UNIVERSIDAD ESTATAL PENÍNSULA

DE SANTA ELENA

FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

TITULO DEL TRABAJO DE TITULACIÓN

DISEÑO DE UN ENTORNO CONTROLADO PARA EL ANÁLISIS Y MONITOREO DE TRÁFICO DE RED EN EL LABORATORIO DE REDES DE FACSISTEL

AUTOR

Carcelén Tomalá, Miguel Ángel

EXAMEN COMPLEXIVO

Previo a la obtención del grado académico en

INGENIERO EN TECNOLOGÍAS DE LA INFORMACIÓN

TUTOR

Lsi. Quirumbay Yagual Daniel Iván, MSIA.

Santa Elena, Ecuador

Año 2025

UNIVERSIDAD ESTATAL PENÍNSULA

DE SANTA ELENA

FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

TRIBUNAL DE SUSTENTACIÓN

Ing. José Sánchez Aquino. Mgt.
DIRECTOR DE LA CARRERA

Lsi. Daniel Quirumbay Yagual. Msia.
TUTOR

Ing. Iván Coronel Suárez. Mgt.
DOCENTE ESPECIALISTA

Ing. Marjorie Coronel Suárez. Mgti.
DOCENTE GUÍA UIC

UNIVERSIDAD ESTATAL PENÍNSULA
DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CERTIFICACIÓN

Certifico que luego de haber dirigido científica y técnicamente el desarrollo y estructura final del trabajo, este cumple y se ajusta a los estándares académicos, razón por el cual apruebo en todas sus partes el presente trabajo de titulación que fue realizado en su totalidad por CARCELÉN TOMALÁ MIGUEL ÁNGEL, como requerimiento para la obtención del título de Ingeniero en Tecnologías de la Información.

La Libertad, a los 14 días del mes de noviembre del año 2025

TUTOR

Daniel Ivan Quirumbay Yagual
Time Stamping Security Data

Lsi. DANIEL QUIRUMBAY, MSIA.

UNIVERSIDAD ESTATAL PENÍNSULA
DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

DECLARACIÓN DE RESPONSABILIDAD

Yo, **Carcelén Tomalá Miguel Ángel**

DECLARO QUE:

El trabajo de Titulación, **"Diseño de un entorno controlado para el análisis y monitoreo de tráfico de red en el Laboratorio de Redes de FACSISTEL"**, previo a la obtención del título en Ingeniero en Tecnologías de la Información, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

La Libertad, a los 14 días del mes de noviembre del año 2025

EL AUTOR

Miguel Ángel Carcelén Tomalá

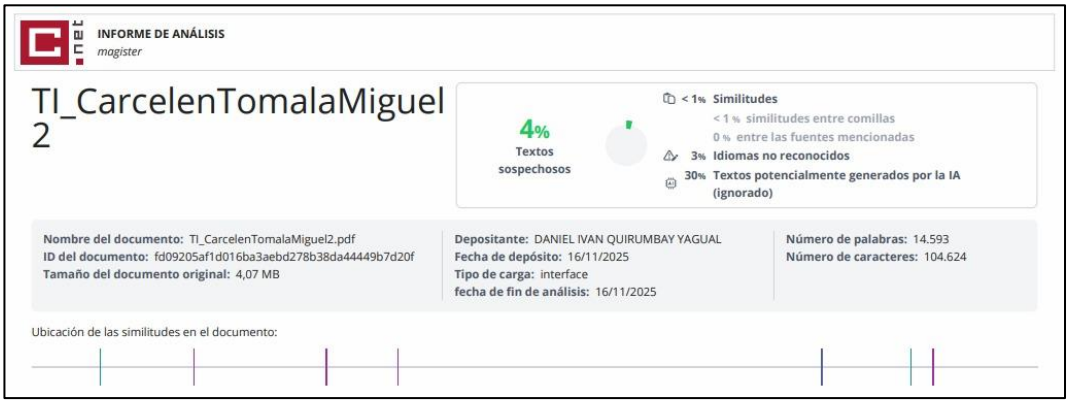
UNIVERSIDAD ESTATAL PENÍNSULA

DE SANTA ELENA

FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CERTIFICACIÓN DE ANTIPLAGIO

Certifico que después de revisar el documento final del trabajo de titulación denominado **"Diseño de un entorno controlado para el análisis y monitoreo de tráfico de red en el Laboratorio de Redes de FACSISTEL"**, presentado por el estudiante, Carcelén Tomalá Miguel Ángel fue enviado al Sistema Antiplagio, presentando un porcentaje de similitud correspondiente al 4%, por lo que se aprueba el trabajo para que continúe con el proceso de titulación.


