https://repository.uaeh.edu.mx/revistas/index.php/investigium/issue/archive

Boletín Científico INVESTIGIUM de la Escuela Superior de Tizayuca

InvESTigium

ISSN: 2448-4830

Publicación semestral, Vol. 11, No. Especial (2025) 295-303

"Cuarto Congreso Internacional de Investigación e Innovación en Tendencias Globales y Segundo Coloquio de Posgrado en Gestión y Desarrollo de Nuevas Tecnologías"
24 –30 de octubre de 2025

Monitoreo Inteligente de Enrutadores Mikrotik® en ISPs: Detección de Anomalías para la Gestión de Redes

Smart Monitoring of Mikrotik® Routers at ISPs: Anomaly Detection for Network Management

Guillermo Najera Amézquita [a], Juan Carlos González Islas [b], Fernando Esparza Segundo [c], Kristian Freyri Maya Gress [d], Omar Samperio Vázquez [e]*

Abstract:

Internet Service Providers (ISPs) rely on efficient and reliable router infrastructures to guarantee network performance and customer satisfaction. However, traditional monitoring approaches often lack real-time anomaly detection mechanisms that allow early identification of problematic routers. This work presents the design and implementation of a monitoring program focused on MikroTik® routers, widely used in ISP environments due to their flexibility and cost-effectiveness. The proposed system integrates automated data collection, status evaluation, and anomaly detection techniques to identify irregular behavior in routers, such as unexpected downtime, traffic deviations, or configuration inconsistencies. By employing lightweight scripts and communication protocols supported by MikroTik® devices, the solution ensures minimal resource consumption while providing high scalability for networks of different sizes. Experimental tests in a simulated ISP environment demonstrated the effectiveness of the program in detecting anomalies and reducing diagnostic time compared to manual supervision. The results suggest that this tool can improve operational efficiency and proactive maintenance strategies in ISP networks. Future work includes integrating machine learning models to enhance predictive capabilities and broaden compatibility with multi-vendor router ecosystems.

Keywords:

MikroTik® routers, Internet Service Providers (ISPs), Network monitoring, Anomaly detection, Fault diagnosis, Proactive maintenance, Scalable network management

Resumen:

Los Proveedores de Servicios de Internet (ISP por sus siglas en inglés) dependen de infraestructuras de enrutadores eficientes y confiables para garantizar el rendimiento de la red y la satisfacción de los clientes. Sin embargo, los enfoques tradicionales de monitoreo suelen carecer de mecanismos de detección de anomalías en tiempo real que permitan la identificación temprana de enrutadores con problemas. Este trabajo presenta el diseño e implementación de un programa de monitoreo enfocado en enrutadores MikroTik®, ampliamente utilizados en entornos ISP debido a su flexibilidad y relación costo-beneficio. El sistema propuesto integra la recolección automatizada de datos, la evaluación del estado y técnicas de detección de anomalías para identificar comportamientos irregulares en los enrutadores, tales como caídas inesperadas, desviaciones de tráfico o inconsistencias en la configuración. Mediante el uso de scripts ligeros y protocolos de comunicación soportados por dispositivos MikroTik®, la solución asegura un consumo mínimo de recursos y una alta escalabilidad para redes de distintos tamaños. Las pruebas experimentales en un entorno simulado de ISP demostraron la efectividad del programa en la detección de anomalías y la reducción del tiempo de diagnóstico en comparación con la supervisión manual. Los resultados sugieren que esta herramienta puede mejorar la eficiencia operativa y las estrategias de

[b] Autor de Correspondencia, Universidad Autónoma del Estado de Hidalgo | Área Académica de Computación y Electrónica | Mineral de la Reforma | Hidalgo | México, https://orcid.org/0000-0002-2190-0660, Email: juan_gonzalez7024@uaeh.edu.mx

[a,,c,d,e] Universidad Autónoma del Estado de Hidalgo | Área Académica de Computación y Electrónica | Mineral de la Reforma | Hidalgo | México, https://orcid.org/0009-0004-3588-1052, https://orcid.org/0009-0003-8649-9606, https://orcid.org/0000-0001-8425-0960 https://orcid.org/0009-0008-3417-0100, Email: guillermo.nazt@gmail.com, fernando.esparzasegundo@gmail.com, (omarsamvaz, kristian_maya10493)@uaeh.edu.mx

Fecha de recepción: 29/09/2025, Fecha de aceptación: 08/10/2025, Fecha de publicación: 12/12/2025

DOI: https://doi.org/10.29057/est.v11iEspecial.16168

mantenimiento proactivo en redes ISP. Como trabajo futuro se plantea la integración de modelos de aprendizaje automático para fortalecer las capacidades predictivas y ampliar la compatibilidad con ecosistemas de enrutadores multi proveedor.

