CIENCIAMATRIA
Revista Interdisciplinaria de Humanidades, Educación, Ciencia y Tecnología
Año VIII. Vol. VIII. Nro. 4. Edición Especial 4. 2022
Hecho el depósito de ley: FA2021000002
ISSN-L: 2542-3029; ISSN: 2610-802X
Instituto de Investigación y Estudios Avanzados Koinonía (IIEAK). Santa Ana de Coro. Venezuela

https://doi.org/10.35381/cm.v8i4.1053

Evaluación de herramientas de monitoreo para mejorar la seguridad de la red de datos

Evaluation of monitoring tools to improve the security of the data network

Milton Luyely Intriago-Cedeño
milton.Intriago@utm.edu.ec
Universidad Técnica de Manabí, Portoviejo, Manabí
Ecuador
https://orcid.org/0009-0009-2864-133X

Freddy Andrés Carrera-Sánchez
freddy.carrera@utm.edu.ec
Universidad Técnica de Manabí, Portoviejo, Manabí
Ecuador
https://orcid.org/0000-0003-3232-0853

Eduardo Morejón-López
gabriel.mmorejon@utm.edu.ec
Universidad Técnica de Manabí, Portoviejo, Manabí
Ecuador
https://orcid.org/0000-0001-8902-4583

Josselyn Stefanía Pita-Valencia
josselyn.pita@utm.edu.ec
Universidad Técnica de Manabí, Portoviejo, Manabí
Ecuador
https://orcid.org/0000-0003-1081-5652

Recibido: 15 de agosto 2022
Revisado: 01 de octubre 2022
Aprobado: 15 de noviembre 2022
Publicado: 01 de diciembre 2022

CIENCIAMATRIA
Revista Interdisciplinaria de Humanidades, Educación, Ciencia y Tecnología
Año VIII. Vol. VIII. Nro. 4. Edición Especial 4. 2022
Hecho el depósito de ley: FA2021000002
ISSN-L: 2542-3029; ISSN: 2610-802X
Instituto de Investigación y Estudios Avanzados Koinonía (IIEAK). Santa Ana de Coro. Venezuela

Milton Luyely Intriago-Cedeño; Freddy Andrés Carrera-Sánchez; Eduardo Morejón-López;
Josselyn Stefanía Pita-Valencia

RESUMEN

El objetivo general de la presente investigación fue evaluar las herramientas de monitoreo para mejorar la seguridad de la red de datos. Se fundamentó en el paradigma positivista, desde la perspectiva cuantitativa, desde una tipología documental-bibliográfica, apoyada en los métodos comparativo referente a la funcionalidad y adaptabilidad de varios sistemas de monitoreo de redes para su posterior aplicación, los mismos que guardan relación para lograr los objetivos. Se desarrolló a través de la metodología PPDIOO que incluye las fases de, Preparar, Planificar, Diseñar, Implementar, Operar y Optimizar. Se concluye que, 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.

Descriptores: Red de información; seguridad de los datos; información y comunicación. (Tesauro UNESCO).

ABSTRACT

The general objective of this research was to evaluate monitoring tools to improve data network security. It was based on the positivist paradigm, from the quantitative perspective, from a documentary-bibliographic typology, supported by comparative methods relating to the functionality and adaptability of various network monitoring systems for subsequent application, the same that are related to achieve the objectives. It was developed through the PPDIOO methodology that includes the phases of Prepare, Plan, Design, Implement, Operate and Optimize. It is concluded that, through the analysis of the results provided by the tools installed, it was possible to identify the activities that cause a degradation in the performance of the network or the operation of the services and, based on this information, control mechanisms are established to protect the data and improve the performance of the network.

Descriptors: Information networking; data security; information and communication**.** (UNESCO Thesaurus)

CIENCIAMATRIA
Revista Interdisciplinaria de Humanidades, Educación, Ciencia y Tecnología
Año VIII. Vol. VIII. Nro. 4. Edición Especial 4. 2022
Hecho el depósito de ley: FA2021000002
ISSN-L: 2542-3029; ISSN: 2610-802X
Instituto de Investigación y Estudios Avanzados Koinonía (IIEAK). Santa Ana de Coro. Venezuela

INTRODUCCIÓN

Hoy en día, el incremento de ancho de banda en las empresas aumenta excesivamente y en las mayorías de los casos suelen bridar un servicio pobre en sus redes, son pocos los gerentes de TI que le dan una gran importancia viéndolo como una inversión. El objetivo fundamental es considerar la inversión en herramientas de monitoreo de seguridad informática para minimizar el personal técnico, permitiendo así obtener datos planificados y la generación de alertas que logren identificar los problemas en los dispositivos de la red de forma rápida y sencilla.

