Monitoreo y Optimización de Red Informática en Tiempo Real: Un Tablero de Control Basado en SNMP y Aplicación en FaCENA-UNNE

Sergio Ariel Zapata[1]

[1] *Universidad Nacional de Nordeste (UNNE)*
sergio.zapata@comunidad.unne.edu.ar

Resumen. En este trabajo presento el desarrollo de un tablero de control interactivo para la gestión y monitoreo de dispositivos de red en la Facultad de Ciencias Exactas y Naturales y Agrimensura (FaCENA), como avance de investigación en el marco de una beca destinada al estudio y aplicación del protocolo SNMP. La aplicación utiliza el protocolo SNMP en sus distintas versiones como base para la recolección de métricas de rendimiento y estado y busca mejorar la administración de la infraestructura de red mediante la visualización en tiempo real sobre el estado de routers, switches y puntos de acceso. Además, integra alertas automáticas y recomendaciones basadas en datos empíricos para optimizar el ancho de banda y la calidad de servicio, ante eventos de alta demanda. El enfoque metodológico combina investigación-acción y revisión sistemática para alinear las funcionalidades de la herramienta con las necesidades concretas de la institución.

Palabras claves: Monitoreo de redes, Tablero de control, SNMP, Métricas, Infraestructura.

Real-Time Computer Network Monitoring and Optimisation: An SNMP-Based Dashboard and Application at FaCENA-UNNE

Abstract. In this paper I present the development of an interactive control panel for the management and monitoring of network devices in the Faculty of Exact and Natural Sciences and Surveying (FaCENA), as a research progress within the framework of a grant for the study and application of the SNMP protocol. The application uses the SNMP protocol in its different versions as a basis for the collection of performance and status metrics and seeks to improve the administration of the network infrastructure by means of real-time visualization of the status of routers, switches and access points. In addition, it integrates automatic alerts and recommendations based on empirical data to optimize bandwidth and quality of service in the face of high demand events. The methodological approach combines action research and systematic review to align the tool's functionalities with the institution's specific needs.

Keywords: Network monitoring, Dashboard, SNMP, Metrics, Infrastructure.

1. Introducción

La administración y mantenimiento de las redes de una institución académica como la Facultad de Ciencias Exactas y Naturales y Agrimensura (FaCENA) no solo implica disponer de hardware y software actualizados, sino que además requiere el desarrollo de estrategias de administración que permitan garantizar el correcto funcionamiento de esta red. Las redes educativas pueden mejorar los resultados de aprendizaje y favorecer la innovación en las actividades de enseñanza (Chapman & Muijs, 2013). La infraestructura tecnológica de FaCENA soporta actividades esenciales, tanto académicas como administrativas, es decir el desarrollo de clases presenciales, híbridas y virtuales, así como la gestión de sistemas de información críticos. Sin embargo, la cada vez más fuerte demanda de servicios hace necesaria la utilización de herramientas que puedan optimizar la administración de la red y de todos sus dispositivos. Según (Kurose & Ross, 2013), el uso de paradigmas de optimización en redes permite mejorar significativamente el rendimiento y garantizar la calidad del servicio en entornos con alta demanda.

Por el momento, FaCENA no cuenta con un tablero de unificado de monitoreo que haga visible la información del estado de los dispositivos de interconexión (switches, routers y puntos de acceso Wi-Fi), y que recomiende ajustes para optimizar el servicio sobretodo en el uso del mismo durante picos de alta demanda. Existen plataformas reconocidas como Observium, que facilitan la gestión de redes de forma completa mediante SNMP, pero estas soluciones implican normalmente problemas de configuración, mantenimiento y uso (Geekflare, 2024). Por esta razón, la presente propuesta contempla una alternativa personalizada, centrada en mostrar el estado de los switches, interfaces y la recepción de alertas, a través de una interfaz gráfica responsive y de fácil acceso a través de cualquier dispositivo.

