el autor manifiesta que la herramienta de monitoreo Nagios es las más óptima en los aspectos de Soporte, Facilidad de uso, Seguridad, administración permitiendo el control de los equipos y dispositivos conectados en la red, llegando a concordar con Bayas (2015) donde refiere que trabajar con Nagios Core como herramienta principal permite cubrir todas las necesidades y requerimientos de red planteados por la empresa, complementadas con herramientas que al ser usadas con software

libre permiten abaratar costos de implementación del sistema de monitoreo de la red.

Aunque el autor de esta investigación no manifiesta el tipo de monitoreo (pasivo, activo) que se realizará en la empresa, es necesario considerar lo que manifiesta Romero y Padua (2018) en la aplicación del monitoreo pasivo a través de distintas técnicas, las cuales pueden acompañarse de la definición de métricas o alarmas, garantizando así el buen funcionamiento de los dispositivos de red, definiendo el alcance de los dispositivos de monitoreo, así como el espectro a analizar en cada uno de ellos logrando de esta forma una estrategia de monitoreo eficiente. Es necesario una correcta selección de las herramientas y dispositivos a emplear dentro de la red, en función de optimizar los recursos y la propia infraestructura.

En su obra González (2011) realiza un análisis comparativo de 5 herramientas de monitoreo de redes, en dicho trabajo obtiene como resultado que la mejor herramienta es Pandora FMS en su versión comercial y le sigue la versión gratuita del sistema antes mencionado, para el caso del presente estudio pandora FMS se ubica en segundo lugar a solo 3 puntos de Nagios.

El Autor de este trabajo en varios párrafos menciona la importancia de las redes en la administración y fluidez con la que se gestiona la información de las organizaciones, así mismo se hace referencia al conocimiento que tienen los administradores de red en cuanto al estado de sus infraestructuras. Estas ideas son compartidas con autores como Saavedra (2018) y Silva (2013).

Según Fernández (2018) uno de los principales desafíos que los usuarios nuevos tienen con Nagios es el hecho de que tiene que hacer toda la configuración en archivos de texto, desde el archivo de configuración principal hasta la configuración requerida para definir hosts y servicios a ser monitorizados, y en consideración a este y otros aspectos el autor antes citado considera que Zabbix es la solución más factible para implementar según la comparativa que realizó en su trabajo. La complejidad de la administración de Nagios es también mencionada en este documento, sin embargo, la

herramienta resulto la más viable a implementar considerando sus otras funcionalidades.

La investigación de Gonzalez (2014) comparte información con el autor de este trabajo en la revisión bibliográfica sobre el protocolo SNMP, ambos coinciden en que este protocolo da un aporte significativo para conocer el mecanismo a través del cual se puede obtener información relevante de los dispositivos que hacen parte la infraestructura de comunicaciones en la empresa, obteniendo como resultado no solo estadísticas de operación sino el comportamiento, y para evidenciarlo ambas investigaciones sugieren que se realicen capturas con el software wireshark.

En el trabajo de Freire & Sánchez (2016) se apuesta por la implementacion de PRTG como solucion de monitoreo puesto que el tiempo de aprendizaje de la herramienta es mucho menor que otros sistemas, además de ser una solucion amigable y autosuficiente. Estas caracteristicas son compartidas por el autor de este trabajo pero considera un inconveniente en el licenciamiento de la herramienta.

CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

- En el desarrollo de la investigación se efectuó una comparativa de herramientas de monitoreo de red, de las cuales se pudo seleccionar la herramienta de análisis con las mejores características y operatividad entre todas las opciones, de manera que determinó adecuadamente las amenazas y componentes defectuosos en la red de computadoras de la empresa Puerto Atún, para posteriormente realizar el diseño de un modelo de red y estrategias de monitoreo que brindaron una mejora a los procesos de control y gestión de las operaciones técnicas.

- El diseño de la estrategia de red nos permitió determinar los equipos tecnológicos que se iban a monitorear en la red a través de la topología de red que tiene la empresa.

- Se identificó cada una de las propiedades de las soluciones Zabbix, Nagios, Pandora FMS y PRTG para conocer cuál es más efectiva.

- Una vez hecha la implementación de las herramientas antes mencionadas se pudo determinar que las más fáciles de instalar y configurar fueron Zabbix y PRTG, el proceso de instalación y configuración de las soluciones Nagios y Pandora FMS resulto más complejo. En la evaluación de las soluciones, Nagios se presentó como la herramienta con el mayor nivel de cumplimiento con los parámetros requeridos para su implantación. La herramienta PRTG cuenta con importantes prestaciones y una administración relativamente sencilla, pero por el tema de licencia no será considerada en la implementación, ya que, el gerente de la empresa manifestó que no se incurra en gastos para el control de la infraestructura tecnológica.

- El análisis comparativo de las herramientas permitió determinar la mejor aplicación para el monitoreo de la red y los servicios de la entidad. A través del análisis de los resultados que brindaron las herramientas instaladas se lograron identificar las actividades que provocan un degrado en el rendimiento de la red o del funcionamiento de los servicios y en base a esa información se establecen los mecanismos de control para la protección de los datos y mejorar el rendimiento de la red mediante un plan de mejoras para la optimización de la red y los servicios. Cabe recalcar que es necesario que en la evaluación de las categorías de las herramientas se estime un tiempo no menor a 5 días, debido a que entre mayor tiempo de funcionalidad de las soluciones se puede determinar un puntaje óptimo de las mismas y de esta manera obtener mejores resultados.

- El plan de mejoras de optimización del monitoreo de la red en Puerto Atún contribuye a un mejor uso y funcionalidad de equipos dentro de la infraestructura de red mediante herramientas de monitoreo.

5.2 RECOMENDACIONES

- Efectuar monitorios en la red de computadoras de la empresa, y posteriormente mandar alertas preventivas de manera periódica, puesto que las estaciones físicas se encuentran aledañas a un sector marítimo del cual tiende a degradar la infraestructura, poniendo así en constante observación el estado de la red.

- Es importante contar con un suministro energético adicional que mantenga la disponibilidad de los equipos que van a monitorear la red de computadoras y, por ende, estos solventen la disponibilidad de los servicios y las comunicaciones internas. También contar con equipos en bodega como un stock de repuestos, de aquellos dispositivos en los que se hallan identificado anomalías en su funcionamiento o sobrecarga en alguno de sus componentes.

- Se sugiere que para la selección de herramientas para la optimización del monitoreo de la red de computadoras se evalúe cada una de ellas para que se obtengan resultados óptimos en el momento de su implementación.

- Se recomienda la implementación de solo una herramienta de monitoreo, la cual es fundamental para garantizar la disponibilidad o pronta recuperación de los dispositivos que sufran algún imprevisto.

- La empresa Puerto Atún puede implementar el plan de mejoras para la optimización de la red en el tiempo que consideren importante, sin dejar de considerar que entre más rápido se implemente más rápido será la optimización de la red y tendrán mayores beneficios.

BIBLIOGRAFÍA

Alava, Z. A., & Guerrero, R. G. (2018). Análisis de uso, Beneficios y Simulación de Pandora FMS para el Monitoreo de Sistemas y Redes. Guayaquil: Facultad de Ciencias Matematicas y Fisicas.

Bayas, V. J. (2015). Servidor de control de dispositivos y servicios mediante el protocolo SNMP para la red de datos en CELEC E.P. Unidad de Negocios Hydragoyan. Ambato.

Dalle, V. A. (2015). Mastering Zabbix. Packt Publishing Ltd.

Dalle, V. A., & Kewan, L. S. (2015). Zabbix network monitoring essentials. Packt Publishing Ltd.

Deokule, K., Modi, P., Mistry, D., Patki, H., Patel, A., & Abuzaghleh, O. (2016). Network Traffic Measurement and Analysis.

Fava, L. A. (2016). Gerenciamiento de Redes de Datos usando Java & SNMP. La Plata.

Fernández, A. A. (2018). Estudio e implementación de un entorno de gestión para la red privada del laboratorio docente de telemática (GIT-UNICAN). Santander: Universidad de Cantabria.

Freire, A. D., & Sánchez, B. R. (2016). Análisis y elaboración de un plan de optimización para los recursos de la red en la empresa CORLASOSA S.A. mediante la implementación de la herramienta PRTG. Guayaquil.

Gallego, A. M. (2015). Rediseño e implementación del sistema de monitoreo de la red de telecomunicaciones de distribuidora NISSAN S.A. Bogotá.

Gavilares, R. L. (2016). Implementación de un sistema de monitoreo en el data center de la empresa Seguros Oriente S.A. Quito.

Ghosh, A., Nashaat, M., & Miller, J. (2019). The current state of software license renewals in the IT industry. Information and Software Technology, 139-152.

González, A. S. (2011). Comparativa d'eines de monitorització de sistemes. Barcelona: Universitat Oberta de Catalunya.

González, V. (2014). Diseño e implementación de un sistema de monitoreo basado en snmp para la red nacional acaemica de tecnilogía avanzada. Tesis de Ingeniería de Telecomunicaciones. Universidad Santo Tomás. Bogotá, Colombia, 1-86.

Issariyapat, C., Pongpaibool, P., Mongkolluksame, S., & Meesublak, K. (2012). Using Nagios as a groundwork for developing a better network monitoring system. Proceedings of PICMET'.

Kora, A. D., & Soidridine, M. M. (2012). Nagios based enhanced IT management system. International Journal of Engineering Science and Technology.

Nagios Core. (4 de Abril de 2019). Obtenido de Nagios Core: https://www.nagios.org/projects/nagios-core/

Newman, M. (2018). Networks. Oxford university press.

Pandora FMS. (2019). Obtenido de Pandora FMS: http://pandorafms.org/es/

Pérez, S. L. (2013). Estudio comparativo de los sistemas de gestión y monitoreo basados en los requerimientos generales de la red de un campus universitario. Quito.

Pilozo, C. D., & Zambrano, B. G. (2013). Estudio del Ancho de Banda para el tráfico de Redes WAN de los ISP, con estudiantes de la Universidad Politécnica Salesiana Sede Guayaquil carrera Ingeniería de Sistemas, mediante la implementación de una página web. Guayaquil.

PRTG Network Monitor. (2019). Obtenido de PRTG Network Monitor: https://www.es.paessler.com/prtg

Qadir, M., & Adnan, M. (2010). Comparative Analysis of two Open Source Network Monitoring Systems: Nagios & OpenNMS.

Quispe, B. J. (2018). Implementacón de un sistema de monitoreo y control de red, para un canal de televisión, basado en herramientas Open Source y Software Libre. Perú: Universidad Nacional del Altiplano.

Romero, G. J., & Padua, S. R. (2018). Los recursos de red y su monitoreo. . Revista Cubana de Informática.

Saavedra, D. C. (2018). Control de servicios de red y servidores basado en herramientas de administración de red y políticas de gestión de calidad. Esmeraldas: PUCESE-Escuela de Sistemas y Computación.

Sánchez, C. D. (2017). Implementación de un sistema de monitoreo y protección de datos en la red de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial. Ambato: Universidad Técnica de Ambato: Facultad de Ingeniería en Sistemas, Electrónica e Industrial.

Silva, P. S. (2013). Análisis e implementación de la herramienta de código libre Pandora FMS para el monitoreo de nodos de telecomunicaciones y servidores en ambientes Windows y Linux, usando el protocolo SNMP y la tecnología instrumental de administración de Windows WMI. Quito.