El monitoreo de redes de computadoras en las empresas, según a obra de White, analizados por los autores Santiago, y Trabaldo. (2015), hace mención a que el mundo moderno de los negocios no podría funcionar sin la comunicación y las redes de computadoras, por tal motivo 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 gerentes, administrativos, usuarios finales y, cualquier persona que utilice un teléfono inteligente o una computadora. Del mismo modo según Ozkaya y Islam. (2019) ellos consideran el enfoque a 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 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) se define como la función principal de internet 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. (Tse Mundaca,2020). Las hherramientas de monitoreo para redes de

datos, según Pérez Santos. (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 los trabajos de Isaariyapat 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. Existen otros autores que apoyan la implementación de Pandora FMS se mencionan los autores Alava Zambrano, y Guerrero Rodríguez. (2018), quienes catalogan esta aplicación como una herramienta que detecta los problemas físicos en los equipos de la infraestructura, así mismo se 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. Por otro lado, el sistema de monitoreo en una infraestructura de Ti, menciona Quispe Bustincio. (2018), 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. Continua el autor, indicando que 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. 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 Drouet, 2018). 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.(Guevara Aulestia, y Sánchez Cunalata,2017).

De acuerdo, a las ideas planteadas se presenta como objetivo general de la presente investigación evaluar las herramientas de monitoreo para mejorar la seguridad de la red de datos.

MÉTODO

Esta investigación se fundamenta en el paradigma positivista, desde la perspectiva cuantitativa, desde una tipología documental-bibliográfica, apoyada en los métodos comparativo referente a la funcionalidad y adaptabilidad de varios sistemas de monitoreo de redes para su posterior aplicación, los mismos que guardan relación para lograr los objetivos. Se ha desarrollado a través de la metodología PPDIOO que incluye las fases de, Preparar, Planificar, Diseñar, Implementar, Operar y Optimizar.

Preparar, en la elección de las soluciones de monitoreo a evaluar se realizó de manera previa la revisión bibliográfica de diversas fuentes que sustentan la elección de las herramientas. (Junco Romero, & Rabelo Padua,2018). Se definieron 7 herramientas: las mismas que fueron valoradas con parámetros generales, además se tuvo como sustento evaluaciones encontradas en sitios específicos y otros artículos relacionados como indica la tabla 1.

CIENCIAMATRIA
Revista Interdisciplinaria de Humanidades, Educación, Ciencia y Tecnología
Año VIII. Vol. VIII. Nro. 4. Edición Especial 4. 2022
Hecho el depósito de ley: FA2021000002
ISSN-L: 2542-3029; ISSN: 2610-802X
Instituto de Investigación y Estudios Avanzados Koinonía (IIEAK). Santa Ana de Coro. Venezuela

Tabla1.
Definition de herramientas.

Herramienta	Libre	Propietaria
Nagios		X
Zabbix	X	
Pandora fms		X
Prtg network monitor		X
Open nms	X	
Dude	X	
Cacti	X	X

Elaboración: Los autores.

Las herramientas de monitoreo de redes se sustentan su aplicabilidad, y en los niveles de popularidad, características considerando herramientas de software libre. Las mismas que fueron seleccionadas mediante una evaluación de cumplimiento de parámetros y estudios comparativos.

Planificar, para esta fase es necesario definir las herramientas a utilizar, los mecanismos de integración y sincronización a través de la implementación de mecanismos hardware y software, se podrán identificar requerimientos técnicos, cronograma de actividades y ejecución de herramientas de monitoreo Nagios, Zabbix, Pandora FMS, PRTG network monitor, Open NMS, Opsview, Zenoss, Cacti como indica la tabla 2. Se realizó la selección de las herramientas de vigilancia mediante una comparativa entre varias soluciones de monitoreo de redes de computadoras, teniendo en consideración soluciones libres, con la finalidad de minimizar costos debido a que las empresas no dan la importancia al proceso de defensa en profundidad y el monitoreo de su infraestructura tecnológica como se muestra la tabla 2.