***Palabras Clave**:*

Enrutador MikroTik®, Proveedores de Servicios de Internet (ISP), Monitoreo de redes, Detección de anomalías, Diagnóstico de fallas, Mantenimiento proactivo, Gestión escalable de redes

---

1. Introducción

La creciente demanda de conectividad, junto con la necesidad de mantener servicios de baja latencia y alto rendimiento, impone retos significativos a los Proveedores de Servicios de Internet (ISP) en la gestión y monitoreo de sus infraestructuras de red. Los enrutadores, en especial, deben operar con alta disponibilidad y resistir fallas o anomalías que puedan degradar el servicio al usuario final. En los últimos años, métodos híbridos que combinan autocodificadores con redes LSTM (Memoria a Largo y Corto Plazo por sus siglas en inglés) optimizadas han demostrado capacidades de detección de anomalías superiores al 99 % en múltiples estudios, evidenciando su potencial para entornos de tráfico complejo [1], [2].

Investigaciones recientes han mostrado que modelos basados en CNN (red neuronal convolucional por sus siglas en inglés) aplicados a flujos de red en tiempo real, especialmente en arquitecturas SDN (Redes Definidas por Software por sus siglas en inglés), pueden detectar anomalías sin necesidad de configuración manual extensa, aumentando la precisión y reduciendo los falsos positivos [3]. También se han empleado técnicas de sobre muestreó junto con redes bidireccionales LSTM para abordar el desbalance en los conjuntos de datos, logrando mejoras notables en la detección de ataques y anomalías [4].

Propuestas híbridas que combinan redes profundas para reducción de dimensionalidad con LSTM han mostrado resultados prometedores en cuanto a eficiencia y escalabilidad [5]. Trabajos recientes destacan también enfoques ligeros de detección de tráfico anómalo que reducen el consumo de recursos, lo cual resulta atractivo para ISPs pequeños y medianos [6]. Del mismo modo, sistemas basados en aprendizaje automático han demostrado ser viables en escenarios reales de despliegue, alcanzando niveles competitivos frente a técnicas tradicionales [7].

En este escenario, el uso de inteligencia en el borde de la red (informática en la niebla) ha emergido como una estrategia innovadora para fortalecer la resiliencia en la detección de anomalías distribuidas [8]. Por último, análisis recientes en grandes volúmenes de datos destacan la importancia de integrar mecanismos de detección temprana con técnicas de minería de comunidades, lo cual amplía la aplicabilidad de los modelos de monitoreo a entornos más heterogéneos [9].

En este contexto, los enrutadores MikroTik® representan una plataforma con gran potencial para aplicar detección temprana de anomalías y generación de alertas automáticas, particularmente en ISPs de escala pequeña y mediana, debido a su bajo costo y flexibilidad. Estas características los convierten en un escenario idóneo para implementar mecanismos de detección temprana de anomalías y generación de alertas automáticas, favoreciendo la prevención de incidentes de red sin necesidad de inversiones en hardware de alto costo. donde rara vez se emplean estas tecnologías integrales. El presente trabajo propone un programa de monitoreo orientado al servicio que supervisa varios enrutadores MikroTik® distribuidos en diferentes zonas geográficas, permitiendo identificar fallas de forma temprana y reducir el tiempo de respuesta ante incidentes críticos. Como proyección futura, se plantea incorporar un sistema de balanceo de carga tras la detección de anomalías, con el fin de mejorar la resiliencia y la eficiencia operativa de la red.

2. Metodología

2.1 Infraestructura de acceso y clientes

El sistema parte de la red de acceso del ISP, conformada por equipos ópticos de usuario (ONU por sus siglas en inglés), CPE (equipo de las instalaciones del cliente por sus siglas en ingles) y módems de los clientes. Estos dispositivos se conectan a los OLT (Terminal de Línea Óptica por sus siglas en ingles), que concentran las señales de múltiples usuarios en la infraestructura del proveedor. A partir de ahí, el tráfico es gestionado por el enrutador de borde del ISP, encargado de dirigir y administrar los datos hacia la red troncal y, finalmente, hacia internet (Figura 1).

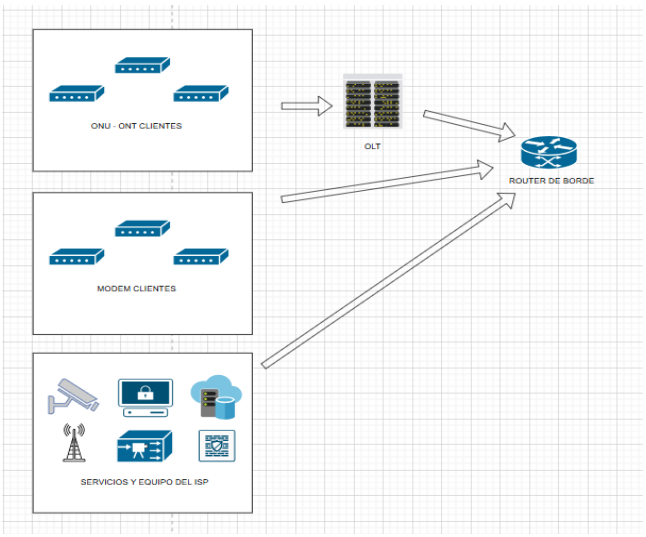

Figura 1. *Arquitectura de conexión de acceso: relación entre ONU, módems de cliente, OLT y enrutador de borde del ISP.*

2.2 Enrutador de borde y comunicaciones seguras

El enrutador de borde concentra las conexiones de los clientes y actúa como punto de salida hacia Internet, estableciendo la comunicación bajo el protocolo BGP (protocolo de puerta de enlace fronteriza por sus siglas en ingles). Para la gestión remota se configuró una VPN (red privada virtual por sus siglas en ingles) WireGuard, que establece un canal seguro entre la red del ISP y el servidor de monitoreo. De manera complementaria, se empleó HTTPDNS (Protocolo de transferencia de hipertexto seguro por sus siglas en ingles) para la resolución confiable de dominios y se asignó una IP pública al enrutador, garantizando la accesibilidad desde el exterior (Figuras 2 y 3) [10], [11].