INFORME DE ANÁLISIS
magister

TI_CarcelenTomalaMiguel2

4% Textos sospechosos

< 1% Similitudes
< 1 % similitudes entre comillas
0 % entre las fuentes mencionadas
3% Idiomas no reconocidos
30% Textos potencialmente generados por la IA (ignorado)

Nombre del documento: TI_CarcelenTomalaMiguel2.pdf
ID del documento: fd09205af1d016ba3aebd278b38da44449b7d20f
Tamaño del documento original: 4,07 MB

Depositante: DANIEL IVAN QUIRUMBAY YAGUAL
Fecha de depósito: 16/11/2025
Tipo de carga: interface
fecha de fin de análisis: 16/11/2025

Número de palabras: 14.593
Número de caracteres: 104.624

Ubicación de las similitudes en el documento:

TUTOR

Daniel Ivan Quirumbay Yagual
Time Stamping Security Data

Lsi. DANIEL QUIRUMBAY, MSIA.

UNIVERSIDAD ESTATAL PENÍNSULA
DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

AUTORIZACIÓN

Yo, **Carcelén Tomalá Miguel Ángel**

Autorizo a la Universidad Estatal Península de Santa Elena, para que haga de este trabajo de titulación o parte de él, un documento disponible para su lectura consulta y procesos de investigación, según las normas de la Institución.

Cedo los derechos en línea patrimoniales del presente trabajo de titulación con fines de difusión pública, además apruebo la reproducción dentro de las regulaciones de la Universidad, siempre y cuando esta reproducción no suponga una ganancia económica y se realice respetando mis derechos de autor

Santa Elena, a los 14 días del mes de noviembre del año 2025

EL AUTOR

Miguel Ángel Carcelén Tomalá

AGRADECIMIENTO

En primer lugar, agradezco profundamente a Dios por ser mi guía constante, por brindarme la fortaleza, la salud y la sabiduría necesarias para culminar esta etapa en mi vida. Su presencia ha sido mi refugio en los momentos de incertidumbre y mi impulso en los días de mayor esfuerzo.

A mis padres, el Sr. Carcelén José y la Sra. Tomalá María, gracias por su amor incondicional, por sus sacrificios y por enseñarme con el ejemplo el valor del compromiso y la perseverancia. A mi abuela, la Sra. Feliz María, por sus oraciones, su ternura y su fe inquebrantable. A mi hermana, María José, por su compañía, su apoyo y por ser parte esencial de este camino. A toda mi familia, por motivarme a seguir adelante y por estar presentes en cada paso de este proceso.

A Orrala Andrea, gracias por tu apoyo, tu escucha y tu presencia en los momentos clave de esta etapa. Tu compañía ha sido valiosa e importante.

A mis amistades, Reyes Diveana, Carvajal James, Galdea Erika, Parra Anthony, Soledispa Jorge y Balón Bryan, gracias por su amistad sincera, por las risas compartidas y por acompañarme en este recorrido académico con efecto y lealtad.

A mis docentes, Ing. Coronel Marjorie, Ing. Coronel Iván e Ing. Castillo Carlos, gracias por su entrega, por compartir sus conocimientos y por ser referentes de excelencia profesional. Agradezco también al Msc. Quijamo Francis, por su apertura y colaboración durante el desarrollo de este proyecto.

Finalmente, extiendo mi más sincero agradecimiento a mi tutor, el Lsi. Quirumbay Daniel, por su guía, su paciencia y su compromiso en cada etapa de este trabajo.

Miguel Ángel, Carcelén Tomalá

DEDICATORIA

Dedico este trabajo a Dios, por darme la fuerza en los momentos difíciles, por acompañarme en silencio cuando las dudas aparecían, por regalarme la salud y la claridad para seguir adelante. Sin su guía, este camino habría sido mucho más duro.

