Importancia de las herramientas CAAT's para monitorear el tráfico de red, en la ejecución de una auditoría de sistemas.

Ana Betsabeth Ávila Parra[1]

Hugo Alberto Lozada Gaviria[2]

Resumen

Las CAAT's (Computer Audit Assisted Techniques), son un conjunto de técnicas y herramientas, que plantea la mejora a la eficiencia, el alcance y la confiabilidad de los análisis realizados por el auditor. Estos contemplan software de auditoría generalizado, software utilitario, datos de prueba y sistemas expertos. En el caso de software utilitario, por ejemplo, encontramos los que están enfocados en el monitoreo del tráfico de redes de datos, en donde la cantidad de información puede llegar a variar dependiendo del tamaño de la red y la tipología.

Este artículo pretende dar a conocer cuáles son los beneficios y ventajas, así como el funcionamiento general de estas herramientas de monitoreo de red, adicionalmente se muestran cuáles son las más utilizadas en el mercado nacional e internacional incluyendo los proyectos que se encuentran en fase de investigación y desarrollo.

También se da una mirada de cómo los CAAT's aportan ventajas y beneficios a las actividades que realizan los auditores de sistemas en la ejecución de pruebas sustantivas, específicamente en la recolección, procesamiento, análisis y presentación de evidencias optimizando tiempo y recursos de un programa de Auditoría.

[1] Ana Betsabeth Ávila Parra, profesional en Ingeniería de Sistemas de la Universidad Distrital Francisco José de Caldas, estudiante de la Especialización de Auditoría de Sistemas en la Universidad Antonio Nariño. abap79@gmail.com

[2] Hugo Alberto Lozada Gaviria, profesional en Ingeniería de Sistemas de la Universidad Salazar y Herrera de Medellín, estudiante de la Especialización de Auditoría de Sistemas en la Universidad Antonio Nariño. hulozadag@gmail.com

Palabras Claves: red, monitoreo, CAAT's, tráfico de red, auditoría.

Abstract

The main problem presented by networks in the red world is the lack of monitoring and control of the devices and services connected to it, being feasible to meet the general objective of this project, which is to show the relevance of network monitoring as well as auditing. The monitoring and control of network elements can be done with these tools in real time and thus get your work done faster and more efficiently using existing technology. With the constant advancement of network technology and the rapid growth of networks, network administrators have the option of an effective solution when it comes to having control of what is happening on the network and monitoring the devices and services they want

I. Introducción

Las CAAT's (Computer Audit Assisted Techniques), son un conjunto de técnicas y herramientas, normalizadas mediante el estándar SAP 1009 (Statement of Auditing Practice), que plantea la mejora a la eficiencia, el alcance y la confiabilidad de los análisis realizados por el auditor. Define métodos y procedimientos administrativos, informáticos y analíticos, que complementan las técnicas tradicionales de auditoría y pueden servir de apoyo, en pruebas de transacciones, analítica de datos, configuración de sistemas operativos, pruebas de gestión de acceso, versionamiento de software, codificación, muestreo de datos, seguimiento a controles informáticos sobre aplicaciones, calidad de datos, etc.

Los CAAT's contemplan software de auditoría generalizado, software utilitario, datos de prueba y sistemas expertos. En el caso de software utilitario, por ejemplo, encontramos los que están enfocados en el monitoreo del tráfico de redes, en donde la cantidad de información puede variar dependiendo del tamaño de la red y la tipología de esta.

Este artículo pretende dar a conocer cuáles son sus beneficios, ventajas y el funcionamiento general de las herramientas de monitoreo de red, adicional, se mostrarán cuáles son las más utilizadas a nivel nacional e internacional incluyendo los proyectos en fase de investigación y desarrollo.

De acuerdo con lo observado durante la investigación, se mostrará como los CAAT's aportan ventajas y beneficios a las actividades que realizan los auditores de sistemas en la ejecución de pruebas sustantivas, específicamente en la recolección, procesamiento, análisis y presentación de evidencias optimizando tiempo y recursos de un programa de Auditoría.

II. Metodología

La auditoría de sistemas ha venido experimentando cambios en su desarrollo, debido al avance de las tecnologías de la información, lo cual hace necesario apoyarse en herramientas que le brinden al auditor la facilidad y practicidad para hallar evidencias que soporten su opinión. Esta investigación, tiene como objetivo resaltar la importancia de los CAAT's en la auditoría para el análisis del tráfico de red, y comparar y describir las herramientas más utilizadas en el mercado.

Las fuentes de consulta para esta investigación son las páginas web de los fabricantes de estas herramientas de monitoreo de red y la documentación de implementaciones ya realizadas.