Tobar, G. A. (2015). Implementación de un sistema de monitoreo de los niveles de servicio acordados por los proveedores de servicio de Internet para la Superintendencia de Telecomunicaciones . Quito: EPN.

Velasco, B. C., & Cagua, O. G. (2017). Implementación de un sistema de monitoreo de redes utilizando herramientas Open Source y proveer

servicios de directorio a través de Active Directory en la facultad de Filosofia, Letras y Ciencias de la Educación de la Universisdad de Guayaquil . Guayaquil.

Wetherall, D. J. (2012). Redes de Computadoras, 5ta Edición.

White, C. (2015). Data communications and computer networks: A business user's approach. . Cengage Learning.

Wu, C. H., & Irwin, J. D. (2016). Introduction to computer networks and cybersecurity. . CRC Press.

Zabbix. (2019). Obtenido de zabbix: https://www.zabbix.com/about

ANEXOS

ANEXO 1

LEVANTAMIENTO DE INFORMACIÓN EN LA EMPRESA PUERTO ATÚN

Jaramijo, 14 de enero de 2019

PARA: Ing. Raúl Paladines Basurto
GERENTE DE LA EMPRESA PUERTO ATUN

ASUNTO: Solicitud de Información para Trabajo de Titulación.

De mi consideración:

Reciba un cordial saludo. Por medio del presente solicito de manera respetuosa, salvo su mejor criterio, se me otorgue el permiso respectivo para efectuar un levantamiento de información, con el propósito de desarrollar del trabajo de titulación: "***COMPARATIVA ENTRE HERRAMIENTAS DE MONITOREO DE RED DE COMPUTADORAS APLICADAS A LA EMPRESA PUERTO ATÚN***", correspondiente al autor Ing. Milton Luyely Intriago Cedeño, estudiante de la Maestría de Tecnología de Información, mención Redes y Sistemas Distribuidos de la ESPAM MFL, del cual se obtendrá una propuesta de mejora a dicha empresa.

Por la atención que se brinde al presente, anticipo mis agradecimientos.

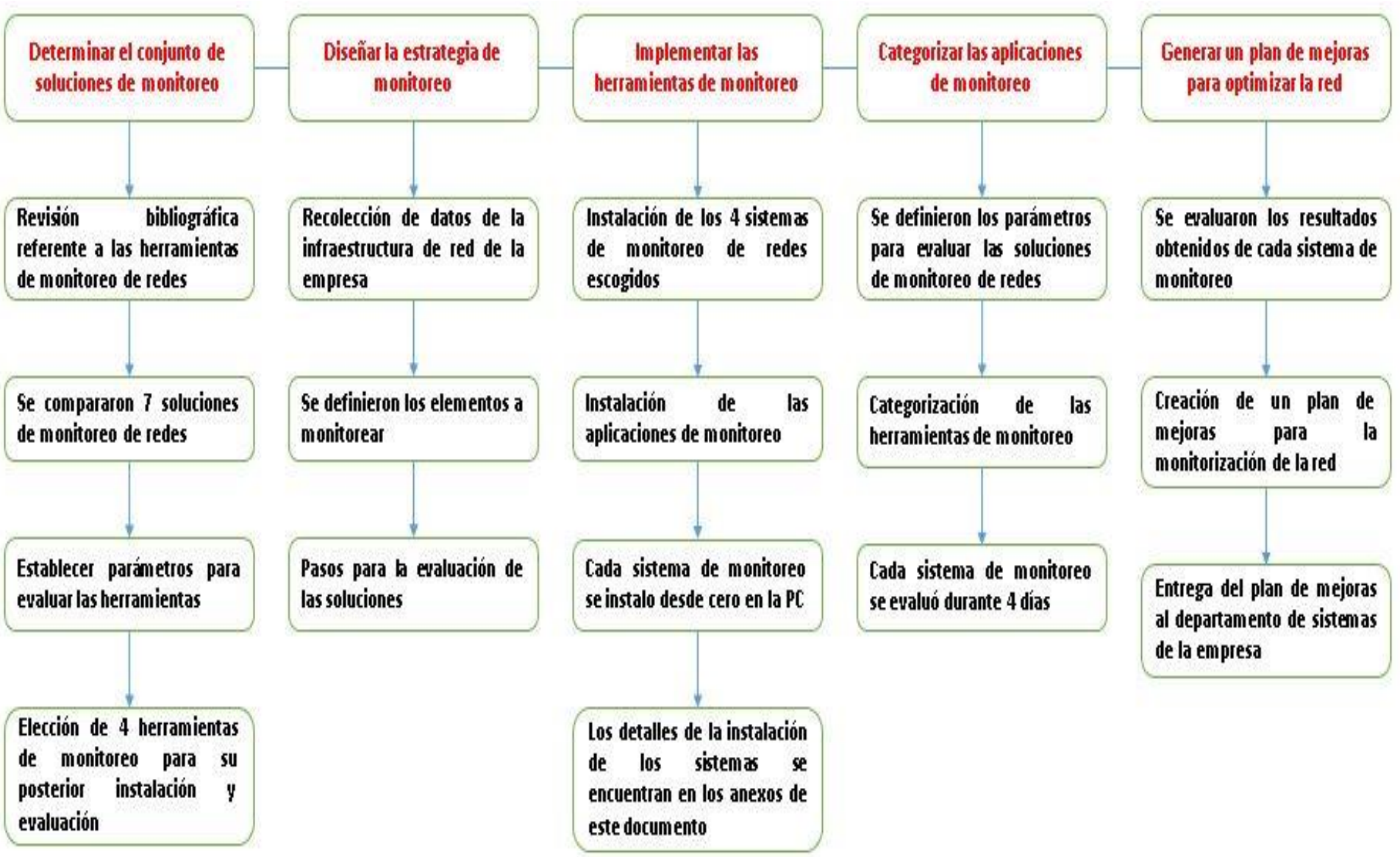
Atentamente,

Ing. Milton Luyeli Intriago Cedeño
C.I. 1313191890
ESTUDIANTE DE LA MAESTRIA EN TI

Acti

ANEXO 2

REPRESENTACIÓN DE LA METODOLOGÍA DE LA INVESTIGACIÓN


Determinar el conjunto de soluciones de monitoreo
Diseñar la estrategia de monitoreo
Implementar las herramientas de monitoreo
Categorizar las aplicaciones de monitoreo
Generar un plan de mejoras para optimizar la red
Revisión bibliográfica referente a las herramientas de monitoreo de redes
Se compararon 7 soluciones de monitoreo de redes
Establecer parámetros para evaluar las herramientas
Elección de 4 herramientas de monitoreo para su posterior instalación y evaluación
Recolección de datos de la infraestructura de red de la empresa
Se definieron los elementos a monitorear
Pasos para la evaluación de las soluciones
Instalación de los 4 sistemas de monitoreo de redes escogidos
Instalación de las aplicaciones de monitoreo
Cada sistema de monitoreo se instalo desde cero en la PC
Los detalles de la instalación de los sistemas se encuentran en los anexos de este documento
Se definieron los parámetros para evaluar las soluciones de monitoreo de redes
Categorización de las herramientas de monitoreo
Cada sistema de monitoreo se evaluó durante 4 días
Se evaluaron los resultados obtenidos de cada sistema de monitoreo
Creación de un plan de mejoras para la monitorización de la red
Entrega del plan de mejoras al departamento de sistemas de la empresa

ANEXO 3

INSTALACIÓN DE LAS HERRAMIENTAS PARA LA OPTIMIZACIÓN DE MONITOREO DE RED DE COMPUTADORAS

ANEXO 3 A. INSTALACIÓN DE ZABBIX

Zabbix es una herramienta de código abierto para el monitoreo de redes y aplicaciones. La empresa ofrece una amplia gama de servicios profesionales diseñados para satisfacer las demandas únicas de cada cliente, entre los que contempla: servicios de implementación, integración, desarrollo personalizado y consultoría, así como diversos programas de capacitación. A continuación, se detalla la instalación de zabbix en Ubuntu Server 16.04 (zabbix, 2019).

1. Instalación de zabbix-server, el frontend y el agente

```
# apt –y install zabbix-server-mysql zabbix-frontend-php zabbix-agent
```

2. Creación y configuración inicial de la base de datos

```
# mysql –u root –p

password
mysql> create database zabbix character set utf8 collate utf8_bin;
mysql> grant all privileges on zabbix.* to zabbix@localhost identified
by 'password';
mysql> quit;
```

3. Importación del esquema inicial y los datos

```
# zcat /usr/share/doc/zabbix-server-mysql*/create.sql.gz | mysql -
uzabbix -p zabbix
```

4. Configuración de la base de datos para zabbix-server

```
DBPassword=password (Este parámetro se edita en:
/etc/zabbix/zabbix_server.conf)
```

5. Configurar PHP para el frontend de zabbix

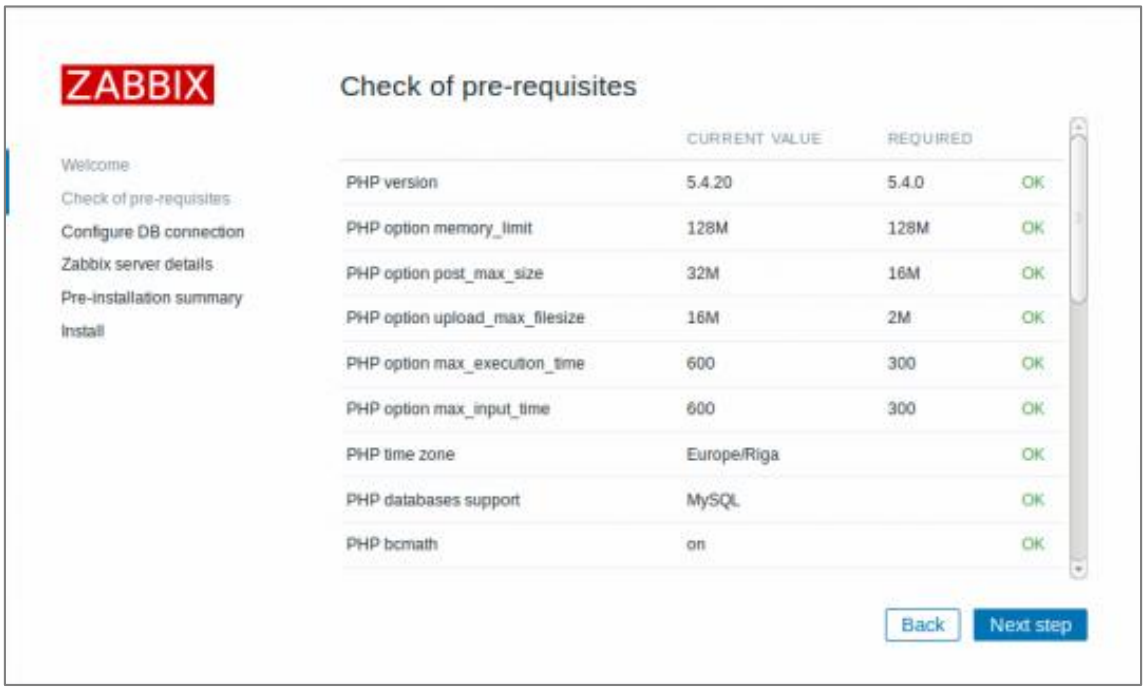
```
php_value date.timezone America/Guayaquil (Editar
/etc/zabbix/apache.conf)
```