Este tablero de control tiene el propósito de no solo ayudar en la práctica habitual del equipo técnico, sino que, también, busca anticipar y subsanar potenciales problemas de conectividad mediante el control activo y el empleo de datos de tráfico, la consulta del estado de cada uno de los puertos, acciones remotas como deshabilitar interfaces comprometidas o la recepción de notificaciones automáticas ante cualquier problema crítico. Por otra parte, se propone como una forma de introducir a estudiantes avanzados de la Licenciatura en Sistemas de Información (LSI) en un proyecto de verdadero impacto, aplicando de este modo la práctica de sus conocimientos en ingeniería de software, redes y desarrollo de sistemas, mientras que a la vez se aplica la investigación aplicada en la universidad. La aplicación práctica de los conocimientos en ingeniería de software es esencial para el desarrollo profesional de los estudiantes, ya que permite integrar teoría y práctica en proyectos reales (Bourque & Fairley, 2014).

Este proyecto no solo se ocupa de dar solución a una necesidad auténtica de FaCENA, además establece el camino para futuras investigaciones y desarrollo de gestión de redes en el área académica, convirtiéndose también en un modelo que puede replicarse en aquellas instituciones que tienen una necesidad similar. Proyectos de investigación en red, como los desarrollados por la Universidad Nacional del Litoral y la Agencia Santafesina de Ciencia, Tecnología e Innovación, demuestran cómo la colaboración interinstitucional puede generar modelos replicables y de alto impacto regional (Universidad Nacional del Litoral [UNL], 2024).

2. Metodología, Diseño y arquitectura del sistema

Se realizó la búsqueda de esta solución mediante una metodología que combina la investigación-acción y la revisión sistemática. Este enfoque metodológico permitió obtener información clave del personal involucrado y realizar un análisis exhaustivo de fuentes documentales, se recabaron datos sobre las limitaciones actuales en el monitoreo de red y sobre las expectativas del personal que trabajara con la aplicación con respecto a las funcionalidades necesarias que debería ofrecer una plataforma personalizada. La investigación-acción es un proceso colaborativo que busca mejorar prácticas a través de la participación reflexiva y crítica de los involucrados, mientras que las revisiones sistemáticas permiten sintetizar información científica de manera estructurada (Higgins et al., 2019; Bausela, 2004).

2.1. Ciclo de investigación-acción aplicado

El proceso metodológico siguió un ciclo de cuatro etapas que se sucede en un ciclo continuo: planificar, actuar, observar, reflexionar (Higgins et al., 2019):

Planificar: Se decidió el problema del ‘no monitoreo centralizado de red’ en FaCENA, tras reuniones con el personal técnico. Se elaboró el plan de acción que se incluye en un desarrollo personalizado de una plataforma basada en el protocolo SNMP, el uso de tecnologías web ligeras, compatibles con el entorno de infraestructura refiriéndose al entorno actual.

Actuar: Se realizó el diseño e implementación del prototipo funcional del sistema, utilizando PHP, Bootstrap, CodeIgniter, FreeDS. x SNMP y MySQL. Se realizaron las instalaciones experimentales de Observium para establecer una línea de base de comparación, se virtualizó el entorno de RouterOS para ampliar la cobertura de las pruebas.

Observar: Se hizo un seguimiento del comportamiento del sistema ante diferentes escenarios (equipos Cisco, switches Aruba y entornos virtualizados). Durante el seguimiento se utilizaron herramientas de análisis para registrar latencia, disponibilidad de métricas y capacidades de gestión remota. Se registraron datos cuantitativos (métricas de red) y cualitativos (feedback de usuarios técnicos).

Reflexionar: Se llevó a cabo una revisión crítica de los resultados, identificando las fortalezas y debilidades del sistema. Las observaciones sirvieron como insumo para identificar las próximas fases del proyecto orientadas en la implementación de SNMPv3, las mejoras de seguridad, y la ampliación del sistema a otros dispositivos.