Tabla 2.
Herramientas de monitoreo.

Herramientas Características	Nagios	Zabbix	Pandora fms	Prtg network monitor	Opennms	Cacti	Dude
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 javas		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				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: Los autores.

Diseñar, para el cumplimiento de este apartado se identificaron los equipos activos y pasivos que componen la topología de red, con el propósito de plasmar la mejor estrategia se desplego solución óptima, permitiendo así indicar la cantidad de routers, switches, puntos de acceso inalámbricos y demás dispositivos tecnológicos como indica la figura 1.

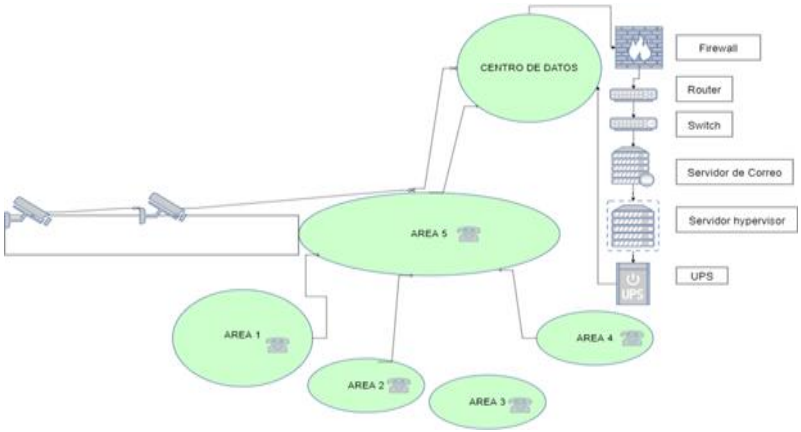

Figura 1. Topología física de la red.
Elaboración: Los autores.

Luego de conocer el entorno; fue necesario definir qué equipos y servicios se iban a monitorizar en la red.

Implementar, después de establecer los parámetros de diseño se procedió con la ejecución del laboratorio de pruebas, la implementación se ejecutó la instalación del sistema de virtualización. Dentro del mismo se configuraron instancias virtuales y físicas para lograr los objetivos, los sistemas operativos y herramientas utilizadas fueron en su mayoría de libre distribución. Para el proceso de implementación es necesario disponer de un equipo hardware con características funcional mínimas. Ver: tabla 3.

Tabla 3.
Equipo.

Detalle	Componente
Cpu	4
Ram	32
Red	1 GB
Monitor	16 Pulgadas

Elaboración: Los autores.

Las herramientas desplegadas para el proceso de análisis se describen la tabla 4, adicionalmente se presenta el direccionamiento IP, mascara de red, sistema de gestor de base de datos, nombre de los hosts, sistema operativo, y numero de puerto.

Tabla 4.
Descripción.

Herramienta	Sistema operativo	Dbms	Direccionamiento ip	Puerto	Nombre del hosts
Zabbix	Ubuntu Server 20.04	Mysql	192.168.1.20/24	80	(zabbix.puertoatun.com)
NAGIOS	Ubuntu Server 20.04	Mysql	192.168.1.21/24	80	(nagios.puertoatun.com)
PRTG	Windows	Microsoft SQL	192.168.1.22/24	80	(prtg.puertoatun.com)
Pandora FMS	Ubuntu Server	Mysql	192.168.1.23/24	80	(pandorafms.puertoatun.com)
Open NMS	Linux Ubuntu20.04	Mysql	192.168.1.24/24	8980	(opennms.puertoatun.com)
DUDE	Linux Ubuntu20.04	MiB	192.168.1.26/24	8291	(zenoss.puertoatun.com)
Cacti	Linux Ubuntu20.04	Mysql	192.168.1.27/24	80	(catic.puertoatun.com)

Elaboración: Los autores.

Operar, en esta fase se especifica el análisis funcional del laboratorio de ensayo realizado en base a los requisitos. Al definir las interfaces y su tipo, puede realizar monitoreos activos de la red, identificando dispositivos informáticos y equipos de red que serán monitoreados a través de las herramientas definidas en las fases anteriores. Para realizar el monitoreo de redes y aplicaciones fue necesario establecer una serie de parámetros que permitiesen valorar cada una de las soluciones desplegadas, los componentes definidos para la evaluación fueron divididos en cinco categorías generales: requerimientos del sistema, seguridad, soporte, facilidad de uso y administración.