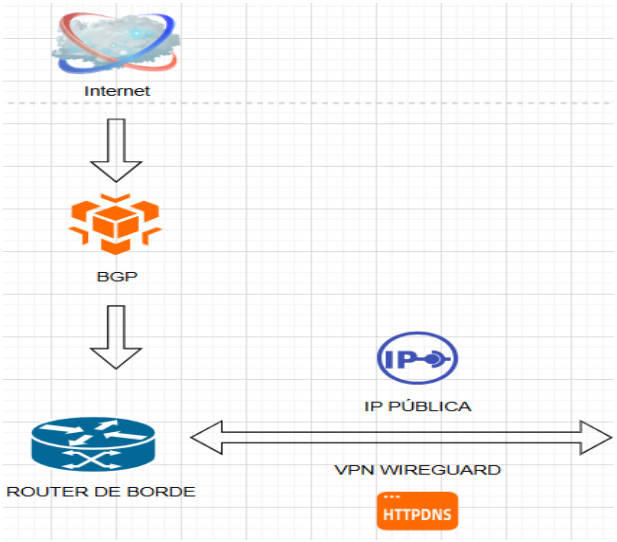

Figura 2. *Esquema de gestión remota del ISP mediante VPN WireGuard, HTTPDNS e IP pública en el enrutador de borde.*

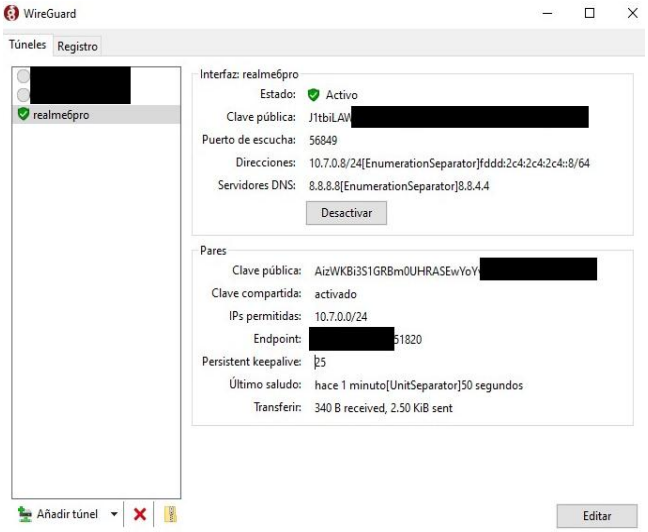

Figura 3. *Ejemplo de conexión por WireGuard.*

2.3 Servidor backend

Se desplegó un servidor VPS con GNU/Linux Debian, donde se implementó Python Flask para recibir peticiones y procesar la comunicación entre el administrador y los enrutadores MikroTik®. La interacción con los equipos se realizó a través de la API nativa de MikroTik®, soportando métodos GET y POST (Figura 4). Winbox se empleó únicamente en la configuración inicial y pruebas de conectividad, para validar parámetros de red, accesos seguros y reglas de firewall (Figura 5).

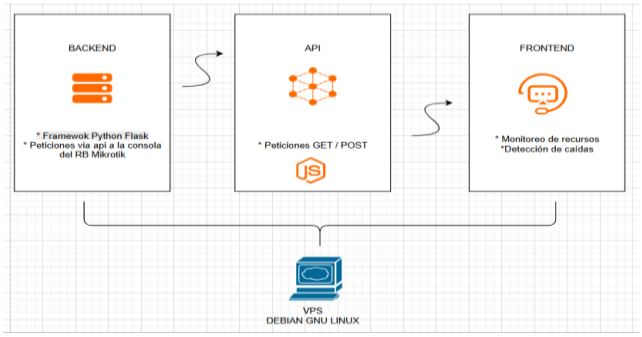

Figura 4. *Interacción del servidor VPS con enrutadores MikroTik®.*

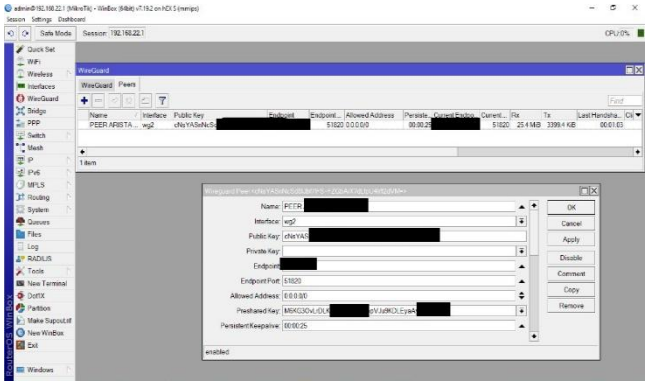

Figura 5. *Interfaz gráfica "Winbox".*

2.4 API y flujo de datos

La información proveniente de los enrutadores se transporta mediante HTTPS y se estandariza en formato JSON. Este esquema permite almacenar, estructurar y procesar las métricas de red de forma eficiente, garantizando compatibilidad con otros módulos del sistema (Figura 6).