A diferencia de soluciones como **Observium**, que requieren entornos complejos y carecen de gestión activa sobre puertos en su versión comunitaria, esta solución:

- Permite acciones remotas directas (ej. deshabilitar puertos).
- Es ligera, modular y personalizada, lo cual es esencial para instituciones educativas con recursos limitados.
- Está desarrollada sobre software libre, facilitando su replicabilidad en otras facultades o contextos similares.

Se definieron varias etapas o módulos para la implementación de la herramienta con el propósito de realizar las funciones clave del sistema: recolección de datos, procesamiento, almacenamiento y visualización. A continuación, se explican cuidadosamente las etapas y las tecnologías que fueron empleadas para la construcción del sistema.

2.2. Módulo de recolección de datos.

El primer componente del sistema realiza la conexión con los switches a través de SNMP, específicamente utilizando la librería FreeDSx SNMP. Esta librería permite realizar consultas (GET y WALK) sobre los dispositivos de red, accediendo así a la información sobre estado de puertos, tráfico, errores, etc. La librería FreeDSx SNMP es una herramienta útil para implementar funcionalidades de cliente SNMP en aplicaciones PHP, sin requerir la extensión SNMP de PHP (FreeDSx, 2025). Con este propósito se realizaron configuraciones de sesiones SNMP v2c y v3 mediante autenticación por comunidad, adecuadas para los modelos Cisco Catalyst WS-C2960 y Aruba 1930 así como la versión 3 con una autenticación más robusta y encriptada. Con esta primera parte se pretende acceder de manera periódica a los datos necesarios para alimentar la plataforma, garantizando así un monitoreo actualizado.

2.3. Interfaz de visualización.

Para la visualización de la información, se realizó el desarrolló de un dashboard responsive o del tipo web por medio de tecnologías web como PHP, HTML5, CSS3 y JavaScript, entre ellos librerías gráficas como Chart.js para la representación de métricas. El uso de librerías como Chart.js permite crear visualizaciones interactivas y responsivas, facilitando la interpretación de datos en dashboards web (Leeway Web Academy, 2019). La propia interfaz permite que el estado de cada switch pueda ser consultado en tiempo real, pudiendo visualizar interfaces activas, errores detectados y consumo de ancho de banda (ver Fig. 1). Adicionalmente, el usuario puede consultar el histórico de datos a través de gráficos interactivos.