III. Resultados y discusiones

Para comprender el funcionamiento y la estructura del monitoreo de la red es necesario entender que, mediante la recopilación y el análisis de tráfico se pueden detectar eventos que podrían afectar la infraestructura tecnológica y podrían causar una baja latencia, pérdida o denegación del servicio, e inestabilidad en general. Si esto sucede se podría dejar de brindar un óptimo servicio a los clientes, causando grandes problemas para la empresa e incomodidad en los clientes.

La gestión en el monitoreo de red va más allá de verificar consumos de ancho de banda, analizar pérdidas de paquetes o comprobar la conectividad de un punto a otro. Su principal ventaja, es permitir el análisis de grandes volúmenes de información en tiempo real mediante Netflow (flujos de información). Adicionalmente se tiene una visibilidad completa de toda la infraestructura de red, el transporte de los datos, el rendimiento y la corrección de fallas.

Monitorear el rendimiento permite anticipar mejoras en la infraestructura y crear alarmas cuando el rendimiento no obedece a la normalidad o cuando se identifiquen amenazas de seguridad de la red, como, un ciberataque que está acompañado de un tráfico de red más alto de lo normal.

De acuerdo con lo anterior, es necesario que las organizaciones cuenten con algún tipo de herramienta para la adecuada administración y gestión de sus redes, por lo tanto, al momento de adquirir alguna de estas herramientas se deberían considerar los siguientes puntos:

- Comunicación de alertas.
- Integraciones con servidores externos.
- Usabilidad y presentación de los datos en un panel de control.
- Integraciones con la base de datos
- Soporte de la mayor cantidad de protocolos de adquisición de datos posibles
- Seguridad
- Integración con máquinas virtuales
- Control remoto
- Inventario de hardware y software
- Geolocalización
- Generación de informes parametrizables.

Estas herramientas de red aprovechan el protocolo SNMP (Simple Network Management Protocol), que ha tenido avances significativos, y que permite hacer un monitoreo de forma segura, puesto que incorpora controles que evitan ataques cibernéticos.

Es importante conocer el protocolo SNMP, porque por medio de él se puede leer o controlar el rendimiento de la red. Su última versión es la 3, que incorpora funcionalidad para IPV6, manteniendo las de IPV4. Adicionalmente maneja parámetros de encriptación y autenticación para poder realizar el monitoreo. La integridad de la información se garantiza mediante algoritmos hash MD5 (Message Digest) o con Sha (Secure Hash Algoritm).

Existen herramientas gratuitas y otras de pago. Dentro de las gratuitas, las más versátiles son Nagios y Cacti. Estas herramientas permiten el monitoreo de toda la infraestructura de red, por estados o por servicios como Http (Hypertext Transfer Protocol), Ssh (Secure Shell), Icmp (Internet Control Message Protocol), permitiendo visualizar degradaciones en estos servicios.

En cuanto a herramientas de pago, existen algunas muy versátiles como Pandora FMS, ManageEngine, Orion de SolarWinds, GlassWire.

Las herramientas de pago incorporan mayor control del flujo de transmisión, incluyen gráficas estadísticas, diagramas de mapas de red, mapas de calor de señal de radio y wifi, descubrimiento de dispositivos en capas físicas, generación de alarmas a través de correos electrónicos y mensajes de texto, y otras funcionalidades que ayudan a tener control completo del tráfico.

Es necesario reconocer la relevancia del uso de herramientas CAAT en la ejecución de una auditoría de sistemas y como uno de los objetivos de este artículo resaltaremos esa importancia:

¿Qué es una auditoría de sistemas a las redes de comunicación?

La auditoría de red son las medidas colectivas que se realizan para analizar, estudiar y recopilar datos sobre una red con el fin de determinar su estado de acuerdo con los requisitos de la organización. Realizar este tipo de auditorías proporciona información sobre cuán efectivas son las prácticas y el control de la red, es decir, su cumplimiento de las políticas internas y externas. Esta auditoría analiza una red con diferentes herramientas para determinar:

- Seguridad
- Implementación de control
- Disponibilidad
- Administración
- Gestión

Para lograr esto, un auditor de sistemas debe recopilar datos, verificar la efectividad de los controles e identificar vulnerabilidades y amenazas a través de técnicas manuales y automatizadas que permitan revisar el estado de la red.

IV. La importancia de la auditoria de redes

Las empresas deben evaluar la seguridad en sus redes puesto que los entornos empresariales dependen en gran medida de la tecnología de la información. La evaluación de seguridad de la red es un componente vital del control, monitoreo, mantenimiento y reparación de la misma.