A mis padres, el Sr. Carcelén José y la Sra. Tomalá María, gracias por estar siempre, por su amor incondicional, por sus palabras de aliento y por enseñarme que los sueños se alcanzan con esfuerzo y humildad. Este logro también es suyo.

A mi abuela, la Sr. Feliz María, por sus oraciones, por su cariño y por ser ese pilar que me sostuvo con ternura y fe. Gracias, madre.

A mi hermana, María José, por su compañía, por sus consejos y por estar presente en cada etapa de este proceso.

Y finalmente, me lo dedico a mí mismo, por no rendirme, por sostenerme en los días de mayor exigencia, por el compromiso, el esfuerzo y la determinación con los que enfrenté cada reto.

Miguel Ángel, Carcelén Tomalá

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURA

ÍNDICE DE ANEXOS

RESUMEN

El propósito de esta propuesta tecnológica tuvo como finalidad diseñar un entorno controlado para el monitoreo del tráfico de red del Laboratorio de Redes de la Facultad de Sistemas y Telecomunicaciones (FACSISTEL), ante la necesidad de mejorar la seguridad informática y la gestión de la infraestructura tecnológica. El objetivo fue implementar una solución que evidenciara el comportamiento de la red en una visualización de tiempo real, la detección de anomalías y la generación de estadísticas para su análisis. Para ello, se integró el router Gigabit Omada ER7206 v2 y la plataforma Omada Controller dentro de un entorno de pruebas. Se aplicó la metodología PDCA y el desarrollo se estructuró en cinco fases: recolección de información, diseño, implementación, pruebas y reporte. Se utilizó un enfoque cuantitativo mediante una encuesta aplicada a estudiantes, además del análisis técnico y procesamiento de datos en Python. Durante el periodo de pruebas se analizó 310 registros de conexión, con un tráfico total mayor a 882 GB, y 35 eventos de seguridad de bajo nivel. Los resultados muestran que el entorno propuesto mejora la supervisión del tráfico, promueve el uso de herramientas profesionales y fortalece la formación práctica en redes.

Palabras claves: Entorno controlado, monitoreo de red, seguridad informática**,** análisis de tráfico, formación técnica.

ABSTRACT

The purpose of this technological proposal was to design a controlled environment for monitoring network traffic in the Network Laboratory of the Faculty of Systems and Telecommunications (FACSISTEL), addressing the need to improve cybersecurity and the management of the technological infrastructure. The objective was to implement a solution that would visualize network behavior in real time, detect anomalies, and generate statistics for analysis. To achieve this, the Omada ER7206 v2 Gigabit router and the Omada Controller platform were integrated within a test environment. The PDCA methodology was applied, and the development was structured in five phases: information gathering, design, implementation, testing, and reporting. A quantitative approach was used, employing a survey administered to students, along with technical analysis and data processing in Python. During the testing period, 310 connection logs were analyzed, representing a total traffic exceeding 882 GB, along with 35 low-level security events. The results show that the proposed environment improves traffic monitoring, promotes the use of professional tools, and strengthens practical network training.

Keywords: Controlled environment, network monitoring, computer security, traffic analysis, technical training.

INTRODUCCIÓN

El presente proyecto, titulado “Diseño de un entorno controlado para el análisis y monitoreo de tráfico de red en el Laboratorio de Redes de FACSISTEL”, surge ante la necesidad de fortalecer la seguridad informática y mejorar la gestión de la infraestructura tecnológica. Si bien el laboratorio cuenta con equipamiento funcional, se identificó la oportunidad de incorporar herramientas de supervisión en tiempo real que mejoren la capacidad de los estudiantes para comprender el comportamiento de la red, detectar anomalías y aplicar prácticas de análisis técnico.

El capítulo I expone la problemática de la falta de supervisión en tiempo real, lo que afecta la capacidad de análisis y respuesta ante eventos de red. Se presentan los antecedentes, el planteamiento del problema, los objetivos, la justificación y el alcance del proyecto, destacando la necesidad de proponer un entorno controlado para poder observar el comportamiento de la red y las medidas de seguridad que se pueden aplicar.