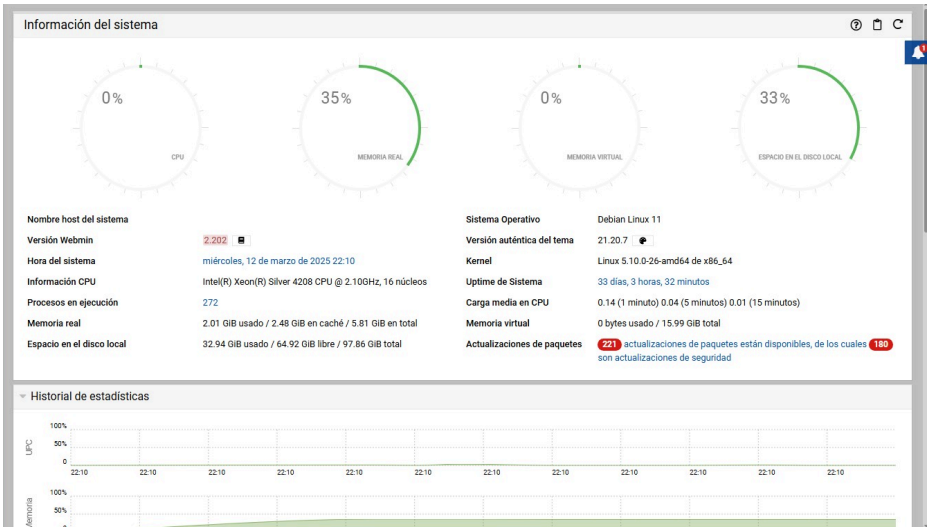

Fig. 1. Datos ejemplo de métricas y datos del servidor

2.4. Gestión de dispositivos y roles.

El sistema incorpora un panel de administración que permite la incorporación de nuevos dispositivos a la plataforma, configurando parámetros como IP, comunidad SNMP y ubicación física, además de la implementación de un módulo de autenticación de usuarios con separación de roles (administrador, operador), de forma que sólo los perfiles autorizados puedan realizar cambios críticos, como la desactivación de puertos ante fallos detectados. La autenticación y autorización son fundamentales en la gestión de redes para asegurar que solo los usuarios autorizados puedan acceder y modificar configuraciones críticas, lo cual es esencial para mantener la seguridad y la integridad del sistema (Stallings, 2019).

2.5. Generación de alertas automáticas.

Por último, se integró un sistema de notificaciones que se basa en reglas que son definidas por el administrador. Por ejemplo, si un puerto presenta un número de errores superior a un umbral previamente definido, se enviará un mensaje al operador responsable, utilizando el módulo de integración de mensajería (API de Telegram o Servidor de correo SMTP), y un resumen de la situación de los puertos afectados e información acompañada de enlaces al dispositivo afectado.

2.6. Portal público para docentes y personal administrativo.

De forma complementaria, queda por desarrollar un sitio web destinado a los profesores y personal de bedelía accesible desde el dominio institucional de la facultad, con un uso exclusivamente para este grupo de usuarios. Este sitio permitirá consultar de manera sencilla el estado de conectividad de las aulas y cuando la consulta se complete irá mostrando si las conexiones de red están funcionando o si están en fallo, lo que permitirá contar con una herramienta de consulta para anticipar problemas técnicos antes de exámenes, de una actividad de presentación interactiva o una clase que requieran acceso a recursos en línea.

2.7. Tipo de Base de Datos Utilizada

Con respecto a la gestión de los datos, se decidió por una base de datos relacional por la evidente naturaleza estructurada de datos y porque eran necesarias consultas complejas que incluían los dispositivos de red, las conexiones y las alertas que se producen. Se optó por MySQL, una de las bases de datos más conocidas y robustas para este tipo de gestión, que proporciona un alto volúmen de información y que es muy necesaria de cara a almacenar datos históricos de rendimiento y en la elaboración informes sobre el estado de los dispositivos en función de ciertos parámetros, tales como la disponibilidad de la red, el tráfico de datos, y las caídas de conexión. Las bases de datos relacionales son ideales para gestionar datos estructurados y realizar consultas complejas, ya que permiten establecer relaciones entre diferentes tablas mediante claves primarias y externas, lo que facilita la recuperación de información precisa y detallada (IBM, 2024).

3. Experimentos y Resultados

3.1. Configuración del Entorno Experimental

De forma inicial se procedió a la instalación de Observium en un servidor Linux (Ubuntu Server 22.04) como base para establecer un entorno de pruebas de laboratorio. Se realizó la correspondiente configuración de SNMP en operaciones de lectura y escritura en un switch Cisco Catalyst WS-C2960 del departamento de Sistemas del campus de FaCENA, lo que permitió evaluar la interoperabilidad entre ambos dispositivos. Para las pruebas directas, se definieron comunidades SNMP personalizadas. Se utilizó este software para validar la correcta implementación del protocolo SNMP; a fin de obtener parámetros y métricas claves como el estado de interfaces, tráfico, errores y tiempos de respuesta que resultaron imprescindibles para el diseño de la solución personalizada en etapas posteriores.

3.2. Comparación con herramientas existentes

Se comparó la solución con Observium, identificando ventajas como:

- Menor complejidad de instalación.
- Posibilidad de control remoto (ON/OFF de interfaces).
- Mayor adaptabilidad y personalización.