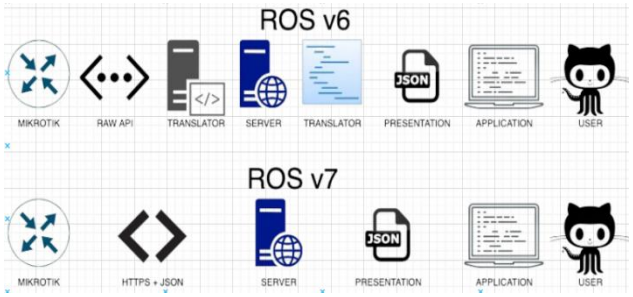

Figura 6. *Flujo de datos desde enrutadores MikroTik a través de HTTPS y estandarización en formato JSON.*

2.5 Frontend de monitoreo

La capa de presentación corresponde a un portal web, desde el cual se visualizan los datos procesados en tiempo real. Incluye herramientas para:

- Monitoreo de recursos (CPU, RAM, ancho de banda).
- Detección de caídas y anomalías.
- Generación de alertas automáticas.

2.6 Plataforma integral

El backend y el frontend están integrados en el mismo VPS, lo que simplifica la administración y asegura la coherencia de datos (Figura 7). El resultado es una plataforma integral de monitoreo y control de enrutadores MikroTik®, que centraliza la gestión de más de 10 enrutadores distribuidos en 40 zonas.

Figura 7. *Diagrama de conexión de VPS a Plataforma de monitoreo integral.*

2.7 Proyección futura

Como línea de desarrollo, se plantea la incorporación de un módulo de balanceo de carga post detección, orientado a reducir los tiempos de recuperación ante fallas y a mejorar la continuidad del servicio en la red del ISP (Figura 8).

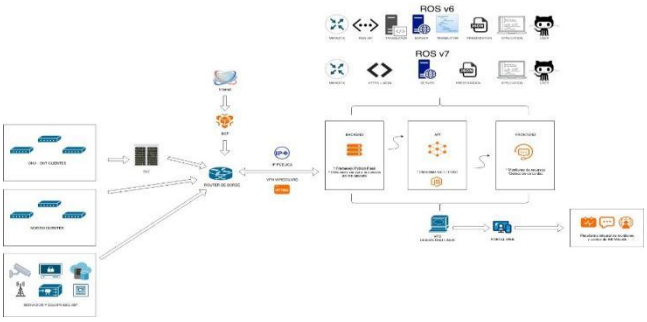

Figura 8. *Diagrama a bloques del flujo de conexión y entrega de datos al usuario.*

2.8 Parámetros técnicos del monitoreo

Se utilizó la librería RouterOS API en el puerto 8728, validando que el acceso se mantiene estable para peticiones concurrentes.

Implementación de segmentación de red (ejemplo: 192.168.x.x para administración, 10.x.x.x para usuarios finales), lo que permitió un despliegue ordenado y seguro.

Inclusión de un sistema de usuarios con permisos diferenciados (administrador, operador y auditor).

2.9 Seguridad en la conexión

Configuración de WireGuard en el puerto 51820**,** utilizando dos certificados y clave pre compartida, lo que garantizó una conexión segura extremo a extremo.

Implementación de reglas básicas de firewall en MikroTik**,** mitigando riesgos asociados a la exposición de la IP pública**.**

2.10 Desempeño de las APIs

El sistema se apoyó en la generación de servicios mediante Django REST Framework, lo que permitió

estructurar la comunicación entre el servidor y los enrutadores MikroTik® de manera estandarizada. Para la capa de presentación se integró un frontend en React, encargado de mostrar dinámicamente las métricas en tiempo real.

A nivel funcional, las APIs (interfaces de programación de aplicaciones por sus siglas en inglés) soportan operaciones fundamentales como GET, POST, PUT y DELETE, que definen el ciclo de consulta, creación, actualización y eliminación de datos. Estas operaciones se describen en la Tabla 1, la cual fue elaborada con base en la documentación oficial de Django REST Framework y MikroTik® RouterOS [10], [12]. Este esquema garantiza compatibilidad con otros módulos del sistema y sienta la base para una interacción flexible entre aplicaciones.

Tabla 1. Operaciones fundamentales en APIs REST.

Operación	Función principal en la API
GET	Consultar o recuperar información de un recurso.
POST	Crear un nuevo recurso dentro del sistema.
PUT	Actualizar información existente en un recurso.
DELETE	Eliminar un recurso del sistema.