Realizar una adecuada auditoría de redes de comunicación les sirve a las organizaciones para:

✓ Inventario: A medida que las organizaciones y sus demandas crecen, se producen fusiones en los dispositivos y pasan de un equipo operativo a otro o se pueden agregar o eliminar dispositivos y por lo tanto los administradores podrían no saber la conformación de su red.

✓ Actualización de la red: Las redes tienden a caer en el estado operativo en el que los administradores se preocupan por su funcionamiento, para mantenerse al día con las demandas, dichas redes deberán actualizarse. Antes de actualizar se debería realizar una auditoría de red para saber el estado actual, qué dispositivos todavía son compatibles con el proveedor (software y hardware), qué dispositivos reemplazar y cuáles actualizar.

✓ Resolución de problemas: Para resolver un problema de red es necesario saber inicialmente qué la conforma y realizar una evaluación para determinar las alternativas de solución.

✓ Cumplimiento: Dependiendo del tipo de negocio en el que se encuentre una organización, se les puede exigir que cumplan con ciertos estándares (por ejemplo, PCI DSS (Payment Card Industry Data Security Standards)). La organización usará una auditoría de red para prepararse para la auditoría y auditores externos para evaluar el cumplimiento (Ciberseguridad, 2022)

V. Técnicas y herramientas de auditoría para el tráfico de red

En la actualidad existen varias técnicas y tecnologías para el monitoreo del tráfico de red. Las redes de datos manejan información con protocolos y aplicaciones cada vez más complejos y adicionalmente se cuenta con una gran cantidad de información que se transfiere de forma simple o cifrada, ha hecho de la tarea del monitoreo una labor compleja. (Arenas, 2015)

Se han venido desarrollando tecnologías de análisis de datos como SIEM (Security Information and Event Management), SIM (Security Information Management), SEM (Security Event Management), NSM (Network Security Monitoring), PNA (Passive Network Audit), etc. Estas tecnologías han ido adicionando modelos de análisis de información e incluso incorporando machine learning para detectar e identificar patrones. Existen también diversas técnicas y herramientas que ayudan a los administradores a elegir un modelo de monitoreo, detección y auditoría que mejore la seguridad de sus organizaciones**.”** (Arenas, 2015)

Algunas técnicas pueden ser más efectivas, dependiendo del monitoreo y tomando en cuenta varios aspectos como características, ventajas y enfoque. La Figura 1 presenta un panorama general sobre la relación entre los modelos de monitoreo y detección.

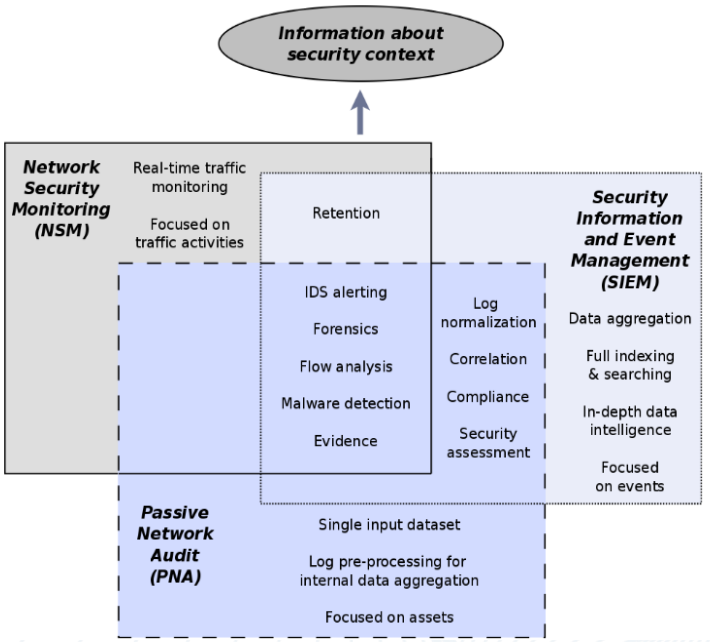

Figura 1. *Panorama general de los modelos de monitoreo y análisis*

Fuente: *revista.seguridad.unam.mx/print/2217*

La *minería de datos* es un proceso de extracción de modelos descriptivos a partir de grandes cantidades de datos, en el contexto de la seguridad en TI, la minería de datos se encuentra en los SIEM (Security Information and Event Management) para la identificación de patrones que detectan, realizan auditoría e interpretan información. Las fuentes de datos a analizar para la evaluación de red pueden ser herramientas como IPS (Intrusion Prevention Systems), IDS, firewalls, routers, bitácoras de sistemas, etc. (Arenas, 2015)

Entre las características principales que los SIEM proporcionan:

✓ Acumulación de datos (data aggregation): Los datos provienen de varias fuentes y alimentan una base de análisis centralizada.