Optimizar, se procedió a realizar las mejoras en lo que respecta a distribución de los equipos activo que realizan la operatividad de la red. Se nos permitió alcanzar y analizar el tráfico de la red considerando reducir los riesgos mediante el monitoreo establecido.

RESULTADOS

Para obtener resultado de tráfico entrante y saliente es fundamental configurar dentro del routers de core un puerto mirror puerto espejo que permitirá obtener el tráfico total y analizarlo mediante las herramientas de monitoreo, las herramientas utilizadas para el laboratorio fueron, Zabbix, PRTG, Nagios, Pandora FMS, OpenNMS, Dude y Cacti. Los sistemas de monitoreo y análisis de tráfico permitieron comparar el procesamiento, y congestión de componentes hardware hosts, RAM, CPU, red. Adicionalmente las permiten la agregación de nuevos servicios. Los mismos que emiten notificaciones mediante sistema de correo electrónico de los fallos que se generan en los equipos monitorizados, incluyendo equipos de radio enlace, en la tabla 5, se muestran los tipos de ponderaciones en base requerimiento del sistema, seguridad, soporte, facilidad de uso y administración.

CIENCIAMATRIA
Revista Interdisciplinaria de Humanidades, Educación, Ciencia y Tecnología
Año VIII. Vol. VIII. Nro. 4. Edición Especial 4. 2022
Hecho el depósito de ley: FA2021000002
ISSN-L: 2542-3029; ISSN: 2610-802X
Instituto de Investigación y Estudios Avanzados Koinonía (IIEAK). Santa Ana de Coro. Venezuela

Tabla 5.
Tipos de ponderaciones.

Herramientas Características	Zabbix 4.0	Prtg network monitor	Nagios core 4.4.3	Pandora fms 7.0	Open nms	Cacti	Dude
REQUERIMIENTOS DEL SISTEMA (5)	**4**	**2.5**	**4**	**3.5**	**3**	**3**	**3.5**
Dificultad de instalación	Baja (1)	Baja (1)	Media (0.5)	Media (0.5)	Media (0.5)	Media (0.5)	Baja (1)
Instalación en Linux	1	0	1	1	1	1	1
Instalación en Windows	0	1	1	1	0	0	0
Licencias	1	0.5	1	1	1	1	1
Bases de datos	1	0	1	0.5	0.5	0.5	0.5
SEGURIDAD (5)	**3.5**	**2**	**2**	**3.5**	**2.5**	**2.5**	**2.5**
Control de versión	**0.5**	**0.5**	**0.5**	**0.5**	**0.5**	**0.5**	**0.5**
Seguimiento de auditoria	**0**	**0**	**0**	**0**	**0**	**0**	**0**
Gestión de sesiones	**1**	**0**	**0**	**1**	**0**	**0**	**0**
Verificación de correo electrónico	**1**	**1**	**1**	**1**	**1**	**1**	**1**
Acceso remoto	**1**	**0.5**	**0.5**	**1**	**1**	**1**	**1**
SOPORTE (6)	**4.5**	**3**	**4.5**	**3.5**	**2.5**	**2**	**3.5**
Soporte comercial	1	1	0.5	0.5	0	0.5	0.5
Foro público	1	0	1	0	0.5	0	1
Manuales comerciales	0.5	0	0.5	0.5	0.5	0.5	1
Ayuda en línea	0.5	1	1	1	0.5	0	0
Desarrollo de terceros	0.5	0	1	1	0.5	0.5	0.5
Aprendizaje comercial	1	1	0.5	0.5	0.5	0.5	0.5
FACILIDAD DE USO (8)	**8**	**7.5**	**7**	**7.5**	**5.5**	**5.5**	**5.5**
Auto descubrimiento	1	1	0.5	1	0.5	0.5	1
Perfiles de usuario	1	1	1	1	1	1	1
Gráficas	1	1	1	1	1	1	1
Informes	1	1	1	1	1	1	1
Mapas	1	0.5	1	0.5	0.5	0.5	0.5
Aplicación web	1	1	1	1	1	1	0
Informar cumplimiento SLA´s	1	1	1	0	0	0	0
Complejidad para administrar nodos	**Baja (1)**	**Baja (1)**	**Media (0.5)**	**Baja (1)**	**Media (0.5)**	**Media (0.5)**	**Baja (1)**
ADMNISTRACIÓN (14)	**10**	**11**	**9**	**6.5**	**8**	**7.5**	**10**
SNMP	1	1	1	0.5	1	1	1
Plugins o sensores	0.5	1	0.5	0.5	0.5	0.5	0
Estadísticas	1	1	1	0.5	1	1	1