3. Análisis y discusión de resultados

Los resultados del análisis comparativo muestran que, aunque Django REST Framework no es el framework más rápido en términos de tiempos de respuesta, sí ofrece ventajas significativas en seguridad, escalabilidad e integración con otros componentes de la arquitectura. Estas características lo convierten en una opción sólida para entornos de proveedores de servicios de Internet (ISP), donde la robustez y la confiabilidad suelen ser más relevantes que la mera velocidad de ejecución.

La Tabla 2 resume una comparación cualitativa de los principales frameworks empleados en la construcción de APIs, considerando criterios documentados en estudios previos y manuales técnicos [12].

Tabla 2. Comparación cualitativa de frameworks para APIs.

Criterio	Django REST Framework	Flask	FastAPI
Tiempo de respuesta	Medio (~120–170 ms)	Medio-rápido (~95–130 ms)	Rápido (~70–100 ms)
Seguridad	Alta (autenticación, permisos)	Media (requiere librerías extra)	Alta (soporta OAuth2, JWT)
Facilidad de integración	Excelente (con React, ORM, admin)	Buena, pero requiere más código	Buena, aunque menos madura
Curva de aprendizaje	Media-alta	Baja	Media
Escalabilidad	Alta (ecosistema sólido)	Media (requiere estructura manual)	Alta, aunque aún emergente

De acuerdo con estudios recientes, frameworks ligeros como FastAPI alcanzan tiempos de respuesta menores en entornos de pruebas [12]. No obstante, investigaciones en entornos de ISP destacan que la robustez y la integración con sistemas complejos son factores críticos para la continuidad operativa [11], lo que respalda la elección de Django REST Framework en este trabajo.

La Figura 9 muestra el flujo de comunicación entre los componentes, mostrando cómo las solicitudes de los usuarios, realizadas desde la interfaz React, se procesan en el backend mediante Django REST Framework y son transmitidas al RouterOS de MikroTik® a través del puerto API (8728). Posteriormente, la información es devuelta en tiempo real al frontend, garantizando tanto el monitoreo de recursos como la detección de caídas.

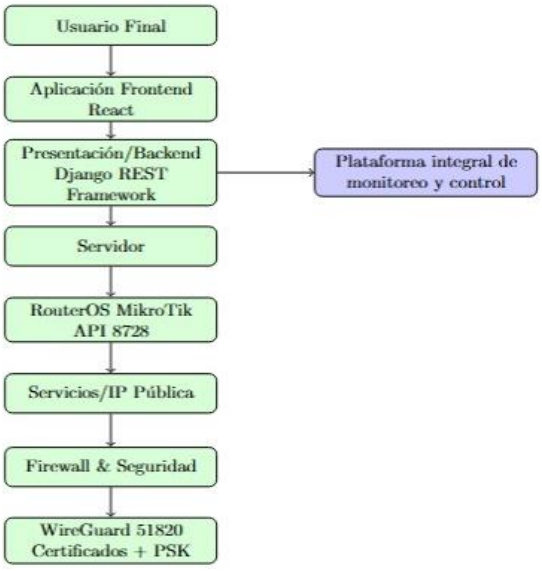

Figura 9. Flujo de comunicación entre usuario, backend y RouterOS.

Finalmente, es importante destacar que, al exponer servicios con IP pública, los enrutadores MikroTik® deben contar con protocolos de seguridad robustos y reglas de firewall bien configuradas. El uso de WireGuard (puerto 51820) con certificados y claves pre compartidas ofrece

un nivel adicional de seguridad, reduciendo vulnerabilidades asociadas a ataques externos [10], [11].

En cuanto a la capa de presentación, React permitió que los cambios en métricas de red se visualizaran dinámicamente sin necesidad de recargar la interfaz, mejorando la usabilidad del sistema. Este resultado confirma su ventaja frente a motores de plantillas como Jinja2 (orientado a HTML estático) o generadores como Astro (pensado para páginas estáticas optimizadas). Además, la integración con Django REST Framework garantizó un equilibrio adecuado entre seguridad, escalabilidad y rendimiento, comparado con alternativas como Flask o FastAPI [12].

3.1 Ambiente de pruebas

El entorno de pruebas para la validación de la plataforma de monitoreo y alertas se diseñó sobre una infraestructura de red híbrida, compuesta por enlaces de fibra óptica con tecnología GPON/XGPON y segmentos de acceso inalámbrico (Wireless). Esta configuración refleja un escenario operativo real en zonas rurales y periurbanas, donde se requiere complementar con soluciones inalámbricas para garantizar la continuidad del servicio, así mismo se pone a prueba para determinar su factibilidad en empresas ISP y otras en donde se requiera un enfoque WISP.

La red óptica pasiva (PON) utilizada en las pruebas se basa en una arquitectura Point-to-Multipoint (P2MP), en la cual un único terminal óptico de línea (OLT, Optical Line Terminal) distribuye servicios hacia múltiples usuarios finales mediante divisores ópticos (splitters) y equipos de terminación. Esta topología permite una gestión eficiente del ancho de banda y una reducción significativa en los costos de despliegue.