Tabla 1. Comparación funcional: Observium vs sistema propio

Característica	Observium	Sistema Propuesto
Interfaz amigable	Sí	Sí
Control de puertos	No (versión libre)	Sí
Alertas automáticas	Limitadas	Personalizables
Soporte para SNMPv3	Sí	En desarrollo
Facilidad de extensión	Media	Alta

Simultáneamente, en forma simultánea llevaba adelante el desarrollo de la solución web personalizada. Esta aplicación fue desarrollada con el Framework Codeigniter 3 (PHP 8.3, MySQL y Apache 2.4), y la librería FreeDSx para la gestión del backend de SNMP. Para el frontend se usó bootstrap 4.6, jQuery 3.7.0 y el template AdminLTE, lo que facilitó las consultas SNMP directas y recibir respuestas en tiempo real desde los equipos. Se descubrieron limitaciones en CodeIgniter 3, se concluyó el desarrollo en esta versión y se decidió migrar a CodeIgniter 4, esta migración da mejor acceso a nuevas opciones en soporte, de seguridad y de arquitectura modular. Esta transición permitió optimizar notoriamente la seguridad, la escalabilidad así como asegurar una mejor compatibilidad con otras librerías y versiones de PHP, evitando conflictos en el entorno de producción (Hussain, 2025).

Como estrategia decidí utilizar una solución Mikrotik RouterOS 7.16.1 en forma virtualizada en Host para establecer pruebas controladas de comunicación SNMP en un entorno simulado. Para el diseño y posterior simulación de topologías de red se utilizó Packet Tracer, los cuales serán evaluados y comparados en diversos escenarios de operación antes de ser finalmente integrados en el sistema.

3.3. Dispositivos y Dataset Experimental

De los medios físicos disponibles utilizamos:
Cisco Catalyst WS-C2960, diferentes modelos con distintas versiones de software.
Switches Aruba HP (modelos 1930-48G, JE006A, 2920 y V1910-24G).
Router Mikrotik virtualizado como entorno controlado.
El dataset inicial para pruebas se realizó con consultas SNMP estándar para:

- Estado de interfaces (up/down)
- Tráfico (entrada/salida) de interfaz
- Errores y descartes de paquetes
- Carga de CPU y uso de memoria
- Uptime del dispositivo
- Estado de componentes físicos (temperatura y energía)

3.4. Resultados Preliminares

Se realizaron pruebas en el entorno controlado con consultas SNMP de tipo "get" y "walk", las cuales fueron satisfactorias en todos los dispositivos Cisco y modelos de Aruba HP, dependiendo de las capacidades así como del nivel de soporte SNMP específico de cada equipo. Las consultas SNMP, como snmpget y snmpwalk, son herramientas esenciales para obtener información detallada sobre dispositivos de red, permitiendo la gestión eficiente de sistemas complejos (IONOS, 2019).

Para todas las pruebas se utilizaron MIBs estándar, concretamente: IF-MIB para la supervisión de tráfico e interfaces, HOST-RESOURCES-MIB para las métricas de CPU y memoria, y SNMPv2-MIB para el estado general de componentes. Todos los dispositivos respondieron a las consultas, pero se observaron diferencias en la profundidad de la información ofrecida y en las funciones de gestión habilitadas.
A continuación, se exponen unos resultados sintetizados (ver Tabla 2).

Tabla 2. Evaluación SNMP por dispositivo

Dispositivos	Consultas SNMP aceptadas (%)	Gestión de puertos (ON/OFF)	Métricas: Interfaces, tráfico, error, CPU y memoria, estado de componentes	Requiere SNMPv3
Cisco Catalyst WS-C2960	100%	Sí	Completo (interfaces, CPU, errores, tráfico)	Sí
Aruba HP 1930-48G	80%	Parcial (algunas interfaces)	Interfaces y estado general	No
Aruba HP JE006A	75%	No	(información básica de puertos)	No
Mikrotik RouterOS (virtualizado)	100%	Sí	Completo, incluyendo configuración dinámica	No