El capítulo II propone la parte del marco teórico y el marco conceptual, relacionando los temas como infraestructura de red, seguridad informática, monitoreo de tráfico, uso de archivos CSV y análisis de datos mediante herramientas tecnológicas. También se relacionan las plataformas utilizadas como Omada Controller y Python, así como las metodologías aplicadas para estructurar el proyecto, incluyendo el enfoque cuantitativo y la metodología PDCA.

El capítulo III presenta la propuesta tecnológica que comienza por los requerimientos funcionales, requerimientos no funcionales, hardware y software. Se expone la arquitectura del entorno, la integración del router Omada ER7206 v2, la configuración del sistema de monitoreo, el script de Python para el análisis de tráfico y también la elaboración del manual de funcionamiento.

CAPÍTULO 1.- FUNDAMENTACIÓN

1.1 Antecedentes.

En la actualidad, las redes de comunicación constituyen un pilar fundamental en el funcionamiento de toda organización moderna [1]. No obstante, la ausencia de mecanismos adecuados para el monitoreo del tráfico de red puede generar problemas en términos de rendimiento y seguridad [1]. La falta de herramientas eficaces para supervisar y analizar el flujo de datos puede derivar en interrupciones del servicio, vulnerabilidades ante ataques cibernéticos y pérdidas económicas asociadas a la disminución de la productividad institucional [2].

La creciente complejidad de la infraestructura tecnológica, provocada por las nuevas tecnologías y el aumento del volumen de datos, ha hecho que la tarea de monitoreo de la red sea cada vez más complicada [3]. Si las organizaciones no cuentan con un sistema eficiente, tienen dificultades para encontrar y solucionar fallos, lo que puede provocar tiempos de inactividad prolongados y experiencias negativas para los usuarios [3].

La Facultad de Sistemas y Telecomunicaciones (FACSISTEL) de la Universidad Estatal Península de Santa Elena (UPSE) se ha convertido en una institución de referencia para la formación de profesionales en el campo de la tecnología [4]. Sin embargo, el aumento sostenido de la comunidad académica ha incrementado las demandas sobre la infraestructura tecnológica, evidenciando la necesidad de proponer soluciones innovadoras que permitan monitorear el tráfico de red. La falta de mecanismos adecuados para gestionar esta demanda ha generado riesgos asociados a la seguridad informática y ha puesto en evidencia las limitaciones del entorno.

En el presente trabajo, se plantea una investigación con enfoque cuantitativo, utilizando la encuesta como técnica principal para la recolección de datos [5]. Se aplicará un muestreo no probabilístico por conveniencia estratificada, seleccionando a los estudiantes que realizan prácticas en el Laboratorio de Redes de la facultad. Esto permitirá explorar las percepciones y necesidades existentes en el área, identificando elementos clave que sustenten el análisis y orienten la

propuesta de mejora. Los resultados obtenidos constituirán un insumo valioso para el diseño y validación del entorno controlado propuesto (Ver Anexo 1).

Entre los antecedentes relevantes, se destaca el trabajo de investigación titulado **"Laboratorio virtual de análisis y comportamiento de malware basado en técnicas y métodos de seguridad informática para los laboratorios en la Facultad de Sistemas y Telecomunicaciones",** en el cual se implementó un entorno virtual para analizar el comportamiento del malware, con el objetivo de reforzar la seguridad y protección de datos [6]. El estudio abordó el problema de una red inestable e insegura en FACSISTEL, cuya vulnerabilidad favorecía la propagación de software malicioso. Se utilizaron herramientas de código abierto para facilitar el análisis estático y dinámico en un entorno controlado, aplicando la metodología ISSAF en tres fases: planificación, evaluación y reporte. Esta estructura permitió estudiar detalladamente la arquitectura y comportamiento del malware, generando informes técnicos que facilitaron la toma de decisiones en seguridad informática [6].

Otro antecedente relevante es el trabajo de investigación titulado **"Implementación de monitoreo de red utilizando los protocolos ICMP y SNMP",** cuyo objetivo fue implementar un servidor capaz de supervisar integralmente los dispositivos y servidores de la Universidad UPSE [7]. El estudio identificó la necesidad de mejorar la gestión y el control del consumo de recursos de la red, en un contexto institucional caracterizado por el manejo de grandes volúmenes de información en múltiples formatos. La propuesta enfatizó la importancia de establecer una gestión robusta mediante un servidor con características avanzadas y software confiables, aprovechando protocolos eficientes y amigables para el usuario. La investigación se fundamentó en métodos hipotético, deductivo, analítico y sintético, asegurando una administración efectiva de los recursos tecnológicos disponibles [7].