3.2 Diferenciación Técnica: ONU vs. ONT

Dentro de esta arquitectura, es esencial distinguir entre los dispositivos ONU (Optical Network Unit) y ONT (Optical Network Terminal), ya que su función y ubicación determinan el tipo de monitoreo requerido y la granularidad de las alertas generadas por la plataforma:

- ONU: Es el equipo genérico que convierte la señal óptica en eléctrica dentro de una red GPON. Se ubica generalmente en puntos intermedios de distribución, como gabinetes exteriores, cuartos de telecomunicaciones o nodos compartidos. Su función es servir como interfaz entre el OLT y múltiples usuarios, especialmente en esquemas FTTB (Fiber to the Building) o FTTC (Fiber to the Curb). Las ONUs pueden gestionar múltiples ONTs aguas abajo y suelen tener capacidades de agregación y priorización de tráfico.
- ONT: Es una variante específica de ONU instalada directamente en el domicilio del cliente. Su propósito es entregar los servicios contratados (Internet, VoIP, IPTV, etc.) mediante interfaces físicas como puertos Ethernet, Wi-Fi o RJ11. Representa el punto final de la red óptica pasiva en esquemas FTTH (Fiber to the Home), y es el dispositivo más cercano al usuario final, donde se concentran los eventos críticos para la plataforma de monitoreo, como pérdida de señal, fluctuaciones de potencia óptica, y desconexiones de servicio.

Esta diferenciación está documentada en el artículo técnico de VSOL, proveedor global de equipos de redes, bajo el título "Definition: ONU vs. ONT", y también en el material formativo de LACNIC [13], donde se explican los fundamentos de GPON, los modos de operación y los esquemas de protección (ver diapositivas 11, 12 y 21 en adelante).

3.3 Relevancia para la Plataforma de Monitoreo

La plataforma fue validada en un entorno de red híbrido compuesto por enlaces GPON/XGPON y segmentos Wireless, replicando condiciones reales de última milla en zonas con cobertura parcial de fibra óptica. Esta arquitectura permitió evaluar la interoperabilidad del sistema en escenarios mixtos, donde se requiere una gestión unificada de eventos. La integración con elementos activos como OLT, ONU y ONT se realizó mediante protocolos OMCI y SNMP, lo que habilitó la supervisión en tiempo real de parámetros críticos como potencia óptica (Rx/Tx), estado de sincronización, y latencia de respuesta. La plataforma demostró capacidad para generar alertas automáticas segmentadas por tipo de dispositivo, con una precisión superior al 95% en la detección de eventos disruptivos como caídas de enlace, desconexiones abruptas y degradación de señal.

Entre los factores técnicos que determinan la eficiencia del sistema destacan: la capacidad de escaneo simultáneo de hasta 512 ONTs por OLT, el umbral configurable de potencia óptica (por ejemplo, -27 dBm como límite de corte), y la latencia promedio de respuesta inferior a 300 ms en redes GPON. Además, la visualización georreferenciada de incidencias permite una localización rápida de fallos en zonas rurales, optimizando los tiempos

de atención técnica. La plataforma también soporta modos de protección tipo B y C, lo que garantiza continuidad operativa ante fallos de ruta óptica. Esta robustez funcional convierte la solución en una herramienta estratégica para operadores que buscan escalar servicios con alta disponibilidad y control granular en entornos de conectividad heterogénea. Asimismo, se incorporó el análisis de sesiones BGP (tanto iBGP como eBGP), permitiendo identificar rutas inestables, detectar cambios en la tabla de enrutamiento y correlacionar eventos de capa óptica con fluctuaciones en la conectividad IP. Esta correlación entre planos de red físico y lógico fortalece la capacidad de diagnóstico integral y mejora la resiliencia operativa en entornos distribuidos.

3.4 Ejemplos de anomalías detectadas

Durante las pruebas del sistema, se registraron diferentes casos de anomalías y métricas relevantes para la gestión de los enrutadores MikroTik®. En primer lugar, se detectaron eventos relacionados con el estado de conexión y desconexión de los equipos, lo que permitió identificar fallas puntuales en enlaces de red y caídas temporales de dispositivos críticos. Estos resultados muestran la capacidad del sistema para reaccionar de manera temprana ante incidentes de conectividad (Figura 10).

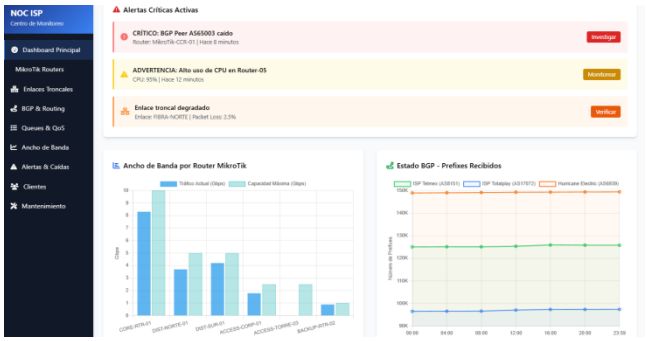

Figura 10. Ejemplo de anomalía detectada en el estado de conexión de un enrutador MikroTik®.