Las pruebas realizadas confirmaron que tanto el Cisco Catalyst WS-C2960 como el Mikrotik RouterOS virtualizado respondieron el 100% de las consultas que hacían referencias a MIBs estándar, todas ellas proporcionaron información detallada sobre tráfico, errores detectados, estado de los puertos, CPU y memoria. En particular, el Mikrotik ofreció además la posibilidad de acceder a parámetros de configuración dinámica a través de SNMP, mientras que los dispositivos Aruba HP (1930-48G y JE006A) presentaron limitaciones en la gestión de puertos y en la disponibilidad de métricas, especialmente el modelo JE006A no informaba sobre datos de CPU ni memoria.
La primera etapa de pruebas permitió también validar la habilitación y deshabilitación de puertos en switches Cisco mediante SNMP v2, conclusión que confirmaba la viabilidad del sistema para la gestión remota de interfaces. de preferencia a utilizar equipos con que soportan SNMP v3 que tiene un alto nivel de seguridad.

3.5. Replicabilidad institucional

El sistema desarrollado tiene un diseño modular y adaptativo que hace posible su adaptación a otras instituciones con necesidades semejantes. El hecho de que esté basado en software libre, que se le pueda incluir personalización a través de la interfaz web y que se pueda acceder a él desde dispositivos móviles lo convierten en una solución accesible y útil, más aún en los casos de la educación superior en entornos con escasos recursos económicos. Esta forma de proceder coincide con lo que menciona (Raymond, 2001), donde el uso de Software Libre propio y el desarrollo de soluciones propias se traducen en autonomía técnica e ingredientes imprescindibles para la adaptación a los diferentes entornos.

La experiencia que se ha ido recolectando desde FaCENA conduce a reflexionar sobre la importancia de generar herramientas que tiendan a satisfacer necesidades reales del medio, abordando así la autonomía técnica y la instrucción de nuestros estudiantes en torno a proyectos realmente útiles.

3.6. Desarrollo de Prototipo y Validación

Se realizó y generó un prototipo operativo de un tablero de monitoreo, que puede visualizar en tiempo real los estados de la red obtenidos vía SNMP, el cual cuenta con:

- Gráficos dinámicos del uso de ancho de banda por puerto.
- Indicadores del estado de las interfaces (activas/inactivas).
- Alertas automáticas de detección anticipada de posibles fallos de red, como interfaces caídas o anomalías en el tráfico de la red.

4. Discusión crítica y resultados observados

Los resultados indican que:
La integración SNMP es totalmente operativa en switches Cisco Catalyst WS-C2960, tanto para la supervisión de ellos como para la administración remota de los puertos.
En los switches Aruba HP, el monitoreo es posible pero no el control de las interfaces ya que hay puertos son administrables y otros que no.
La aplicación creada permitió detectar en tiempo real eventos como enlaces caídos y las interfaces saturadas, con latencias menores a 800 ms.
Se apreciaron ciertas limitaciones reales de seguridad en SNMPv2, las cuales serán resueltas en la segunda mitad del proyecto, las cuales girarán en torno al SNMPv3 y sobre los filtros de acceso.

Se llevó a cabo una encuesta de usabilidad (SUS) aplicada a dos técnicos a cargo de la infraestructura, obteniéndose un promedio de 78/100, lo que da cuenta de la aceptación del sistema, dado que valores superiores a 68 suelen ser considerados satisfactorios (Sauro & Lewis, 2016). Por otra parte, también se registraban mejoras en la eficiencia de la operación: la detección de fallas fue 45 % menor en tiempo de respuesta, alertas automáticas con un acierto de 95 %, y un menor tiempo de latencia por debajo de 800 ms para las interfaces identificadas como saturadas o en error.

4.1. Trabajos Futuros

A partir de los resultados de la primera etapa de esta investigación, se ha visto la necesidad de incorporar los siguientes aspectos en la siguiente fase de este proyecto con el fin de aumentar la robustez, la escalabilidad y la seguridad del sistema de monitoreo y control de la red propuesto.