- ✓ Correlación: Identifica relaciones y se hacen interpretaciones.
- ✓ Alertas.
- ✓ Cumplimiento: Identificar el cumplimiento de políticas.
- ✓ Retención: Se almacenan datos históricos.
- ✓ Análisis forense: Se crean líneas de tiempo para reconstruir eventos.
- ✓ Inteligencia: Descripción de escenarios seguros para la toma de decisiones.

Auditoría Pasiva de Red (Arenas, 2015)

La Auditoría Pasiva de Tráfico de Red (Passive Network Audit) analiza bitácoras y correlaciona datos. La PNA es un modelo de análisis independiente a los SIEM porque se limita al uso de tráfico de red como fuente principal y única para obtener información y generar reportes. PNA solo usa herramientas pasivas para la extracción de información, es decir, que ninguna acción es durante el proceso de análisis altera la operación de la red que se analiza.

Los SIEM acumulan datos (*data aggregation*) de diversas fuentes como *firewalls*, bitácoras de sistemas, IDS, IPS, *routers*, etc. PNA enfoca al tráfico de red como fuente de información. Como se aprecia en la Figura 2, la acumulación de datos se hace de manera interna, e involucra un proceso adicional que es el procesamiento y decodificación de datos para generar bitácoras o datos que serían la fuente de información para un SIEM, sin embargo, en este caso son obtenidos a partir del tráfico de red y son en realidad bitácoras reales. Dicha extracción implica una interpretación y extrapolación de información a partir de datos que representen una firma sobre una actividad o sistema. A partir de este procesamiento previo es posible identificar y decodificar protocolos, versiones de software, dominios, alertas de IDS, flujos, etc., que en otras condiciones serían tomados de bitácoras de sistemas u otros dispositivos, con la ventaja de que el proceso se desarrolla de manera pasiva y únicamente a partir de tráfico de red. (Arenas, 2015)

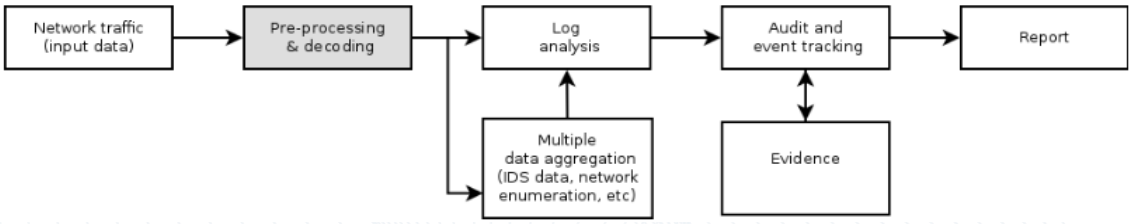

Figura 2 *Diagrama de auditoría pasiva de tráfico de red*
Fuente: *revista.seguridad.unam.mx/print/2217*

PNA también se conoce como Identificación Pasiva de Red (Passive Network Discovery) y algunas fuentes la describen como una tecnología para responder a las preguntas *¿Quién y qué hay en la red de la organización? y ¿Qué se está haciendo en la red de la organización?*, mediante identificación de utilización de la red, análisis forense de eventos, identificación de vulnerabilidades y perfiles de activos (equipos, servidores, entre otros).

VI. Análisis de las herramientas

Actualmente en el mercado existen diferentes herramientas de monitoreo de red, que, de acuerdo con el número de usuarios y versatilidad, son las más usadas a nivel nacional e internacional para ello. Algunas de ellas pueden ser utilizadas de manera gratuita y en otras es necesario pagar por su licenciamiento dependiendo del alcance y complejidad.

✓ *Herramientas de Monitoreo Gratuitas.*

Cacti

Es de libre distribución, con licencia GPL (licencia de derecho de autor usada en el mundo del software libre y código abierto, y garantiza a los usuarios finales la libertad de usar, estudiar, compartir y modificar el software), y programado en PHPJavaScript (lenguaje de secuencias de comandos del lado del cliente y del servidor. PHP no se ejecuta dentro del

navegador, mientras que JavaScript se ejecuta dentro del navegador), y sus informes se basan en gráficas, cuya información en series de tiempo se almacena en una base de datos relacional.

Permite visualizar y monitorear los equipos de una red que posean el protocolo SNMP y se puede observar el ancho de banda consumido por cliente, se detectan congestiones en el tráfico, y se pueden monitorear detalladamente puertos de red. También se obtienen datos sobre la temperatura de los dispositivos de red, voltajes, número de impresiones, etc.

Sus informes son configurables, y contiene plantillas para varios fabricantes. Posee gestión de usuarios, mediante asignación de roles con distintos permisos sobre la administración.