6. Iniciar zabbix y el agente, configurar que ambos se carguen cuando arranca el sistema, desde el navegador acceder a: http://ip_servidor/zabbix

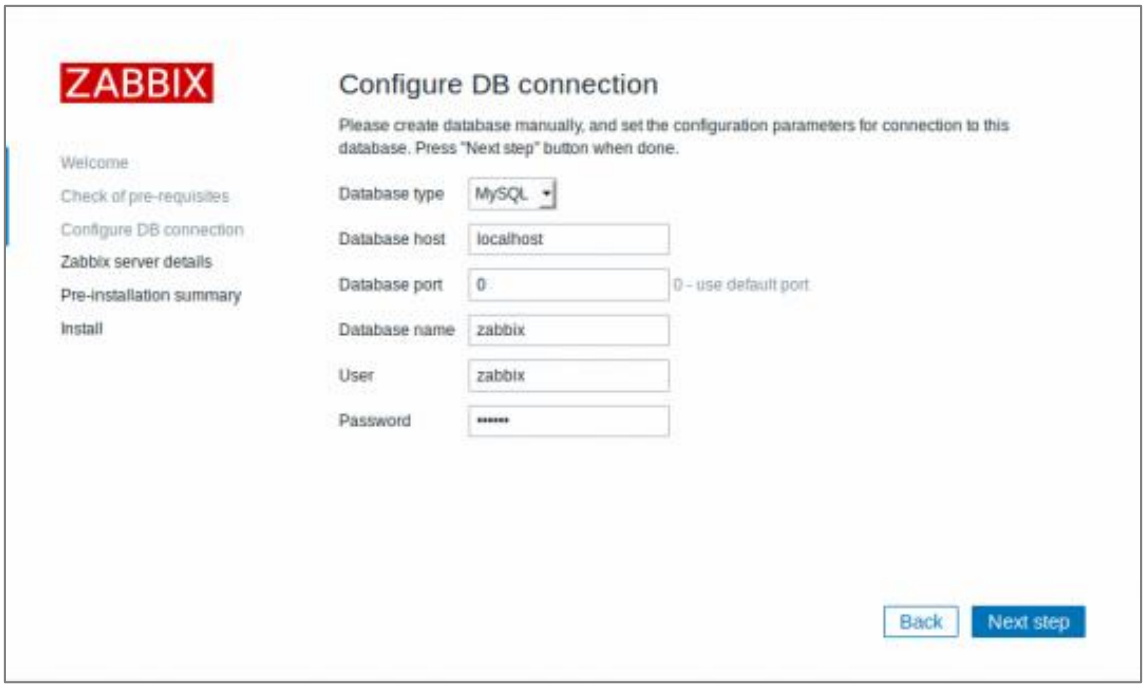
```
# systemctl restart zabbix-server zabbix-agent apache2
# systemctl enable zabbix-server zabbix-agent apache2
```

7. Luego de finalizar la instalación por consola hay que ingresar mediante navegador a la url: http://ip_servidor/zabbix

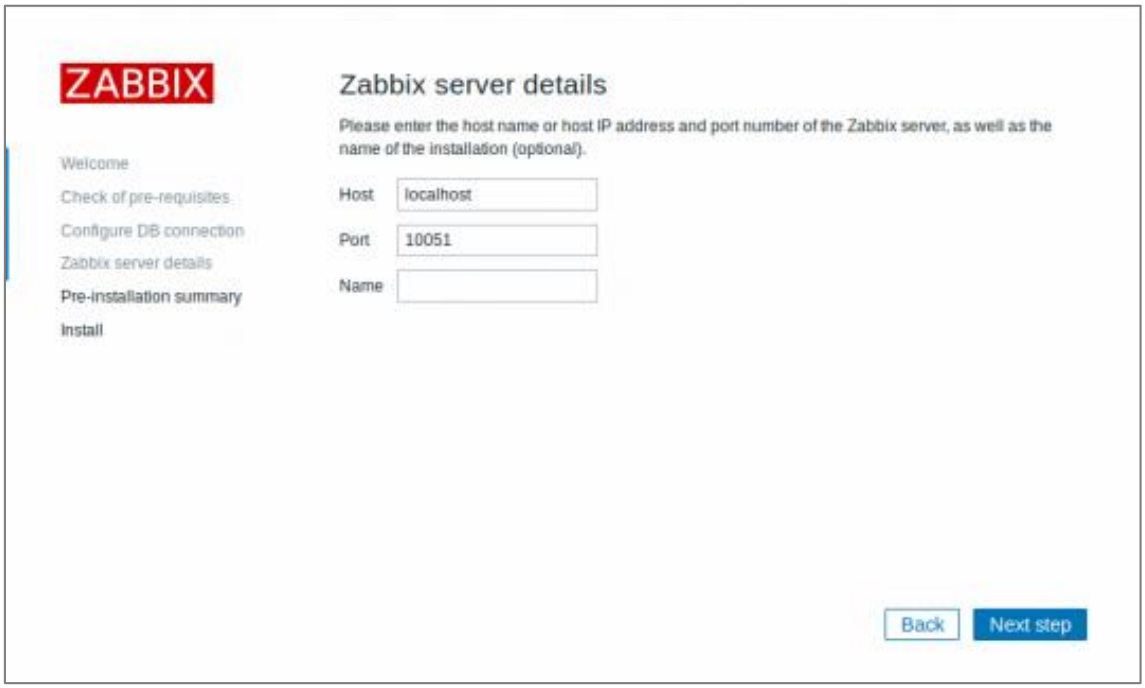
8. Verificar que todos los prerrequisitos de software estén instalados



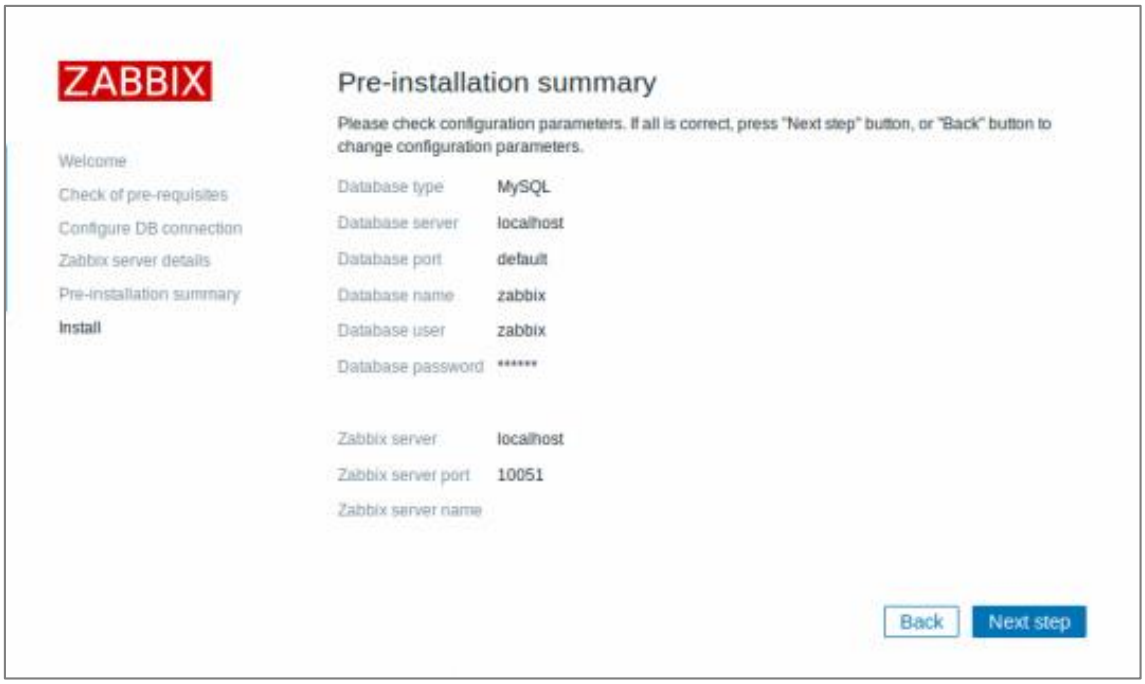
9. Ingresar los datos de conexión a la base de datos que ya fue creada para zabbix



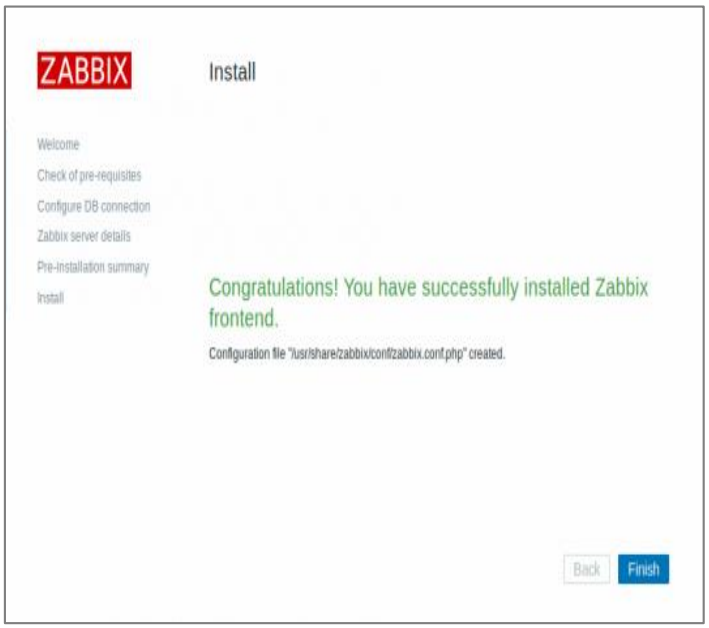
10. Ingresar los detalles del servidor zabbix solicitados

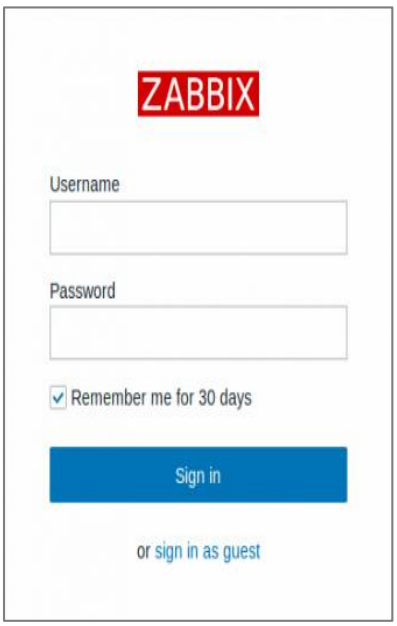


11. Revisar y verificar el resumen de configuraciones



12. Finalizando el proceso de instalación y formulario de acceso al panel de administración del servidor, el usuario por defecto es admin y la contraseña zabbix





ANEXO 3 B: INSTALACIÓN DE NAGIOS CORE

Nagios Core es un sistema de monitorización de redes ampliamente utilizado, de código abierto, que se encarga de controlar los equipos y servicios que se especifican, alertando cuando el comportamiento de los mismos no sea el

adecuado. Además sirve como un programador de eventos básico, procesa dichos eventos y administra las alertas que se producen en los elementos monitorizados, cuenta con varias API's que se utilizan para ampliar sus capacidades para realizar tareas adicionales (Nagios Core, 2019).