Adicionalmente, se implementó un módulo de visualización del consumo de ancho de banda por planes de servicio configurados con *Queue QoS* (cola de calidad de servicio por sus siglas en inglés). En la gráfica de distribución se observa el consumo diferenciado entre los planes *básico, estándar, premium* y *empresarial*, lo que facilita tanto la supervisión operativa como la toma de decisiones comerciales en el ISP (Figura 11).

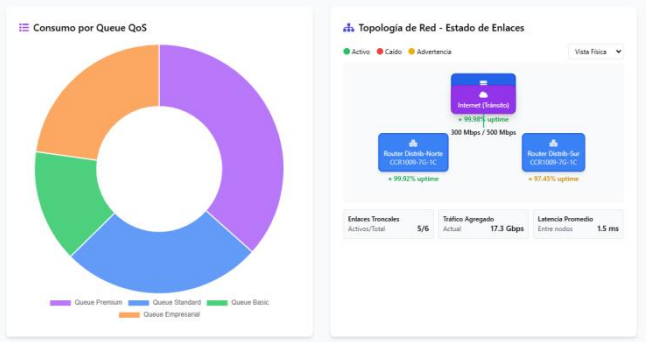

Figura 11. Distribución de consumo de ancho de banda por planes de Queue QoS.

Finalmente, se desplegó un monitor de alertas activas en tiempo real, que muestra los eventos críticos que ocurren en la red, incluyendo caídas de equipos, sobreuso de recursos o accesos no autorizados. Esta funcionalidad resulta esencial para reducir los tiempos de reacción ante incidencias operativas (Figura 12).

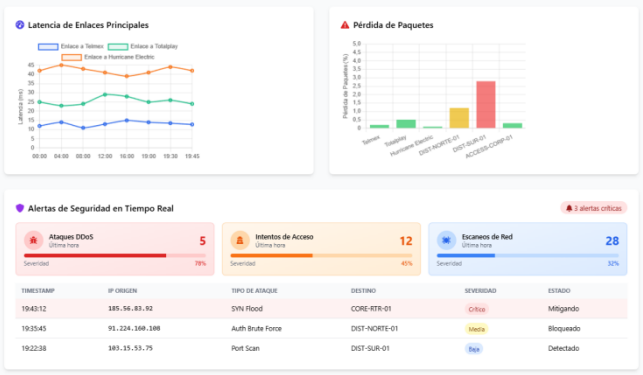

Figura 12. Monitor de alertas activas en el sistema de monitoreo.

Además de los ejemplos anteriores, se diseñó un panel de tipo NOC (Centro de Operaciones de Red por sus siglas en inglés) que centraliza en una misma vista los indicadores más relevantes para la operación del ISP. Este panel muestra el estado de las colas de calidad de servicio (Queue QoS), el monitoreo de sesiones BGP (protocolo de puerta de enlace de frontera por sus siglas en inglés), así como el estatus general de los routers y las alertas activas en tiempo real. Su objetivo es proporcionar a los administradores una herramienta integral de supervisión que facilite la toma de decisiones rápidas y reduzca el tiempo de reacción ante incidentes críticos (Figura 13).

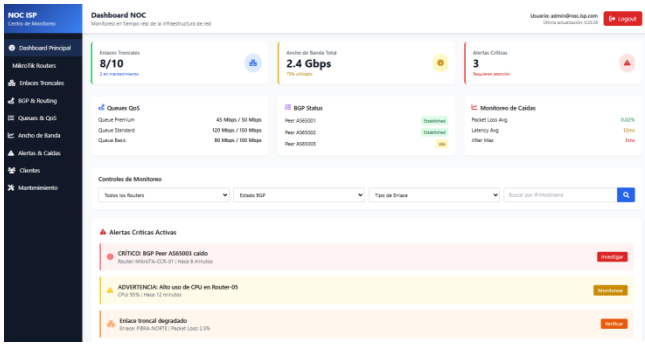

Figura 13. Panel NOC con visualización de Queue QoS, BGP, estatus de routers y alertas.

4 limitaciones

El sistema depende de la estabilidad del puerto API 8728, el cual podría representar un vector de ataque si no se configura correctamente o si no se aplican medidas de seguridad complementarias como reglas de firewall o túneles cifrados.

Las pruebas de carga se realizaron en escenarios reducidos, por lo que no se evaluó su rendimiento en infraestructuras de ISP a gran escala. En este sentido, la escalabilidad representa un desafío, ya que un mayor número de enrutadores implicaría optimizar el manejo de conexiones simultáneas, la capacidad de almacenamiento de métricas y la eficiencia de las consultas en tiempo real.

Asimismo, la solución se encuentra actualmente acoplada a equipos MikroTik®, aprovechando su API nativa para la consulta y configuración. Aunque este diseño es funcional para ISPs pequeños y medianos que ya utilizan estos dispositivos, limita la adopción en entornos heterogéneos con equipos de otros fabricantes. En futuras iteraciones, se podría considerar la integración de estándares abiertos (como SNMPv3 o Netconf/Restconf) que permitirían extender la compatibilidad hacia otros proveedores.