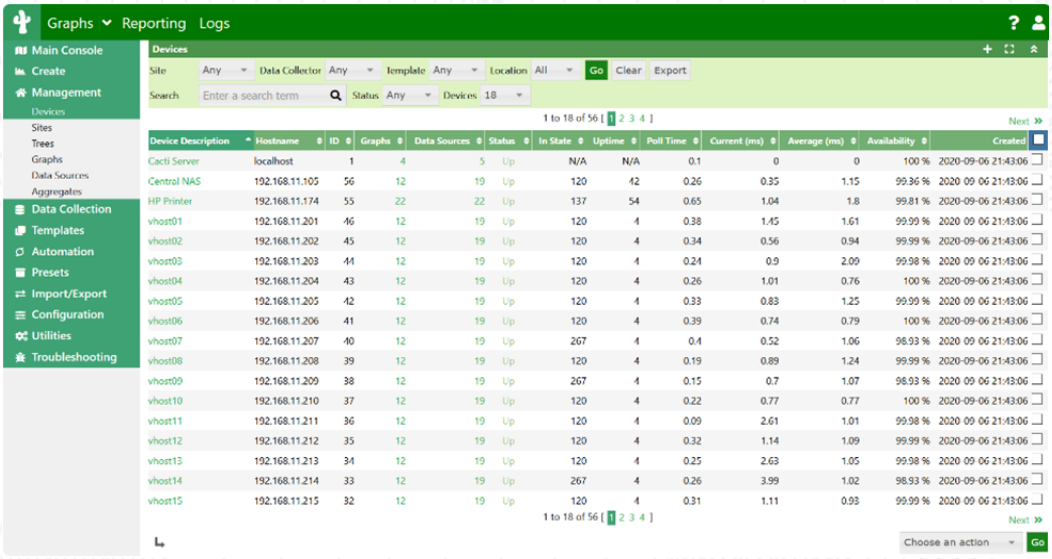

Figura 3. *Reporte de monitoreo por dispositivo.*
Fuente: *Cacti.net, 2022*

Nagios

Esta herramienta es open source, sin embargo, realiza un cobro único de USD $2.000 aprox. correspondiente a soporte. Su principal característica es que almacena estados de dispositivos y al comparar dichos estados, genera alarmas cuando el comportamiento de ellos se

aleja de la línea base. El monitoreo se puede realizar de forma remota utilizando el protocolo SNMP, y puede analizar el procesamiento, utilización de disco, memoria, puertos, etc.

Otra característica, es la generación de eventos por fallas, lo que lo convierte en un orquestador proactivo puesto que, si son recurrentes, autogestiona la solución evitando una indisponibilidad.

También verifica si existe degradación del servicio, mediante el análisis de ICMP, HTTP (Hypertext Transfer Protocol – Protocolo de Transferencia de Hipertexto), ssh (Secure Shell – Protocolo de Administración Remota), etc.

Incluye una sección de informes de disponibilidad configurables, mediante complementos que los usuarios pueden diseñar usando Bash, C++, Perl, Ruby, Python, PHP, C#, etc.

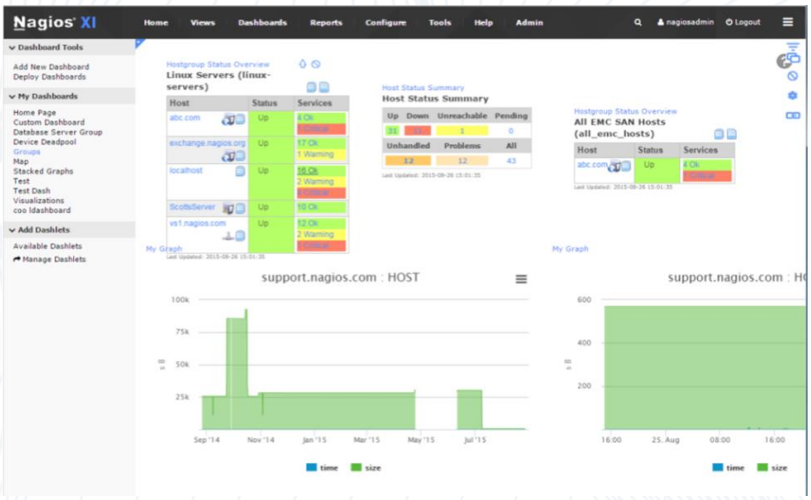

Figura 4. *Monitoreo de host, discriminado por estados y servicios.*
Fuente: *https://www.appvizer.es/it/monitoreo-red/nagios-xi, 2022*

✓ *Herramientas de Monitoreo de Pago.*

Pandora FMS

Posee una licencia GPL privativa, y su valor para la versión Enterprise es de USD $1.000 por año. Existen dos variantes, la primera utiliza agentes por máquina, que reportan actividad a un servidor y la segunda realiza un monitoreo de forma remota mediante protocolo TCP/IP y no

requiere instalar agentes. Puede alcanzar dispositivos como balanceadores de carga, routers, switches, sistemas operativos, aplicaciones o impresoras, validando las cargas de los procesadores, uso de discos y memorias, procesos en ejecución, eventos del sistema en el registro, temperatura, luz, humedad, valores en una aplicación, etc.