1. Desabilitar SELINUX modificando el archivo /etc/selinux/config

SELINUX=enforcing (para aplicar los cambios hay que reiniciar el sistema)

2. Es necesario habilitar los puertos del servicio web y reiniciar el firewall

```
# firewall-cmd --permanent –add-port=80/tcp
# firewall-cmd --permanent –add-port=443/tcp
# firewall-cmd --reload
```

3. Instalar las dependencias necesarias para instalar Nagios

```
# yum install –y gettext wget net-snmp-utils openssl-devel glibc-common unzip perl epel-release gcc php gd automake autoconf httpd make glibc gd-devel net-snmp perl-Net-SNMP
```

4. Agregar el usuario Nagios

```
# useradd nagios
```

5. Agregar como grupo secundario Nagios al usuario apache

```
# usermod –a –G nagios apache
```

6. Descargamos Nagios desde github con wget

 # https://github.com/NagioEnterprises/nagioscore/releases (de esta url copiar el enlace de [nagios-4.4.2.tar.gz])

 # wget https://github.com/NagioEnterprises/nagioscore/releases/download/nagios-4.4.2/nagios-4.4.2.tar.gz (este es el enlace copiado del punto anterior)

7. Descomprimir el archivo descargado de Nagios

```
# tar -xzvf nagios-4.4.2tar.gz
```

8. Ingresar a la carpeta descomprimida, para luego compilar e instalar Nagios

```
# cd nagios-4.4.2

# ./configure

# make all

# make install

# make install-init

# make installcomand-mode

# make install-config

# make install-webconfig
```

9. Habilitar el servicio de Nagios para que cargue al iniciar el sistema

```
# systemctl enable nagios (crea un enlace simbólico)
```

10. Habilitar el servicio de apache para que cargue al iniciar el sistema

```
# systemctl enable httpd (crea un enlace simbólico)
```

11. Configurar parámetros de seguridad de httpd para usuarios específicos

```
# htpasswd –c /usr/local/nagios/etc/htpasswd.users nagiosadmin

Password: 'Aquí ingresa el password'
```

12. Iniciar y comprobar los servicios

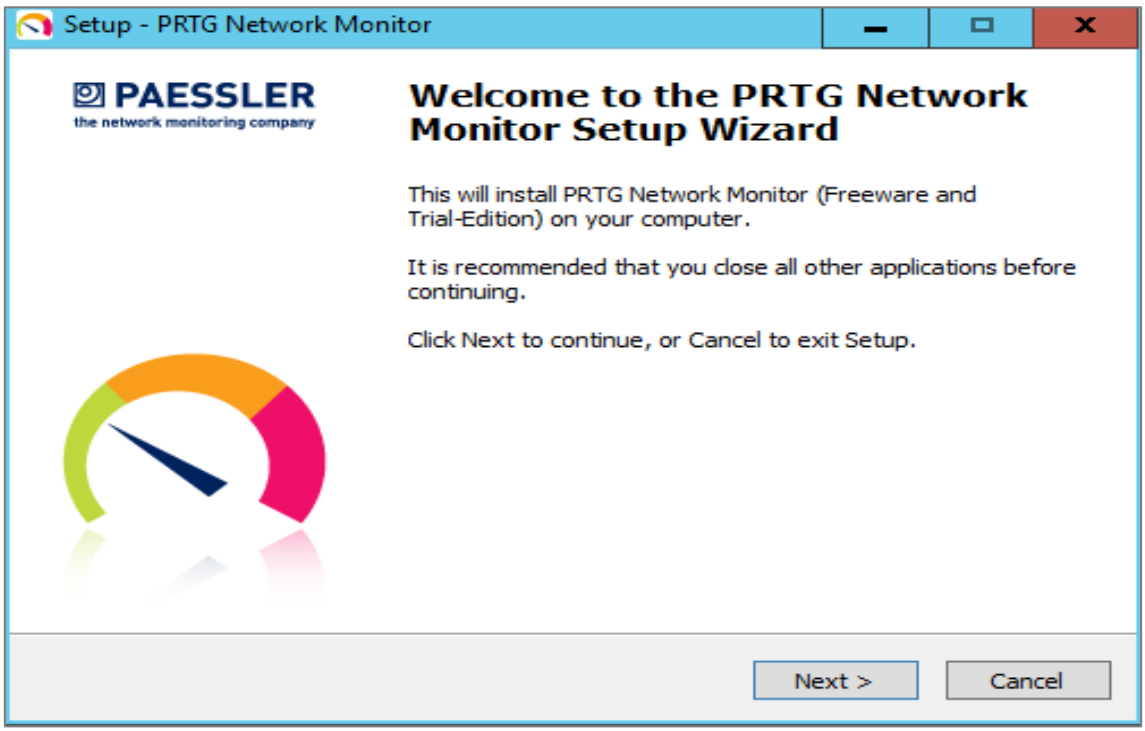
```
# systemctl start httpd

# systemctl start nagios

# systemctl status httpd

# systemctl status hnagios
```

13. Acceder a Nagios con la url: http://ip_address_servidor/nagios y acceder con los datos de seguridad para httpd que fueron configurados anteriormente

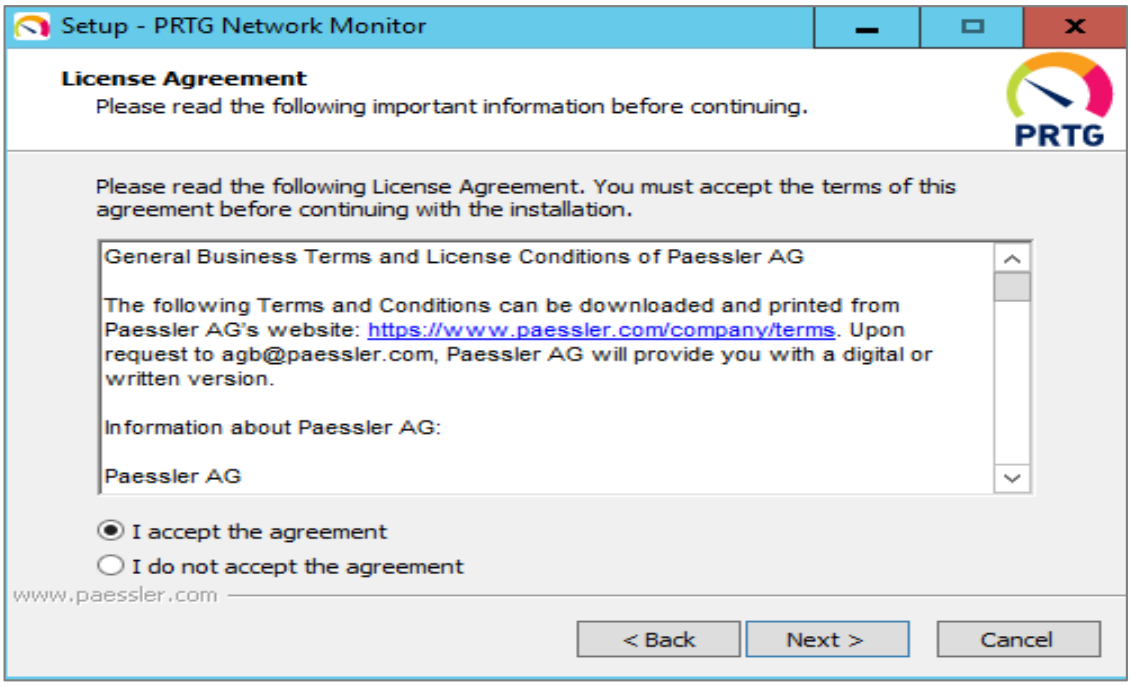
ANEXO 3 C: INSTALACIÓN DE PRTG

PRTG Network Monitor es una herramienta que supervisa los sistemas, dispositivos y aplicaciones de las infraestructuras de TI. Esta solución puede monitorizar el tráfico de red, los paquetes, el ancho de banda, las aplicaciones, servicios en la nube, bases de datos, entornos virtualizados, tiempo de actividad, entre otros sistemas y servicios, es una solución únicamente disponible para entornos Windows y que cuenta con la versión comercial y la versión gratis luego de 30 días de prueba, la cual está limitada en sus funcionalidades. A continuación se detalla el proceso de instalación de la herramienta en sobre el sistema Windows 10. (PRTG Network Monitor, 2019)

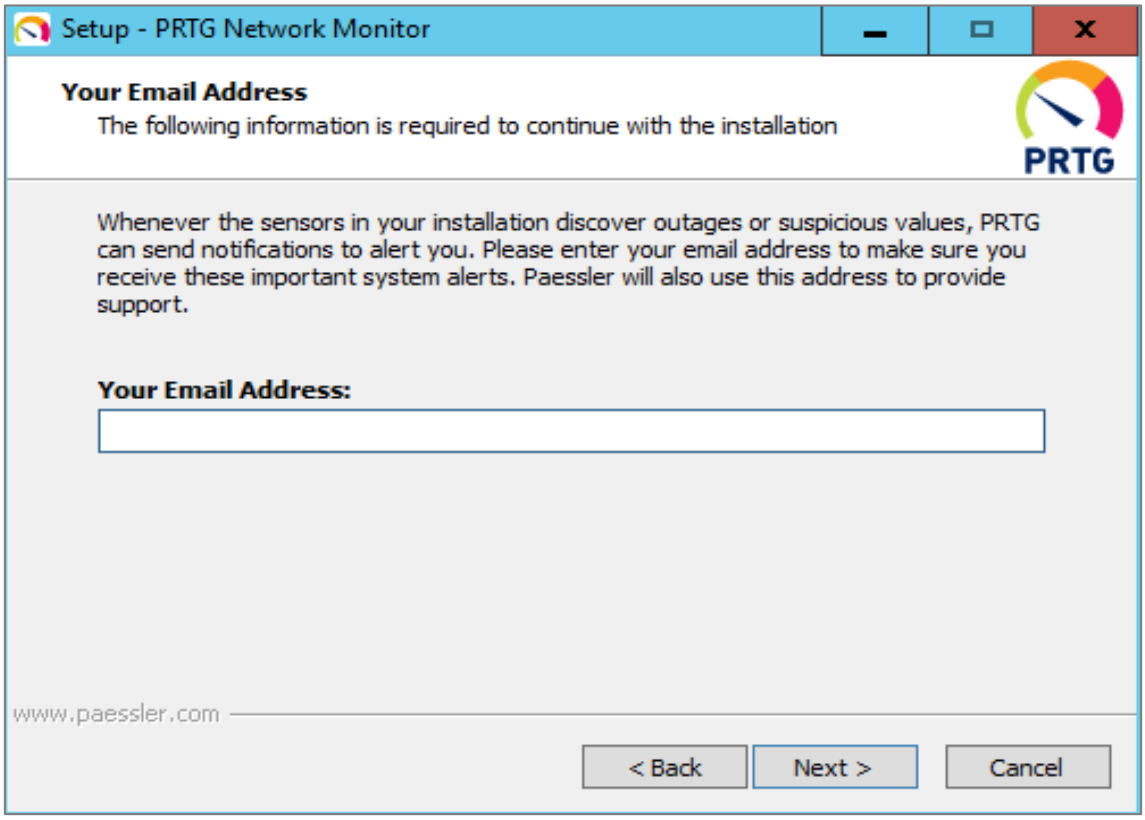
1. Ejecutar el instalador de PRTG como administrador