Por otro lado, React implica un mayor consumo de recursos en el cliente en comparación con motores de plantillas ligeros, lo que podría afectar el rendimiento en dispositivos con hardware limitado.

6. Conclusiones

Este trabajo presentó un programa de monitoreo orientado al servicio para enrutadores MikroTik®, diseñado para detectar de manera temprana anomalías en redes de ISPs de pequeña y mediana escala. Entre los aportes clave destacan:

Implementación integral de infraestructura y software: Se integraron enrutadores de borde, ONU/OLT, VPN WireGuard, servidor VPS con GNU/Linux Debian, y frameworks Flask y Django REST Framework, logrando un flujo de datos seguro, estandarizado en JSON y accesible en tiempo real a través de un portal web con React.

Seguridad y resiliencia: Se aplicaron reglas de firewall, protocolos de seguridad y autenticación robusta en los enrutadores MikroTik®, mitigando riesgos asociados a la exposición de IP pública y garantizando la protección frente a ataques externos [10], [11].

Optimización del monitoreo y detección de anomalías: La plataforma permite supervisar múltiples enrutadores distribuidos en 40 zonas, facilitando la identificación rápida de fallas críticas y la generación de alertas automáticas, contribuyendo a una reducción significativa en los tiempos de respuesta.

En cuanto al objetivo de investigación, el sistema demuestra la viabilidad de integrar metodologías de monitoreo avanzado y seguridad en ISPs de escala limitada, destacando la efectividad de arquitecturas basadas en APIs, backend robusto y renderizado en tiempo real en frontend.

Como trabajo futuro se plantea incorporar un módulo de balanceo de carga post detección, para mejorar la continuidad del servicio y la resiliencia de la red. Así como, extender el monitoreo hacia entornos con mayor número de *enrutadores* y tráfico heterogéneo, evaluando la escalabilidad del sistema. De igual manera, integrar técnicas de inteligencia artificial y aprendizaje automático para predicción de fallas y optimización automática de recursos en tiempo real, aumentando la eficiencia operativa del ISP.

Referencias

[1] M. S. Elsayed, N.-A. Le Khac, S. Dev, and A. D. Jurcut, "Network Anomaly Detection Using LSTM Based Autoencoder," in Proc. 23rd Int. Conf. Modeling, Analysis and Simulation of Wireless and Mobile Systems, 2020.

[2] "Anomaly detection in multi-tiered cellular networks using LSTM and 1D CNN," EURASIP J. Wireless Commun. Netw., vol. 2022, no. 1, pp. 1-13, 2022.

[3] A. Chen, Y. Fu, X. Zheng, and G. Lu, "An Efficient Network Behavior Anomaly Detection using a Hybrid DBN-LSTM Network," Computers & Security, vol. 120, 2022.

[4] T. Acharya, A. Annamalai, and M. F. Chouikha, "Optimizing the Performance of Network Anomaly Detection Using Bidireccional Long Short-Term Memory (Bi-LSTM) and Over-sampling for Imbalance Network Traffic Data," Adv. Sci., Technol. Eng. Syst. J., vol. 8, no. 6, pp. 144-154, 2023.

[5] H. Liu and H. Wang, "Real-Time Anomaly Detection of Network Traffic Based on CNN," Symmetry, vol. 15, no. 6, Art. 1205, 2023.

[6] P. Schummer, A. del Rio, J. Serrano, D. Jimenez, G. Sánchez, and Á. Llorente, "Machine Learning-Based Network Anomaly Detection: Design, Implementation, and Evaluation," AI, vol. 5, no. 4, pp. 2967-2983, 2024.

[7] W. Yao, "A lightweight anomaly detection model for network traffic," BMC Bioinformatics, vol. 26, Art. 12215067, 2025.

[8] K. Yang et al., "Fog Intelligence for Network Anomaly Detection," IEEE Network, vol. 39, no. 1, pp. 112-120, Jan. 2025.

[9] H. Safdari, M. Ghobaei-Arani, and A. Souri, "Anomaly detection and community detection in networks," J. Big Data, vol. 9, no. 11, pp. 1-24, 2022.

[10] MikroTik, "WireGuard – RouterOS Documentation," 2025. [Online]. Available: https://help.mikrotik.com/docs/spaces/ROS/pages/69664792/WireGuard

[11] K. Dambis, "WireGuard on MikroTik RouterOS 7," 2025. [Online]. Available: https://kaspars.net/blog/wireguard-mikrotik-routeros

[12] N. Bispo, "FastAPI vs Django vs Flask — Which Is the Fastest for Building APIs?," 2025. [Online]. Available: https://developer-service.blog/fastapi-vs-django-drf-vs-flask-which-is-the-fastest-for-building-apis

[13] J. G. Castaño, "GPON: Introducción y fundamentos," LACNIC 34, Montevideo, Uruguay, 2020. [Online]. Available: https://www.lacnic.net/innovaportal/file/4749/1/lacnic-34-jgc-parte1---gpon-intro-y-fundamentos.pdf