Soporte para IPv6	1	1	0.5	0.5	0.5	0.5	1
Aplicación móvil	1	1	1	0.5	0	0	1
Alertas	1	1	0.5	0.5	1	1	1
Notificaciones vía mail	1	1	1	0.5	1	1	1
Notificaciones vía sms	1	1	0.5	0	0.5	0.5	0.5
Notificaciones por mensajería instantánea	0	0	0.5	0	0	0	0
Mapas	0.5	1	0.5	1	0.5	0.5	0.5
Monitorización distribuida	1	1	0.5	1	1	0.5	1
Scripts externos	0	0	0.5	0	0	0	1
Creación de complementos	0	0	0.5	0	0	0	0
Registro de Logs	1	1	0.5	0.5	1	1	1
Ponderación total	**30**	**26**	**26.5**	**24.5.**	**21.5**	**20.5**	**25**

Elaboración: Los autores.

En el análisis de cada una de las herramientas al momento de su operación y ejecución se encontraron los siguientes eventos, apagado de equipos en la red, la sobrecarga de CPU, RAM, Estabilidad de la red, Firmware, sobre carga de almacenamiento o apagado de alguno de ellos. Ver: tabla 6.

Tabla 6.
Eventos.

Herramientas / Eventos	Prtg	Zabbix	Pandora	Nagios	Ip
No se detectó ping detección en tiempo real	x				192.168.10.244
Detectó todo los host caídos detección por correo electrónico	x				192.168.10.0/24
Firewire ha sido actualizado		x			192.168.10.1
Uso de ancho de banda		x			192.168.10.1
Sobrecarga del CPU				x	192.168.10.1
Sobre carga en disco duro + 90% detección de tiempo real				x	192.168.10.252
Sobre carga CPU del computador, detección en tiempo real				x	192.168.10.93
Apagado de central telefónica detección por correo electrónico			x		19.168.10.252

Elaboración: Los autores.

CIENCIAMATRIA
Revista Interdisciplinaria de Humanidades, Educación, Ciencia y Tecnología
Año VIII. Vol. VIII. Nro. 4. Edición Especial 4. 2022
Hecho el depósito de ley: FA2021000002
ISSN-L: 2542-3029; ISSN: 2610-802X
Instituto de Investigación y Estudios Avanzados Koinonía (IIEAK). Santa Ana de Coro. Venezuela

Requisito del sistema

En cuanto al cumplimiento de los requisitos de los sistemas operativos Linux y Windows, en este apartado la ponderación más alta es 5 Puntos, por los cual se determinó que la herramienta Zabbix y Nagios es la de mayor porcentaje de cumplimiento con un valor de 4 puntos mientras que PRTG es la aplicación de menor satisfacción con un valor de 2,5. Gráfico1.

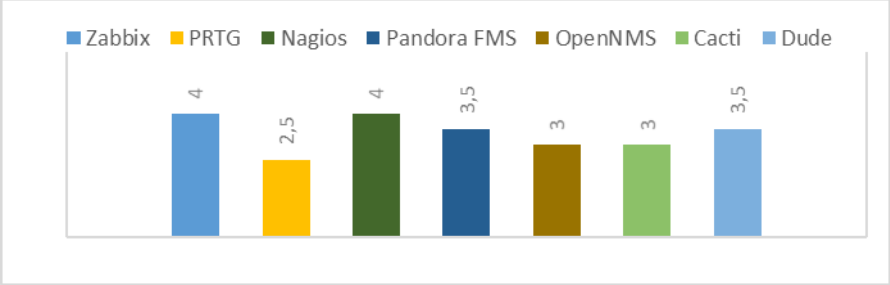

Gráfico 1. Cumplimiento de requisitos del sistema operativo Linux y Windows
Elaboración: Los autores.

Seguridad

En Cuanto a los parámetros de seguridad de las 7 herramientas de monitoreo de red se llegó a la conclusión que Zabbix y Pandora FMS son las soluciones con más altos estándares de seguridad con un valor de 3,5/5. Gráfico 2.