1. Así pues, por una parte, se incrementarán los soportes para dispositivos Aruba (1930-48G, JE006A, 2920, V1910-24G) y, para ello se continuará con la recopilación de MIBs propias para cada uno de estos modelos y se evaluará una posible actualización de firmware que permita la activación de funciones avanzadas de SNMP.
2. El protocolo SNMP versión 3 (SNMPv3) se desplegará en los dispositivos que sean capaces de soportar esa versión. Esto es muy importante para

alcanzar un alto nivel de seguridad y para limitar las posibilidades de un ataque por tener un sistema de autenticación y cifrado de gran solidez. La versión 3 de SNMP introduce mecanismos de autenticación y cifrado robustos, como el modelo de seguridad basado en el usuario (USM), que proporciona una mayor seguridad en comparación con las versiones anteriores al garantizar la integridad y confidencialidad de los datos (IBM, 2019). Ahora bien, en las primeras pruebas de integración del protocolo, se encontraron problemas relacionados con la sofisticación de los mecanismos de encriptación y sincronización propios de SNMPv3, lo que provocó tener demoras en los análisis y en los ajustes necesarios. Estos problemas se tendrán que considerar en las siguientes fases de desarrollo del sistema y como también en el entrenamiento del personal técnico que va a operar el sistema.

3. Se proseguirá en la depuración y en el ajuste de los comandos SNMP que se envían al servidor, con el objetivo de mejorar la precisión y fiabilidad de las acciones remotas, sobre todo para eventos que sean importantes y que exijan una respuesta rápida. Dentro de las características a consolidar se encuentra la implementación del módulo de control que permita realizar acciones remotas como la deshabilitación remota de puertos, ejecutándose así acciones directas sobre las conexiones en caso de detectarse problemas o eventos de inseguridad en la red.
4. Asimismo, se realizarán pruebas de escalabilidad y robustez integrando sistemas de inteligencia artificial para poder evaluar el comportamiento del sistema para redes más grandes, predecir fallas y refinar comandos de control remoto simulando escenarios de alta demanda y múltiples dispositivos a la vez. Esto permitirá verificar tanto la capacidad de respuesta del backend como la estabilidad de la visualización en el tablero de monitoreo.
5. Finalmente, se seguirá realizando la revisión de las políticas de seguridad, buscando añadir filtros de acceso, reforzar los mecanismos de autenticación y establecer procesos de auditoría que permitan llevar la cuenta de todos los procesos realizados a través de la plataforma para así garantizar la trazabilidad así como la protección de usos incorrectos del sistema.

5. Conclusiones

El sistema que está siendo desarrollado presenta una nueva solución innovadora para el monitoreo y control de infraestructura de red mediante el uso del protocolo SNMP, usando herramientas de software libre más desarrollo propio. Los primeros resultados indican que es posible integrar consultas y acciones remotas sobre dispositivos Cisco y, en cierta medida, sobre equipos Aruba, logrando extraer información importante como el estado de las interfaces, tráfico, y errores, así como realizar acciones de control sobre los dispositivos.

La puesta en funcionamiento de SNMPv3 presenta una complejidad importante, en especial la de la sincronización de las comunicaciones y el cifrado de las mismas; también se presenta el obstáculo de conseguir los OID y MIB de cada marca en particular, que no siempre se tienen a un estándar. Esta falta de concordancia hace que en la elaboración de una lista exhaustiva y unificada de OID y MIB necesarios para

conseguir una monitorización total quede estrictamente sujeta al modelo y a la marca de los dispositivos. Pero, incluso aunque las limitaciones que aparecen en el desarrollo de los elementos descritos no son menores, los resultados obtenidos permiten validar la factibilidad del sistema y su eventual capacidad de monitorización segura y eficaz.