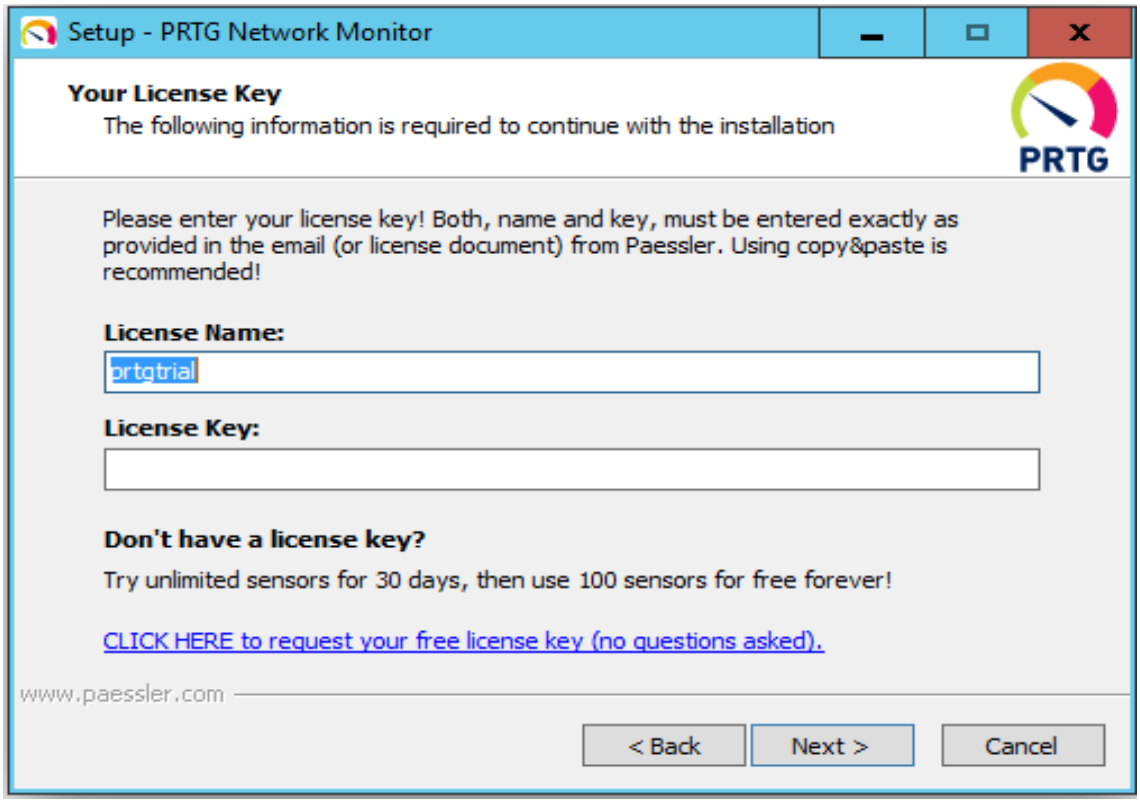
2. Aceptar los términos de la licencia para seguir con la instalación



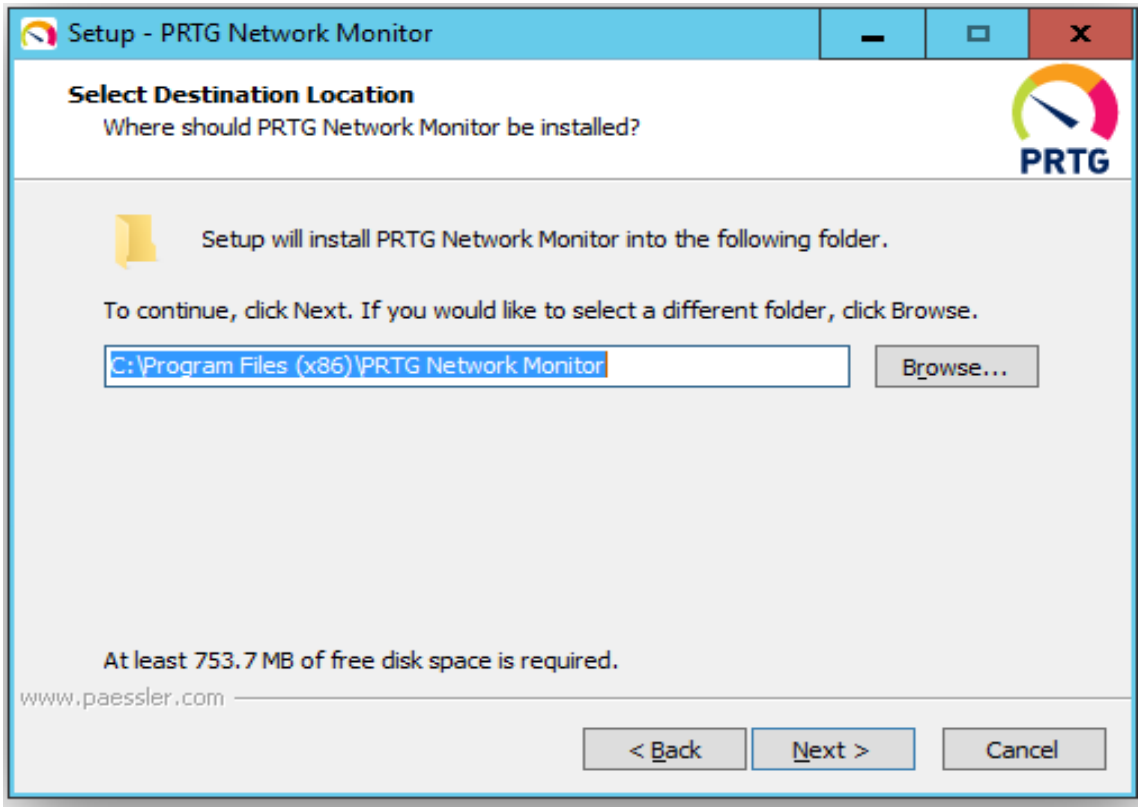
3. Ingresar su correo electrónico



4. Ingresar el serial que se obtiene desde la página al momento de la descarga



5. Escoger la ruta de la instalación o dejar la ruta por defecto



ANEXO 3D: INSTALACIÓN DE PANDORA FMS

Pandora FMS es una solución de código abierto y comercial desarrollada por la compañía española Ártica ST que sirve para monitorizar y facilitar la gestión de la infraestructura de TI. Permite conocer el estado de los componentes de un dispositivo y de los diferentes servicios implementados en una organización, dispone de un histórico de datos y eventos que facilitan a los administradores prevenir fallos y brindar soluciones oportunas para las eventualidades que se presenten. A continuación se detalla el proceso de instalación de Pandora FMS sobre Ubuntu server 16.04 (Pandora FMS, 2019).

1. Antes de instalar Pandora FMS se debe actualizar el sistema, instalar e inicializar mysql-server

```
# apt-get update
# apt-get install mysql-server (configurar en el proceso de instalación)
# systemctl start mysql-server o (etc/init.d/mysqld start)
```

2. Instalación de Pandora FMS

```
# apt-get install pandorafms-console pandorafms-server
```

3. En el caso de que falten complementos o se desee realizar la instalación manual se deben instalar los siguientes paquetes

```
# apt-get install snmp snmpd libtime-format-perl libxml-simple-perl libxml-twig-perl libdbi-perl libnetaddr-ip-perl libhtml-parser-perl wmi-client xprobe2 nmap libmail-sendmail-perl traceroute libio-socket-inet6-perl libhtml-tree-perl libsnmp-perl snmp-mibs-downloader libio-socket-multicast-perl libsnmp-perl libjson-perl libencode-locale-perl php5 libapache2-mod-php5 apache2 mysql-server php5-gd php5-mysql php-pear php5-snmp php-db php-gettext graphviz mysql-client php5-curl hp5-xmlrpc php5-ldap dbconfig-common
```

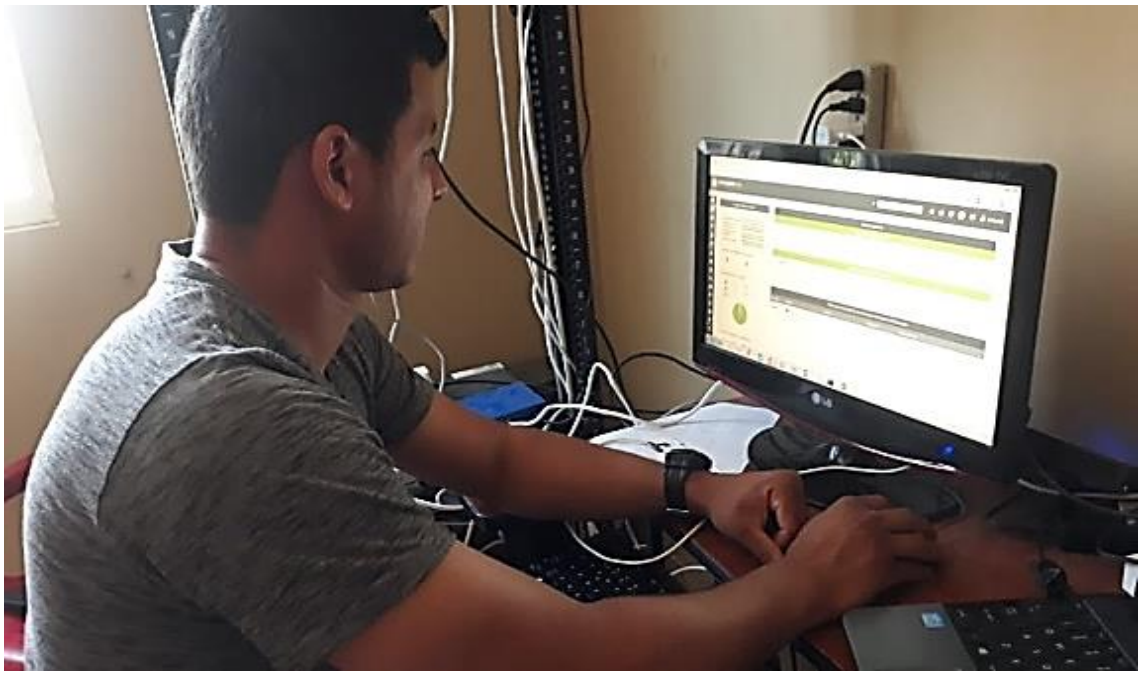
4. Para versiones de Pandora FMS 729 o superior, será necesario instalar las dependencias de PHP 7 para un correcto funcionamiento de la consola
5. Por último, acceder a http://ip_servidor/pandora_console/ para administrar la herramienta, en caso de presentar algún error en la autenticación del servicio es necesario modificar el usuario y contraseña de la base de datos en el archivo que correspondiente.