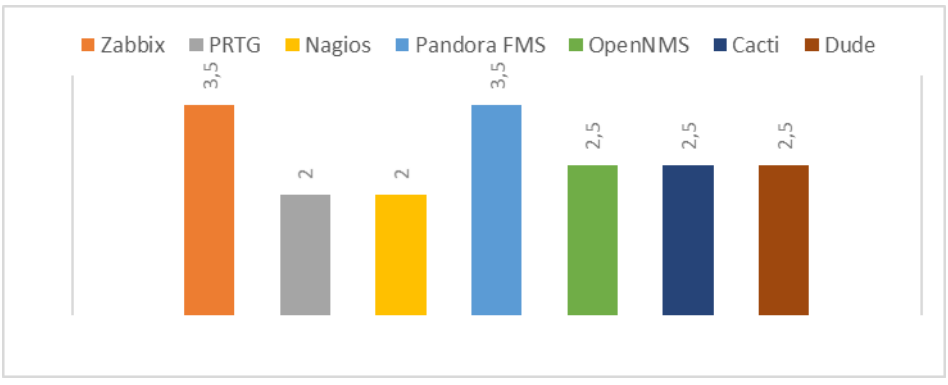

Gráfico 2. Parámetros de seguridad de las herramientas de monitoreo de red.
Elaboración: Los autores

Prestaciones de soporte

Prestaciones de soporte de las herramientas este parámetro fue analizado con una ponderación máxima de 7. Zabbix y Nagios brindan mayores facultades de soporte con un valor de 4,5 mientras que la aplicación de menores prestaciones en este aspecto es Cacti con un valor de 2. Gráfico 3.

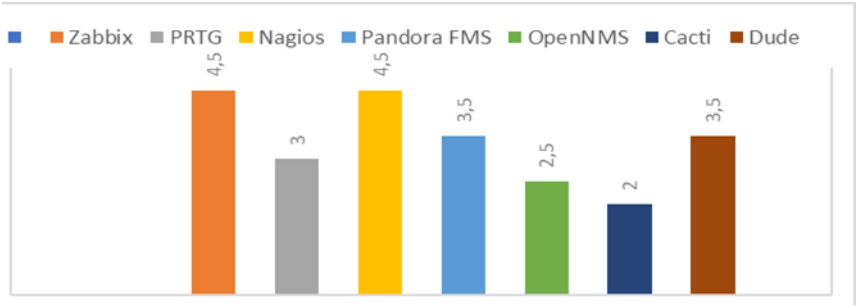

Gráfico 3. Prestaciones de soporte de las herramientas.
Elaboración: Los autores.

Facilidad de uso

Facilidad de uso de las herramientas se pondero como máximo 8 puntos definiendo en los análisis de cada ítem el cumplimiento de Zabbix alcanza el máximo de los parámetros asignados. Gráfico 4.

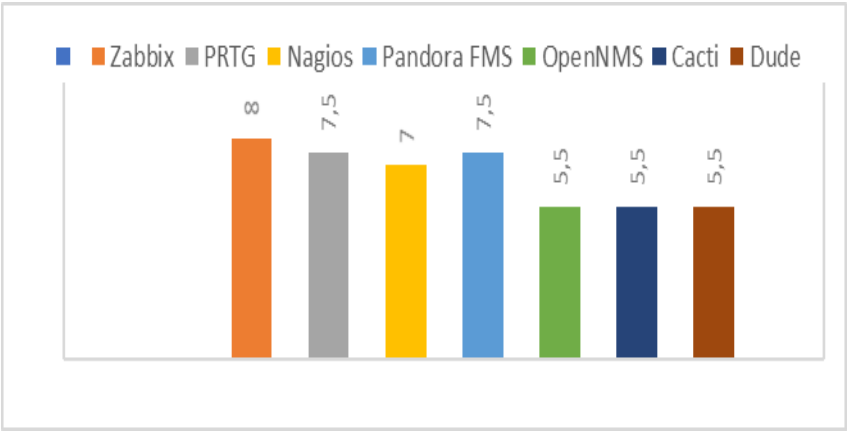

Gráfico 4. Facilidad de uso de las herramientas de monitoreo.
Elaboración: Los autores.