Esta herramienta posee características como el monitoreo de red en tiempo real mediante flujo, conocido como Netflow. Puede diseñar mapas, y descubrimiento automático de dispositivos de capa 2 (enlace) y 3 (red) del modelo OSI. Permite ver tráfico de consumo utilizando el protocolo SNMP, utiliza también el ping (utilidad de diagnóstico en redes, que comprueba el estado de la comunicación del anfitrión local con uno o varios equipos que ejecuten IP). Analiza tiempos de latencia, y muestra disponibilidad de los servicios. Cuenta con más de 300 complementos, que incluso se integran con sistemas antivirus y de backup, por medio de los agentes.

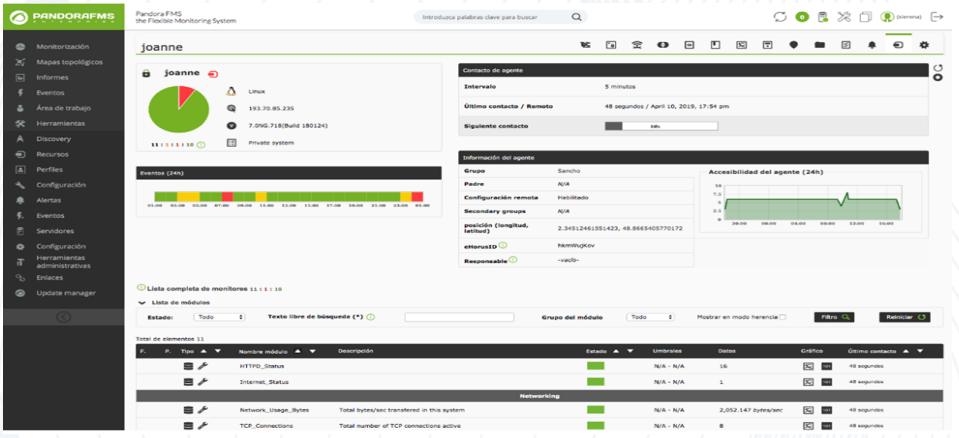

Figura 5. *Monitoreo de dispositivos.*
Fuente: *https://www.appvizer.es/it/monitoreo-red/pandora-fms, 2022*

Manaengine

Es una de las tres divisiones de la multinacional Zoho, dedicada a distintos ámbitos de tecnología. Manaengine se enfoca en más de 90 productos, muchos de ellos gratuitos, y que

contribuyen a la gestión de directorio activo, mesa de ayuda IT, redes y servidores, aplicaciones, seguridad de IT, analítica de datos, servicios en la nube y servicios administrados.

Es un software que tiene tipo de licencia freeware que es limitada por número de usuarios, pero si se desea ampliar este uso se debe pagar una licencia dependiendo del número de nodos o agentes.

Permite el monitoreo de red y descubrimiento de dispositivos, tales como: routers, switches, firewalls, servidores, impresoras etc. En caso de una falla, puede detectar la causa, eliminarla antes de que se vea afectada toda la infraestructura y además permite conocer su estado y disponibilidad enviando alarmas vía correo electrónico o SMS cuando se ha detectado un problema. Visibiliza consumo de ancho de banda real, y uso de VPN, y ayuda a precisar necesidades futuras con base en el rendimiento actual. Puede supervisar URL's destino y bloquear tráfico de red que no se desee con análisis mediante patrones de tráfico.