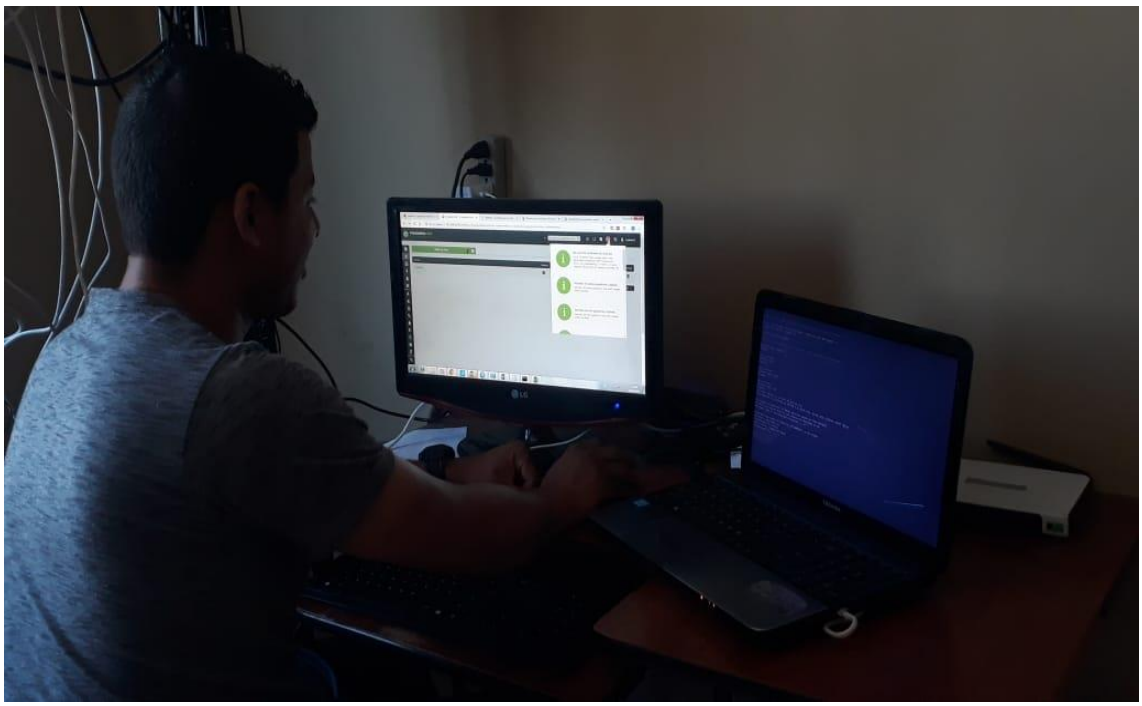
ANEXO 4

EVALUACIÓN DE LAS HERRAMIENTAS DE MONITOREO DE RED DE COMPUTADORAS EN LA EMPRESA PUERTO ATÚN

ACTIVIDADES

- Ejecutar cada una de la herramientas a monitorizar
- Dejar todas las herramientas detectando falencias en la red
- Analizar los resultados de cada sistema de monitoreo
- Raquear las herramientas por los resultados obtenidos





ANEXO 5

PLAN DE MEJORAS PARA LA OPTIMIZACIÓN DE MONITOREO DE RED DE COMPUTADORAS EN LA EMPRESA PUERTO ATÚN

PLAN DE MEJORAS PARA LA OPTIMIZACIÓN DE LA RED DE DATOS EN LA EMPRESA PUERTO ATÚN BASADA EN HERRAMIENTAS DE MONITOREO

JULIO 2019

CONTENIDO

CONTENIDO DE CUADROS Y FIGURAS

1. INTRODUCCIÓN

El propósito del presente plan es proveer mejoras en cuento al rendimiento de la infraestructura de red en la empresa Puerto Atún del cantón Jaramijó, que por medio de una comparativa de herramientas de monitoreo se describe una solución tecnológica para controlar los servicios y las actividades importantes que se llevan a cabo según los procesos y sus estados en tiempo real, de manera que se determine una serie de alternativas de funciones en cuanto a la prioridad a las estrategias de monitoreo que se desee aplicar en el entorno de TI.

Dado que, al determinar las herramientas de monitoreo se pudo llegar a la selección de la mejor y que por la categorización fue la elegida para brindar la optimización, control y seguimiento al análisis consecutivo de la red.

De esta manera, se pueden prevenir fallas, amenazas o componentes defectuosos a futuro dentro de la red, que provocaría inconveniente en la comunicación de los servicios, sistemas, enlaces inalámbricos y dispositivos en la red, y con ello mantener la disponibilidad, seguridad y la confidencialidad en la empresa.

2. ALCANCE

Este plan es aplicable solo para la empresa objeto de investigación, debido que solo el estudio de monitoreo se hizo con los puntos o nodos conectados a la red, en este caso fueron aproximadamente 65 nodos. Solo se implementará una solución de monitoreo, Nagios Core, debido a que si se implementan más herramientas puede causar una sobrecarga en los equipos, consumo de más recursos y se perdería la disponibilidad de los servicios. Este plan solo propone realizar el monitoreo de la red más no del mantenimiento de la misma.

3. OBJETIVOS

1.1. OBJETIVO GENERAL

Diseñar un plan de mejoras que permita la optimación de los procesos de control de red de datos mediante herramientas de monitoreo en la Empresa Puerto Atún.

1.2. OBJETIVOS ESPECÍFICOS

- Definir la herramienta de monitoreo de red de computadoras.
- Monitorizar la red de computadoras mediante la herramienta seleccionada.
- Proporcionar acciones de mejoras mediante el análisis de los resultados obtenidos del monitoreo de la red de computadoras.

4. GLOSARIO DE TÉRMINOS

CÓDIGO ABIERTO: Se refiere a cualquier programa cuyo código fuente se pone a disposición para su uso o modificación, conforme los usuarios u otros desarrolladores lo consideren conveniente (Margaret, 2019).

CONTROL: Es el mecanismo que en función de la identificación ya autentificada permite acceder a datos o recursos en dominio, mando y preponderancia, o a la regulación sobre un sistema (TECNOSeguro, 2019).

DISPONIBILIDAD: Es el acceso de personas u organismos a diversos datos, mediante mecanismos seguros y sencillos, que garanticen los procesos que información de una empresa (Asper, 2015).

ESTRATEGIA DE MONITOREO: Según el autor es una propuesta que indica una serie de acciones de mejoras que conlleva a la mitigación de problemas defectuosos o lentos en el control de la red para dar solución a nivel empresarial.

EVALUACIÓN: Es la acción y consecuencia de evaluar el rendimiento y los eventos producidos en una red de datos.

EVENTOS: Es un proceso que se enfoca a la gestión de la seguridad que busca proporcionar una visión de seguridad de la tecnología de la información (TI) de una organización (Rouse, 2019).

FACILIDAD DE USO: Es aquella que hace referencia a la forma la aplicación debe ofrecer una interfaz adecuada al usuario (CarlosPes, 2019).

GESTIÓN: Se refiere a las diligencias que permiten la realización de cualquier actividad o proceso dentro una situación o administración de una empresa (Bautista, 2019).

HERRAMIENTAS DE MONITOREO: Son sistemas de diagnóstico para telecomunicaciones, servidores o redes que buscan componentes defectuosos o lentos, con el fin de informar a los administradores mediante correo electrónico, sms, entre otros (Nagios, 2016).

IMPREVISTOS: Es aquel que no fue previsto: es decir, que no pudo ser visto, detectado o conocido con anticipación en una red (Pérez, 2019).

INFRAESTRUCTURA DE RED: Es el medio proporcionado por las redes cableada e inalámbrica para efectuar comunicaciones y equipamiento dentro de una empresa (Sevilla, s.f.).

NAGIOS: Es aquel que proporciona monitoreo de todos los componentes de infraestructura de misión crítica, incluidas aplicaciones, servicios, sistemas operativos, protocolos de red, métricas de sistemas e infraestructura de red (Nagios, 2019).

OPENNMS: Es una plataforma de código abierto altamente integrada, de nivel de operador, diseñada para crear soluciones de monitoreo de red (OpenNMS, 2017).

OPSVIEW: Se encarga del monitoreo de sistemas empresariales para infraestructuras de TI físicas, virtuales y basadas en la nube (Opsview, 2019).

PANDORA FMS: Es un software de monitorización para gestión de infraestructura TI. Esto incluye equipamiento de red, servidores Windows y Unix, infraestructura virtualizada y todo tipo de aplicaciones (FMS, 2018).

PARAMENTOS DE SEGURIDAD: Son los Elementos que conforman una serie de aspectos de seguridad en la infraestructura de red.

RECUPERACIÓN: Es el proceso por el cual se estable la acción de recuperar la información que ha sido afectada o dañada en una empresa.

PRTG: Es un software de monitorización de red, que analiza procesos continuamente en la red, realiza informes y alerta al personal IT en el momento en el que se produce un error o los valores críticos se sobrepasan, es altamente recomendable con el fin de garantizar disponibilidad, rendimiento y correcto uso (PRTG, 2019)

PUERTO ATÚN: Es una empresa que se encarga del desarrollo de la actividad productiva en el sector pesquero, que brinda mejorar la calidad en la comercialización y procesamiento atunero en la Provincia de Manabí.

RED DE DATOS: Un conjunto de equipos y dispositivos que están conectados entre sí, y comparten recursos, información, y servicios (Coria, 2019).

RENDIMIENTO: Es aquel que refiere a la proporción que surge entre los medios empleados para obtener algo y el resultado que se consigue de manera continua y favorable (Pérez, 2019).

REQUISITOS DEL SISTEMA: Es una necesidad documentada sobre el contenido, forma o funcionalidad de un producto o servicio en el área de TI(Anda, s.f.).

SOLUCIONES DE SOFTWARE LIBRE: Son considerados alternativas de solución, las cuales código abierto, en el cual la libertad de los usuarios de ejecutar, copiar, distribuir, estudiar, cambiar y mejorar el software se aplica en casos sistematización de procesos (Ecured, s.f.).

SOPORTE INFORMÁTICO: Es el servicio mediante el cual los especialistas en apoyo informático proporcionan asistencia técnica, soporte remoto y

asesoramiento a individuos y organizaciones que dependen de la tecnología de la información (Mikogo, s.f.).

ZABBIX: es un Sistema de Monitorización de Redes creado por Alexei Vladishev. Está diseñado para monitorizar y registrar el estado de varios servicios de red, Servidores, y hardware de red (Zabbix, 2013).

ZENOSS: Es un producto de código abierto de monitorización que proporciona las funcionalidades necesarias para gestionar eficazmente la configuración, la estabilidad, el rendimiento de las redes, servidores y aplicaciones a través de un único paquete de software integrado (ZENOSS, 2017).

5. MONITOREO DE RED Y SU APLICABILIDAD EN LA EMPRESA PUERTO ATÚN

La dependencia de contar con una infraestructura computacional en las empresas modernas conlleva un intrínseco control sobre dicha infraestructura, en el trabajo de Tobar (2015) se define como sistema de monitorización y gestión de redes al conjunto de sistemas, normativas y protocolos de gestión que facilitan las actividades de monitoreo y mantenimiento de la red.

De acuerdo a lo antes mencionado, este monitoreo es aplicable a la empresa objeto de estudio, debido a que la organización maneja grandes cantidades de información y es necesario que se adapte una guía para el control de la red y de esta forma mantener la disponibilidad 24/7 de los servicios. Además, la herramienta sugerida para llevar este control de monitoreo y hacer posible la optimización de la red, tiene las mejores características de acuerdo a la evaluación hecha por el autor de esta investigación, lo que amerita que será de gran beneficio implementar este plan.