CIENCIAMATRIA
Revista Interdisciplinaria de Humanidades, Educación, Ciencia y Tecnología
Año VIII. Vol. VIII. Nro. 4. Edición Especial 4. 2022
Hecho el depósito de ley: FA2021000002
ISSN-L: 2542-3029; ISSN: 2610-802X
Instituto de Investigación y Estudios Avanzados Koinonía (IIEAK). Santa Ana de Coro. Venezuela

Administración

En los parámetros de administración de las herramientas en el análisis de cumplimiento de otorgo a PRTG que tiene un valor de 11 puntos sobre 14 que sería la puntuación máxima en este análisis. Gráfico 5.

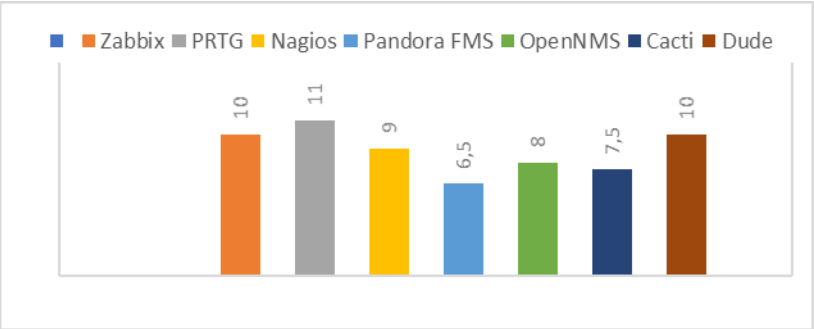

Gráfico 5. Parámetros de administración de las herramientas.
Elaboración: Los autores.

Una vez obtenido el registro de actividades, 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 un tiempo prudente en días.

Evaluación total de las herramientas

La evaluación total de las herramientas, verificando que el sistema de monitoreo con mejores prestaciones es Zabbix con un valor de 30/38 de cumplimiento de los puntos establecidos entre todas las herramientas, seguidamente se ubica Nagios con un total de 26.5/38, mientras que PRTG tiene un valor de 26/38, seguido del sistema Dude con el valor de 25/38, mientras que Pandora tiene un valor de 24.5/38, y con valores menores podemos encontrar a Open NMS con 21.5/38 seguido del bajo del análisis es el sistema Cati con un valor de 20.5/38. Gráfico 6.

Año VIII. Vol. VIII. Nro. 4. Edición Especial 4. 2022
Hecho el depósito de ley: FA2021000002
ISSN-L: 2542-3029; ISSN: 2610-802X
Instituto de Investigación y Estudios Avanzados Koinonía (IIEAK). Santa Ana de Coro. Venezuela

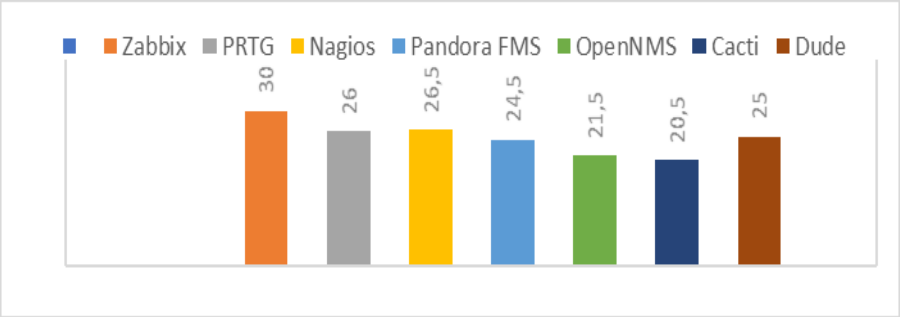

Gráfico 6. Evaluación total de las herramientas.
Elaboración: Los autores

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 González Álvarez. (2013), 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. De acuerdo lo que manifiestan Junco Romero, & Rabelo Padua. (2018) que existe un gran número de herramientas para resolver el problema del monitoreo de red. Existen soluciones comerciales como basadas en software libre. La elección depende de varios factores tanto. Humanos, económicos, como de infraestructura.

CONCLUSIÓN

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. La implementación se realizó de manera física por ende nos permitió identificar

que en la actualidad las empresas cuentan con hardware mínimo para el despliegue de herramientas de monitoreo y su ejecución para la optimización de los recursos de la red.

FINANCIAMIENTO

No monetario.

AGRADECIMIENTO

A la Universidad Técnica de Manabí; por motivar el desarrollo de la investigación.