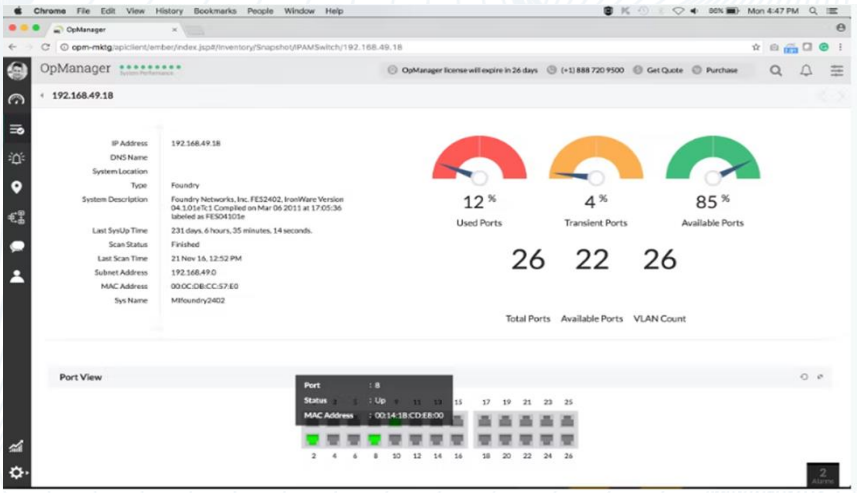

Figura 6. *Monitoreo de direcciones IP.*
Fuente: *https://www.manageengine.com/latam/network-monitoring/, 2022*

Orion – SolarWinds

Es una herramienta de monitoreo que utiliza el módulo NPM (Network Performance Monitor) para realizar el monitoreo de red que permite un período de evaluación de 30 días totalmente funcional y luego se deberá adquirir la licencia para continuar con su funcionamiento.

Es una herramienta bastante intuitiva y configurable, además de personalizable, que permite realizar el monitoreo de fallas, medir el desempeño, la disponibilidad de los equipos de red de varios proveedores, analizar el desempeño de aplicaciones, bases de datos, seguridad, servicio y calidad TI y optimización de la señal wifi mediante el diseño de mapas de calor en los que se sugiere evitar puntos físicos de acceso dudosos.

Permite la creación de una línea base del desempeño de la red, para alertar comportamientos anormales.

Es utilizada por más de 33.000 clientes alrededor del mundo, pero en el año 2020 fue hackeada por inteligencia rusa, que afectó a varias oficinas gubernamentales de Estados Unidos y de Europa, esto se realizó durante 7 meses y en este tiempo no se detectó la intrusión.

Figura 7. *Detección de fallas de dispositivos de red*
Fuente: *https://www.solarwinds.com/es/network-bandwidth-analyzer-pack, 2022*

VII. Proyectos de Implementación

A continuación, se presentan algunos proyectos implementados donde se utilizan las herramientas de monitoreo de red.

Implementación Cacti:

Por su tipo de licencia y funcionalidad, es muy utilizado por pymes a nivel nacional, y también en el ámbito académico nacional e internacional.

- Edesa S.A. (Barriga, 2013)

Implementa Cacti para la gestión y monitoreo de la red, ya que sus empleados han aumentado.

Se dedica a la fabricación de sanitarios de cerámica y productos complementarios para el baño que se distribuyen en el mercado nacional e internacional.

Implementación de Nagios:

Por su tipo de licencia y funcionalidad, es muy utilizado por pymes a nivel nacional, y por empresas de 200 a 10.000 empleados.

- WILLAX TV

No se contaba con un sistema de monitoreo y era un problema para la organización puesto que se realizan transmisiones en vivo sobre líneas dedicadas. Con NAGIOS se logró una comprobación efectiva y constante de los servicios y dispositivos, asegurando una reacción oportuna ante los fallos que se presenten. NAGIOS supervisa la red en busca de problemas causados por enlace de datos o conexiones de red sobrecargadas, así como por el monitoreo de disco duro, memoria RAM y conmutadores. (Quispe Bustincio, 2017)

Implementación de Pandora FMS:

- Flux Its. (PandoraFMS, 2022)

FLUX ITS es una empresa proveedora de soluciones de integración tecnológica en automatización, control y seguridad para proyectos de infraestructura de transporte, industrial y comercial para los sectores público y privado en México.

Pandora FMS permite realizar el monitoreo de la infraestructura con más de 500 equipos. Ahora se detecta rápidamente cualquier anomalía y se realiza la reparación, minimizando los tiempos.

Se ha conseguido ahorrar tiempo de los recursos humanos para trabajos preventivos, lo que antes tardaba varios días, ahora se repara en unas horas, reduciendo el SLA en más de 50%.

- Toshiba. (PandoraFMS, 2022)

Se requería tener controlados los quioscos de venta de un cliente, ya que al tratarse de máquinas remotas que no están en contacto con el personal del local, si dejaban de funcionar no había posibilidad de repararlas. Se necesitaba una herramienta flexible y que permitiera aumentar considerablemente los acuerdos de nivel de servicio.

Implementación de Manaengine:

- Leche La Alquería. (Manaengine, 2022)

Para el inicio de la pandemia, no estaban preparados para modalidades de teletrabajo, así que adquirieron toda la suite de manaengine, que les permitió robustecer la plataforma para poder seguir operando con sus administrativos desde casa.