6. COMPONENTES GENERALES PARA EL MONITOREO DE COMPUTADORAS

Para la optimización de la red mediante herramientas de monitoreo, se utilizaron los siguientes componentes con características mínimas para hacer un buen control de la red:
Como requisito principal es necesario tener un servidor físico.

Hardware

- Computador INTEL
- Procesador Core 7
- Memoria RAM de 8GB
- Almacenamiento de 1TB
- Sistema de 64 bits.

Software

Sistema Operativo Linux

Herramienta de Monitoreo

Nagios Core 4.4.3 (gratuita)

7. SELECCIÓN Y CATEGORIZACIÓN DE HERRAMIENTAS PARA MONITOREO

En el cuadro 1 se realizó la comparativa entre varias herramientas de monitoreo de redes de computadoras considerando las soluciones de software libre en su mayoría, ya que en ocasiones las empresas no dan la importancia que merece el monitoreo de su infraestructura tecnológica, aun así se consideró para esta comparativa la versión shareware del sistema PRTG teniendo en cuenta que es uno de los más populares en el mercado y que el tiempo que está activa la prueba brinda casi todas sus funcionalidades.

Cuadro 1. Comparativa de herramientas de monitoreo de red de computadoras

HERRAMIENTAS / CARACTERÍSTICAS	NAGIOS	ZABBIX	PANDORA FMS	PRTG NETWORK MONITOR	OPENNMS	OPSVIEW	ZENOSS
Monitoreo de red	X	X	X	X	X	X	X
Monitoreo en la nube	X	X	X	X		X	
Monitoreo de aplicaciones	X	X	X	X		X	X
Monitoreo de servidores	X	X	X	X	X	X	X
Monitoreo web o remoto	X	X	X	X			
Dispositivos de almacenamiento	X	X	X				
Monitoreo de máquinas virtuales	X	X	X	X	X	X	X
Aplicaciones java		X			X		
Monitoreo de bases de datos	X	X	X	X	X	X	X
KPI/SLA		X	X				
Telefonía	X	X	X	X	X	X	X
Monitoreo de seguridad	X	X		X	X	X	
Temperatura de un servidor	X	X	X	X	X	X	X
Temperatura de un sistema	X	X	X	X	X	X	X
Monitoreo de sistema operativo	X	X	X	X	X	X	X
Herramienta tolerante a fallos (servidor de respaldo)				X			
Monitoreo de rendimiento de un computador	X					X	
Monitoreo de correo electrónico	X	X	X	X	X	X	X
Linux	X	X	X		X	X	X
Windows	X		X	X	X	X	

Fuente: El autor

Para efectuar la categorización de las herramientas de monitoreo de redes, se estableció una serie de parámetros que permitan valorar cada una de las soluciones implementadas y que para la evaluación fueron los siguientes:

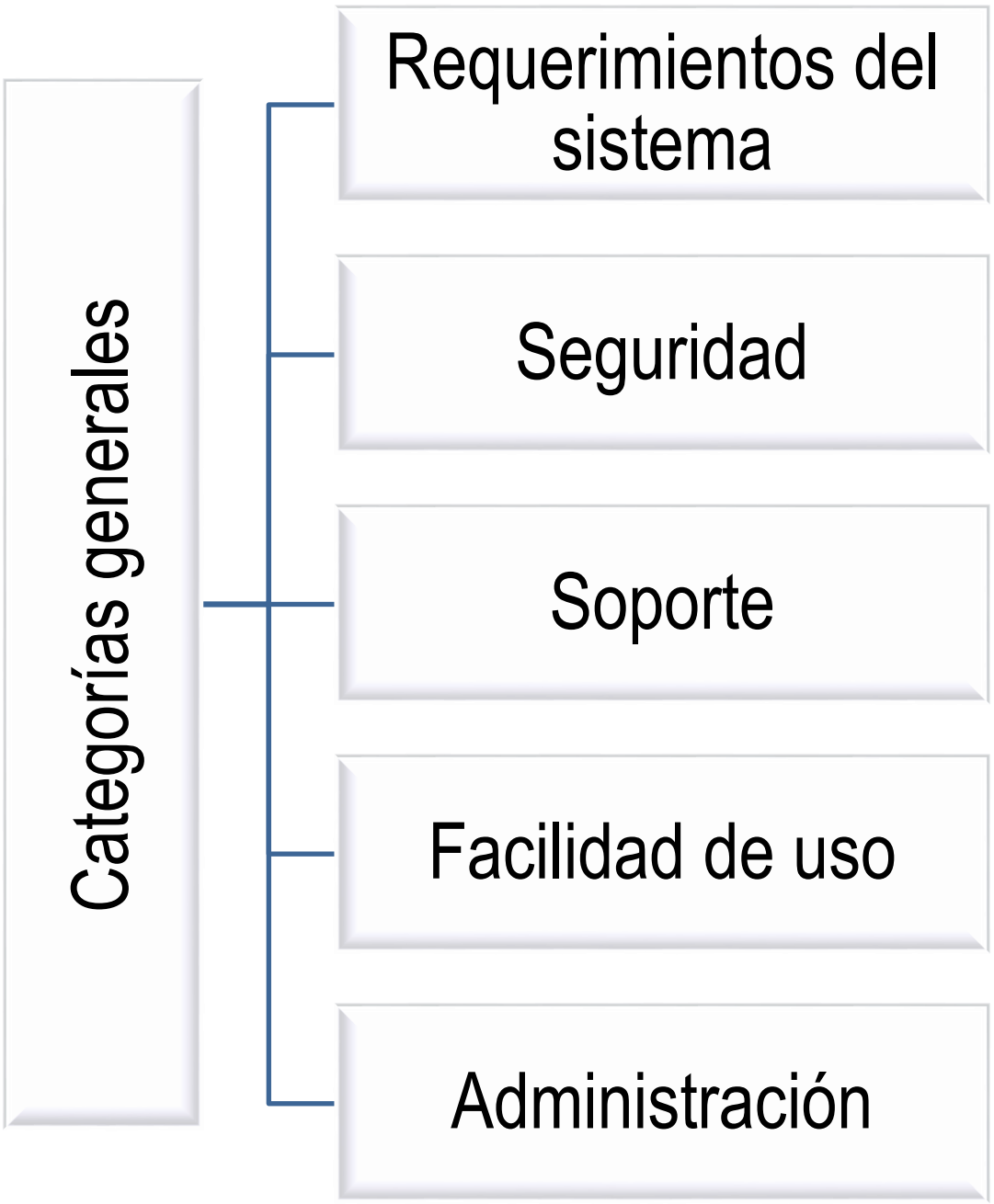


Figura 1. Categorías Generales de las herramientas de monitoreo de red

Fuente: El autor

8. PROCESOS Y PROCEDIMIENTOS

A continuación se da a conocer los procesos y procedimientos aplicados para el monitoreo de red de datos para la empresa Puerto Atún del Cantón Jaramijó, detallada a continuación:

Cuadro 2. Descripción de los procesos y procedimientos

PROCESOS	PROCEDIMIENTOS
Análisis de requerimientos	Se identifica los procesos que conlleva la infraestructura de red
	Se define un inventario de las redes de computadoras en la empresa (solo las activas).
Planteamiento de estrategias de monitoreo	Se establecen estrategias de monitoreo para determinar la topología de la red, la cantidad de routers, switches, puntos de acceso inalámbricos y demás dispositivos tecnológicos que conforman la red.
Determinación e implementación de herramientas para el monitoreo de redes de computadoras	Se elige sistemas de monitoreo de redes de computadoras.
	Se implementan las herramientas de monitoreo de red.
	Se determina los roles en un sistema de monitoreo de una infraestructura de TI.
	Se categoriza las herramientas a partir de paramentos valorados en soluciones de análisis.
	Se elige la herramienta más óptima, eficiente y eficaz.
	Se generan reportes del estado de la infraestructura de la red en tiempo real.
Análisis de monitoreo	Se identifican las actividades en cuanto al rendimiento de la red o del funcionamiento de los servicios.
	Se establecen los mecanismos de control para la protección de los datos y mejorar el rendimiento de la red.
Acciones de mejora	Se planea acciones de mejora para brindar soluciones ante los eventos registrados en los análisis del rendimiento de la infraestructura tecnológica.

Fuente: El autor

9. ENTORNO DE PRÁCTICA

9.1. MEDIDAS Y CONTROLES

Para la puesta en marcha del entorno de práctica, se efectúan las siguientes medidas:

- Nivel de usabilidad
- Nivel de implementación.
- Indicador de estado de monitoreo.
- Dimensión de la herramienta.
- Comunicación de notificaciones a través de correo electrónico

Y por otro lado los controles que se consideran son:

- Revisión de monitoreo activo
- Aplicación de técnicas de monitoreo activo
- Definición de métricas en el monitoreo activo
- Priorización las revisiones según el estado de los eventos dentro de la red.
- Efectuar mantenimientos correctivos y preventivos en los problemas suscitados dentro de la infraestructura de red.
- Brindar soluciones de mejoras en la red de datos.

9.2. VALIDACIÓN Y ADAPTACIÓN

Para llevar a cabo esta sección, se tienen que considerar que las herramientas de monitoreo a utilizar sean óptimas y que realicen sus procesos eficiente y eficazmente en el control de monitoreo de red de datos, de manera que sean adaptables en la infraestructura de red y permitan arrojar datos relevantes del análisis de monitoreo, y así apoyar en las funciones de gestión y rendimiento que se lleven a cabo en los procesos de la empresa, de manera que si existan problemas se puedan conocer y efectuar soluciones de mitigación, proponer mejoras proactivas y mantener una correcta toma de decisiones.

10. ANÁLISIS DE MONITOREO

En el siguiente cuadro se muestra la comparativa de las soluciones que se implementaron y se categorizaron en 5 aspectos generales (Requerimientos del sistema, Seguridad, Soporte, Facilidad de uso y Administración), cada una de ellas obtuvo un resultado de acuerdo a la asignación de 3 posibles valores según el nivel de cumplimiento de cada característica. Se le asigna el valor de 1 al parámetro que se cumpla totalmente, el valor de 0.5 es asignado a las características que se cumplan a medias y el valor de 0 para los parámetros que no se cumplen. Adicionalmente se agregaron medidas cualitativas que consideró importante el autor de este trabajo en este proceso de desarrollo. También, estos datos fueron obtenidos luego de implementar cada una de las soluciones y dejarlas en ejecución durante 5 días.