REFERENCIAS CONSULTADAS

Alava Zambrano, A., Y Guerrero Rodríguez, G. (2018). Análisis de uso, beneficios y simulación de pandora FMS para el monitoreo de sistemas y redes. [Usage analysis, benefits and simulation of pandora FMS for system and network monitoring]. Tesis de Grado. Universidad de Guayaquil. Recuperado de: https://n9.cl/52ldr

Becerra Orrala, E. (2016). Implementación de monitoreo de red utilizando los Protocolos icmp y snmp. [Implementation of network monitoring using icmp and snmp protocols]. Tesis der Grado. Universidad Estatal Península de Santa Elena. Recuperado: https://n9.cl/4vqo0

González Álvarez, S. (2013). Comparativa d'eines de monitorització de sistemes. Tesis de Grado. Universitat Oberta de Catalunya. Recuperado de: https://n9.cl/7ovk6

Guevara Aulestia, D. y Sánchez Cunalata, 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. [Implementation of a monitoring and data protection system in the network of the School of Systems, Electronics and Industrial Engineering]. Tesis de Grado. Universidad Técnica de Ambato. Recuperado de: https://n9.cl/oy2cv4

Issariyapat C., Pongpaibool P., Mongkolluksame S., y Meesublak, K. (2012). Uso de Nagios como base para desarrollar un mejor sistema de monitoreo de red.[Using Nagios as a basis for developing a better network monitoring system].*Actas de PICMET.: Gestión de tecnología para tecnologías emergentes*, BC, Canadá; 2771-2777.Recuperado de: https://n9.cl/5c32m

Junco Romero, G., & Rabelo Padua, S. (2018). Los recursos de red y su monitoreo. [Network resources and their monitoring]. *Revista Cubana de Informática Médica*, 10(1), 76-83. Recuperado de: https://n9.cl/y1mr7

Newman, M. (2018). Networks. Edición 2. Editor Oxford University. Recuperado de: https://n9.cl/hoxr2

Ozkaya E., y Islam R. (2019). Inside the Dark Web. Editor CRC Press. Recuperado de: https://n9.cl/fcy14

Pérez Santos, L. (2013). Estudio comparativo de los sistemas de gestión y monitoreo basados en los requerimientos generales de la red de un campus universitario. [Comparative study of management and monitoring systems based on the general requirements of a university campus network]. Tesis de Maestría. Pontificia Universidad Católica Del Ecuador. Recuperado de: https://n9.cl/sp9c

Quispe Bustincio, J. (2018). Implementación de un sistema de monitoreo y control de red, para un canal de televisión, basado en herramientas Open Source y Software Libre, Lima – 2017. [Implementation of a network monitoring and control system for a television channel, based on Open Source and Free Software tools, Lima – 2017]. Tesis. Universidad Nacional del Altiplano. Recuperado de: https://n9.cl/bqa09

Saavedra Drouet, C. (2018). Control de servicios de red y servidores basado en herramientas de administración de red y políticas de gestión de calidad. [Control of network and server services based on network management tools and quality management policies]. Tesis de Grado. Pontificia Universidad Católica Del Ecuador Sede Esmeraldas. Recuperado de: https://n9.cl/c8c02

Santiago, R. y Trabaldo, S. (2015). Mobile learning: Nuevas realidades en el aula. [Mobile learning: New realities in the classroom]. Editor Digital-Text. Recuperado de: https://n9.cl/4gjlg

Tse Mundaca, A. (2020). Integración de un Sistema de monitoreo de energía y clima para un centro de datos de tipo Tier III. [Integration of an energy and climate monitoring system for a Tier III data center]. Tesis de Grado. Universidad Tecnológica de Perú. Recuperado de: https://n9.cl/yg0yck

CIENCIAMATRIA
Revista Interdisciplinaria de Humanidades, Educación, Ciencia y Tecnología
Año VIII. Vol. VIII. Nro. 4. Edición Especial 4. 2022
Hecho el depósito de ley: FA2021000002
ISSN-L: 2542-3029; ISSN: 2610-802X
Instituto de Investigación y Estudios Avanzados Koinonía (IIEAK). Santa Ana de Coro. Venezuela

Milton Luyely Intriago-Cedeño; Freddy Andrés Carrera-Sánchez; Eduardo Morejón-López;
Josselyn Stefanía Pita-Valencia