- Financiera Fundeser en Nicaragua. (Manaengine, 2022)

Aunque se contaba con una amplia experiencia en TI los programas que utilizaban no ofrecían una visibilidad completa y tenían problemas para garantizar una integración adecuada. Esta situación, unida al uso de programas de software con capacidades limitadas, complicaba las tareas básicas y era imposible una integración, ante esta situación se implementó la suite de ManageEngine para controlar el dominio y monitorear la red, OpManager.

- American Cement Company. (SolarWinds, 2022)

El departamento de TI de la empresa utiliza SolarWinds para administrar el entorno de red a diario. Brinda una visión profunda más allá de lo que pueden hacer otras herramientas y también se relaciona con el almacenamiento y el hardware, lo que brinda una vista de panel único.

- *Finastra. (SolarWinds, 2022)*

(Santillán Arenas, 2015) SolarWinds Network Performance Monitor es el software de gestión de red para el NOC (Network Engineering & Operations). Se usa para administrar los balanceadores de carga tanto en la nube como en las instalaciones, enrutadores y conmutadores, infraestructura inalámbrica, infraestructura de firewall, LAN y WAN, y todos los demás elementos de red. SolarWinds alerta la gestión de umbrales y la generación de informes de rendimiento.

VIII. Conclusiones y comentarios

- Las herramientas de monitoreo de red ofrecen un apoyo a las funciones de administración y gestión de red, pero también se han venido convirtiendo en un aliado de los auditores de sistemas al momento de realizar pruebas sustantivas, a la hora de reunir, procesar y presentar evidencias en menos tiempo del que tomaría un proceso manual.
- Las herramientas de monitoreo de red cuentan con módulos de generación de reportes, que pueden ser adaptados de acuerdo con las necesidades de la organización o del auditor de sistemas, para presentar la información requerida en determinados formatos.
- El volumen de información ha venido aumentando exponencialmente en todo el ámbito de las tecnologías de la información, por lo que contar con un software que automatice tareas manuales que antes consumían bastante tiempo, es uno de los pilares fundamentales en la

optimización, y la auditoría de sistemas no puede negarse a avanzar en este aspecto, al utilizar herramientas que le sean favorables para reunir, procesar y presentar evidencias.

- La seguridad informática y seguridad de la información, también tienen protagonismo en las nuevas funcionalidades de las herramientas de monitoreo de red. La gestión llevada a cabo con las herramientas de red, aporta también al cumplimiento de normativas regulatorias de seguridad informática y seguridad de la información, ayudando a mitigar riesgos mediante la aplicación efectiva de controles.

IX. Lista de Referencias

Arenas, J. U. (19 de Junio de 2015). *Revista Seguridad Universidad Nacional Autónoma de México.* Obtenido de https://revista.seguridad.unam.mx/numero24/frameworks-para-monitoreo-forense-y-auditor-de-tr-fico-de-red-i

Auditorías de red: herramientas, informes y procedimientos. (2022, 14 septiembre). Recuperado 21 de octubre de 2022, de https://www.paessler.com/es/network-audit

Auditorías y análisis de redes e infraestructuras. (2019, 23 diciembre). Ciberseguridad. Obtenido de https://ciberseguridad.com/servicios/auditorias-analisis-redes-infraestructuras/

Barriga, E. L. (2013). *Universidad Politécnica Salesiana - Quito*. Obtenido de https://dspace.ups.edu.ec/bitstream/123456789/4353/6/UPS%20-%20ST000983.pdf

Ciberataques, vulnerabilidades informáticas. Obtenido de https://ciberseguridad.com/servicios/auditorias-analisis-redes-infraestructuras/

IFAC, I. F. (2002). *International Standard on Auditing.* Quito: Corporación Edi-Ábaco Cía. Ltda.

Manaengine. (2022). *Manaengine*. Obtenido de https://download.manageengine.com/latam/network-monitoring/

PandoraFMS. (2022). *Pandora FMS*. Obtenido de https://pandorafms.com/es/flux-caso-de-exito/

Quispe Bustincio, J. W. (2017). *Red de Repositorios Latinoamericanos*. Obtenido de https://repositorioslatinoamericanos.uchile.cl/handle/2250/3278004

SolarWinds. (2022). *SolarWinds*. Obtenido de https://www.solarwinds.com/es/

Team, P. F. (2022, 13 octubre). *Las 16 mejores herramientas de monitoreo de Redes*. Pandora FMS - The Monitoring Blog. Recuperado 21 de octubre de 2022, de https://pandorafms.com/blog/es/herramientas-de-monitoreo-de-redes/

Villa Rasero, C. (25 de febrero de 2016). *BDO, Auditoría & Co*. Obtenido de https://auditoria-auditores.com/articulos/articulo-auditoria-uso-de-herramientas-caat-s-en-las-revisiones-de-control-interno-it/