Cuadro 3. Análisis comparativo de las herramientas de monitoreo de la red por categorías

HERRAMIENTAS / CARACTERÍSTICAS	ZABBIX 4.0	PRTG NETWORK MONITOR 19.1.48.239	NAGIOS CORE 4.4.3	PANDORA FMS 7.0 NG 732
REQUERIMIENTOS DEL SISTEMA (5)	**4**	**2.5**	**4.5**	**4**
Dificultad de instalación	**Baja (1)**	**Baja (1)**	**Media (0.5)**	**Media (0.5)**
Instalación en Linux	**1**	**0**	**1**	**1**
Instalación en Windows	**0**	**1**	**1**	**1**
Licencias	**1**	**0.5**	**1**	**1**
Bases de datos	**1**	**0**	**1**	**0.5**
SEGURIDAD (5)	**2**	**2**	**2**	**3.5**
Control de versión	**0.5**	**0.5**	**0.5**	**0.5**
Seguimiento de auditoria	**0**	**0**	**0**	**0**
Gestión de sesiones	**0**	**0**	**0**	**1**
Verificación de correo electrónico	**1**	**1**	**1**	**1**
Acceso remoto	**0.5**	**0.5**	**0.5**	**1**

SOPORTE (6)	**4.5**	**3**	**4.5**	**3.5**
Soporte comercial	**1**	**1**	**0.5**	**0.5**
Foro público	**1**	**0**	**1**	**0**
Manuales comerciales	**0.5**	**0**	**0.5**	**0.5**
Ayuda en línea	**0.5**	**1**	**1**	**1**
Desarrollo de terceros	**0.5**	**0**	**1**	**1**
Aprendizaje comercial	**1**	**1**	**0.5**	**0.5**
FACILIDAD DE USO (8)	**7.5**	**7.5**	**7**	**7.5**
Auto descubrimiento	**1**	**1**	**0.5**	**1**
Perfiles de usuario	**1**	**1**	**1**	**1**
Gráficas	**1**	**1**	**1**	**1**
Informes	**1**	**1**	**1**	**1**
Mapas	**0.5**	**0.5**	**1**	**0.5**
Aplicación web	**1**	**1**	**1**	**1**
Informar cumplimiento SLA´s	**1**	**1**	**1**	**1**
Complejidad para administrar nodos	**Baja (1)**	**Baja (1)**	**Media (0.5)**	**Baja (1)**
ADMINISTRACIÓN (14)	**10**	**11**	**14**	**10,5**
SNMP	**1**	**1**	**1**	**1**
Plugins o sensores	**0.5**	**1**	**1**	**0.5**
Estadísticas	**1**	**1**	**1**	**1**
Soporte para IPv6	**1**	**1**	**1**	**1**
Aplicación móvil	**1**	**1**	**1**	**1**
Alertas	**1**	**1**	**1**	**1**
Notificaciones vía mail	**1**	**1**	**1**	**1**
Notificaciones vía sms	**1**	**1**	**1**	**1**
Notificaciones por mensajería instantánea	**0**	**0**	**1**	**0**

Mapas	**0.5**	**1**	**1**	**1**
Monitorización distribuida	1	1	1	1
Scripts externos	**0**	**0**	**1**	**0**
Creación de complementos	**0**	**0**	**1**	**0**
Registro de Logs	**1**	**1**	**1**	**1**

Fuente: El autor

Según el análisis comparativo de las soluciones de monitoreo de red se puede determinar que hay 2 soluciones (Zabbix y Nagios) con un puntaje alto, y de acuerdo a estos datos solo una solución se recomienda para implementar en la empresa, la cual es Nagios, debido a que cumple con las mejores características de funcionalidad para el monitoreo de red.

11. ESTRATEGIA DE MONITOREO

Para llevar a cabo estrategias de monitoreo óptimas para la infraestructura de red, se indican las más necesarias a considerar:

- Tener una buena utilización de ancho de banda
- Consumo de CPU.
- Consumo de memoria.
- Estado físico de las conexiones.
- Tipo de tráfico.
- Alarmas para garantizar el buen funcionamiento de los dispositivos de red.
- Servicios (Web, correo, bases de datos, proxy, servidores, entre otros).
- Efectuar enfoques de monitoreo.
- Seleccionar las herramientas y dispositivos a emplear dentro de la red**.**
- Medir el rendimiento o caracterizar y/o contabilizar el uso de la red**.**
- Mantener la función de disponibilidad 24/7 en la empresa.
- Realizar priorización en los procesos de monitoreo.
- Analizar los eventos en el monitoreo en secuencias de tiempo.
- Efectuar mejoras ante problemas suscitados en la infraestructura de red, para su solución correctiva y preventiva.

12. RESPONSABLES

El responsable asignado para implementar este plan será el director/coordinador del área de sistemas de la empresa Puerto Atún, este a su vez asignará a las personas a su cargo en el cuarto de control para llevar a cabo con las consideraciones planteadas en esta guía de implementación.

13. CONCLUSIONES Y RECOMENDACIONES

13.1. CONCLUSIONES

- La empresa cuenta con el hardware y software necesario para la implementación de la herramienta de monitoreo y de esta manera conseguir la optimización de los recursos de la red. La topología de la red permite la distribución de la red de una manera más eficiente.

- La herramienta Nagios de acuerdo a sus características de requerimiento de sistema, seguridad, soporte, facilidad de uso y administración es la más recomendable para la implementación, y también esta no presenta tantos eventos como las demás herramientas evaluadas.

13.2. RECOMENDACIONES

- A la empresa se sugiere comprar UPS para el almacenamiento de energía cuando se va la electricidad, sobre todo en el área del sistema de vigilancia para un mayor control de la empresa.
- Además, en caso de querer implementar otra herramienta para uso específico de monitoreo como las antenas marca UBIQUITI, se recomienda adoptar Zabbix porque permite ver el estado en tiempo real de los equipos instalados en ellas.

BIBLIOGRAFÍA

Anda, L. (s.f.). Especificación de Requisitos del Sistema. Disponible en: http://www.juntadeandalucia.es/servicios/madeja/contenido/recurso/407

Asper. (2015). ¿Qué es la disponibilidad informática? Disponible: https://blog.apser.es/2015/08/19/que-es-la-disponibilidad-informatica-y-cual-es-su-importancia

Bautista, E. (2019). Definición de Gestión. Disponible en: https://conceptodefinicion.de/gestion/

CarlosPes. (2019). Facilidad de Uso. Obtenido de Facilidad de Uso: http://www.carlospes.com/minidiccionario/facilidad_de_uso.php

Coria, D. (2019). RED DE DATOS. Disponible en: https://davidcoriablog.wordpress.com/2012/11/22/definicion-de-red-de-datos/

Ecured. (s.f.). Software libre. Disponible en: https://www.ecured.cu/Software_libre

FMS, P. (2018). ¿Qué es Pandora FMS? Disponible en: http://pandorafms.org/es/

Margaret, R. (2019). Fuente abierta o código abierto (open source). Disponible en: https://searchdatacenter.techtarget.com/es/definicion/Fuente-abierta-o-codigo-abierto-open-source

Mikogo. (s.f.). ¿Qué es el soporte informatico? Disponible en: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=2ahUKEwj8lN3_i9DhAhUMtlkKHVBNCmUQFjABegQIDBAE&url=https%3A%2F%2Fwww.mikogo.es%2Fguia%2Fsoporte-informatico%2F&usg=AOvVaw3nSRVmDze18PvDgBWTqAWB

Nagios. (2016). Herramientas de Monitoreo. Disponible en: https://www.greencore.co.cr/herramientas-de-monitoreo.html

Nagios. (2019). What can Nagios help you do? Disponible en: https://www.nagios.com

OpenNMS. (2017). OpenNMS . Disponible en: https://www.opennms.org/en

Opsview. (2019). Cloud and Infrastructure Monitoring Software and Tools. Disponible en: https://www.opsview.com

Pérez, J. (2019). RENDIMIENTO. Disponible en: https://definicion.de/rendimiento/

Pérez, J. (2019). IMPREVISTO. Disponible en: https://definicion.de/imprevisto/

PRTG. (2019). Monitoriza tu Red con Paessler PRTG. Disponible en: https://www.danysoft.com/paessler-prtg/

Rouse, M. (2019). Gestión de eventos e información de seguridad (SIEM). Disponible en: https://searchdatacenter.techtarget.com/es/definicion/Gestion-de-eventos-e-informacion-de-seguridad-SIEM

Sevilla, U. d. (s.f.). Estudios de Infraestructura de Red. Disponible en: https://sic.us.es/servicios/infraestructuras-comunicaciones-hw-y-sw/estudios-de-infraestructura-de-red

TECNOSeguro. (2019). Control de un Sistema. Disponible en: https://www.tecnoseguro.com/faqs/control-de-acceso/que-es-un-control-de-acceso

Tobar, G. A. (2015). Implementación de un sistema de monitoreo de los niveles de servicio acordados por los proveedores de servicio de Internet para la Superintendencia de Telecomunicaciones . Quito: EPN.

Zabbix. (2013). ¿Que es Zabbix? Disponible en: http://911-ubuntu.weebly.com/zabbix_como_funciona/conoce-la-estructura-de-zabbix-y-como-usarlo

ZENOSS. (2017). ¿QUÉ ES ZENOSS? Disponible en: http://conocimientosasir.blogspot.com/2017/06/monitorizacion-de-una-red-con-zenoss.html

ANEXOS

ANEXO 1

INSTALACIÓN DE NAGIOS CORE

NAGIOS CORE 4.4.3

Nagios Core es un sistema de monitorización de redes ampliamente utilizado, de código abierto, que se encarga de controlar los equipos y servicios que se especifican, alertando cuando el comportamiento de los mismos no sea el adecuado. Además, sirve como un programador de eventos básico, procesa dichos eventos y administra las alertas que se producen en los elementos monitorizados, cuenta con varias API's que se utilizan para ampliar sus capacidades para realizar tareas adicionales (Nagios Core, 2019).

1. Desabilitar SELINUX modificando el archivo /etc/selinux/config

SELINUX=enforcing (para aplicar los cambios hay que reiniciar el sistema)

2. Es necesario habilitar los puertos del servicio web y reiniciar el firewall

```
# firewall-cmd --permanent –add-port=80/tcp
# firewall-cmd --permanent –add-port=443/tcp
# firewall-cmd --reload
```

3. Instalar las dependencias necesarias para instalar Nagios

```
# yum install –y gettext wget net-snmp-utils openssl-devel glibc-common unzip perl epel-release gcc php gd automake autoconf httpd make glibc gd-devel net-snmp perl-Net-SNMP
```

4. Agregar el usuario Nagios

```
# useradd Nagios
```

5. Agregar como grupo secundario Nagios al usuario apache

```
# usermod –a –G nagios apache
```

6. Descargamos Nagios desde github con wget

```
# https://github.com/NagioEnterprises/nagioscore/releases (de esta url copiar el enlace de [nagios-4.4.2.tar.gz])

# wget https://github.com/NagioEnterprises/nagioscore/releases/download/nagios-4.4.2/nagios-4.4.2.tar.gz (este es el enlace copiado del punto anterior)
```

7. Descomprimir el archivo descargado de Nagios

```
# tar -xzvf nagios-4.4.2tar.gz
```

8. Ingresar a la carpeta descomprimida, para luego compilar e instalar Nagios

```
# cd nagios-4.4.2

# ./configure

# make all

# make install

# make install-init

# make installcomand-mode

# make install-config

# make install-webconfig
```

9. Habilitar el servicio de Nagios para que cargue al iniciar el sistema

```
# systemctl enable nagios (crea un enlace simbólico)
```

10. Habilitar el servicio de apache para que cargue al iniciar el sistema

```
# systemctl enable httpd (crea un enlace simbólico)
```

11. Configurar parámetros de seguridad de httpd para usuarios específicos

```
# htpasswd –c /usr/local/nagios/etc/htpasswd.users nagiosadmin
Password: 'Aquí ingresa el password'
```

12. Iniciar y comprobar los servicios

```
# systemctl start httpd
# systemctl start nagios
# systemctl status httpd
# systemctl status hnagios
```

13. Acceder a Nagios con la url: http://ip_address_servidor/nagios y acceder con los datos de seguridad para httpd que fueron configurados anteriormente