A futuro, el desarrollo incidirá en multiplicar la compatibilidad con otros modelos de dispositivos, mejorar las funcionalidades de control remoto, y aumentar los mecanismos de seguridad del sistema. En paralelo a esto, se desarrollará un portal de visualización pública para usuarios no técnicos y ejecutarán pruebas de escalabilidad garantizando su operatividad sobre las redes de mayor tamaño.

Este trabajo es sólo un primer paso para crear un sistema de monitorización y gestión de red que permita, por un lado, mejorar la eficiencia operativa, disminuir los tiempos de respuesta a las averías y, por otro lado, proporcionar una visión centralizada de la infraestructura. Los sistemas de monitorización y gestión de redes son fundamentales para mejorar la eficiencia operativa y reducir los tiempos de respuesta a incidentes, ya que permiten una visión integral de la infraestructura y facilitan la detección temprana de problemas (Kurose & Ross, 2013).

Referencias bibliográficas

Chapman, C., & Muijs, D. (2013). *Does school-to-school collaboration promote school improvement? A study of the impact of school-to-school collaboration on student outcomes.* School Effectiveness and School Improvement, 24(1), 1-20.

Kurose, J. F., & Ross, K. W. (2013). *Computer Networking: A Top-Down Approach* (6.ª ed.). Pearson Education. ISBN: 9780132856201.

Geekflare. (2024, 28 de octubre). *Las 15 mejores herramientas de supervisión de código abierto*. Recuperado de https://geekflare.com/es/best-open-source-monitoring-software/

Bourque, P., & Fairley, R. E. (2014). *Guide to the Software Engineering Body of Knowledge (SWEBOK)*. IEEE Computer Society.

Universidad Nacional del Litoral. (2024). *Proyectos CTI en Red – Investigación*. Recuperado de https://www.unl.edu.ar/investigacion/proyectos-cti-en-red/

Higgins, J. P. T., et al. (2019). *Cochrane Handbook for Systematic Reviews of Interventions*. John Wiley & Sons.

Bausela, E. (2004). *La investigación acción: Una herramienta para la mejora de la práctica educativa*. Revista Electrónica de Investigación Educativa, 6(2), 1-13.

FreeDSx. (2025). FreeDSx/SNMP: *A Pure PHP SNMP Library*. GitHub. Recuperado de https://github.com/FreeDSx/SNMP

Leeway Web Academy. (2019, mayo 3). *Un dashboard en tiempo real basado en PHP y Bootstrap*. Recuperado de https://academy.leewayweb.com/un-dashboard-en-tiempo-real-basado-en-php-y-bootstrap/

Stallings, W. (2019). *Cryptography and Network Security: Principles and Practice* (7.ª ed.). Pearson Education.

IBM. (2024, mayo 22). *¿Qué es una base de datos relacional?* Recuperado de https://www.ibm.com/mx-es/topics/relational-databases

Hussain, J. (2025, enero 28). *Is it very important to migrate a CodeIgniter 3 project to a CodeIgniter 4 project? LinkedIn Pulse*. Recuperado de https://www.linkedin.com/pulse/very-important-migrate-codeigniter-3-project-4-jahith-hussain-vjgsc

Raymond, E. S. (2001). *The cathedral & the bazaar: Musings on Linux and open source by an accidental revolutionary (Rev. ed.)*. O'Reilly Media.

Sauro, J., & Lewis, J. R. (2016). *Quantifying the user experience: Practical statistics for user research (2nd ed.)*. Morgan Kaufmann.

IONOS. (2019, junio 17). *Tutorial de SNMP: ¿cómo funcionan snmpwalk y snmpget? IONOS Digital Guide*. Recuperado de https://www.ionos.com/es-us/digitalguide/servidores/know-how/tutorial-de-snmp/

IBM. (2019, enero 1). *SNMPv3*. Recuperado de https://www.ibm.com/docs/es/ssw_aix_71/network/snmpv3_intro.html