Asimismo, el trabajo de investigación titulado **"Implementación y evaluación de sistema de monitoreo de seguridad basado en flujos de paquetes IP"**, se enfoca en analizar el tráfico de red para detectar amenazas, desarrollando un sistema capaz de evaluar la información contenida en los paquetes IP con fines de seguridad

informática [8]. El estudio permitió identificar actividades maliciosas mediante el análisis de origen y destino de los paquetes, destacando la detección de propagación de malware a través de ataques masivos de conexión. Se diseñó un sistema offline para analizar el tráfico IP proveniente de redes distribuidas, enfrentando el desafío de la traducción de direcciones realizada por el router [8]. Los resultados obtenidos sentaron las bases para nuevos métodos de detección que fortalecen la seguridad informática institucional.

En consecuencia, se plantea el desarrollo de un entorno controlado que permita el análisis del tráfico de datos y detectar anomalías en tiempo real. Esta propuesta no solo fortalecerá las estrategias de seguridad, sino que también proporcionará un espacio práctico para el desarrollo de habilidades fundamentales en el ámbito de redes y telecomunicaciones.

1.2 Descripción del proyecto.

El presente trabajo se enfoca en el diseño de un entorno controlado para el monitoreo del tráfico de red en el laboratorio de Redes de la Facultad de Sistemas y Telecomunicaciones (FACSISTEL). Ante la situación, se plantea establecer un entorno que permita analizar el flujo de datos, identificar anomalías y evaluar estrategias de seguridad.

Este espacio controlado permitirá la evaluación de distintas estrategias de monitoreo y el análisis del rendimiento de la red. Además, funcionará como recurso educativo, brindando la oportunidad de practicar y mejorar habilidades técnicas necesarias en un entorno seguro y real. Este trabajo no solo busca mejorar la gestión de la red y protección, sino también enriquecer la formación necesaria en la práctica de los futuros profesionales del área.

La metodología aplicada corresponde al ciclo de mejora continua PDCA, también conocido como ciclo de Deming, el cual se adapta al diseño, simulación e implementación de infraestructura de red [9]. Este enfoque estructurado permite una planificación clara, facilita la ejecución por fases y garantiza un desarrollo ordenado del sistema de monitoreo, fortaleciendo la validez metodológica al seguir un estándar reconocido en la industria [9].

Fase I: Recolección de información.

La recolección de la información se llevará a cabo mediante una encuesta hacia los estudiantes que realizan prácticas en el laboratorio de Redes con la finalidad de obtener información directa y detallada sobre el estado actual de la infraestructura. Para la selección de los estudiantes se aplicará un muestreo no probabilístico por conveniencia estratificada con el fin de identificar la percepción sobre la falta de un entorno de simulación y su impacto en el desarrollo de las habilidades prácticas (Ver Anexo 1).

De forma complementaria, se llevará a cabo una revisión técnica de equipos de enrutamiento con la finalidad de identificar características relacionadas con la captura y análisis de datos. Esto permitirá determinar qué dispositivo ofrece condiciones adecuadas en un sistema de monitoreo eficiente y didáctico.

- Encuesta aplicada a estudiantes del Laboratorio de Redes.
- Percepción estudiantil sobre la falta de un entorno de simulación funcional.
- Evaluación técnica de equipos de enrutamiento.

Fase II: Diseño del entorno controlado.

Se llevará a cabo la elaboración de una topología de red, incorporando el router Omada ER7206 v2 como elemento central de la infraestructura, permitiendo establecer rutas de conexión, puntos de captura de tráfico e integración con dispositivos existentes.

Asimismo, se seleccionarán herramientas de análisis que faciliten la interpretación de los datos recolectados, como la plataforma Omada Controller, que permite gestionar y visualizar el comportamiento de la red. Se desarrollará un script en Python orientado al procesamiento de archivos en formatos CSV, con el fin de extraer patrones, generar estadísticas y detectar alertas relevantes.

- Diseño de la topología de red.
- Selección de la herramienta de análisis Omada Controller.
- Desarrollo de script en Python para el procesamiento de datos.

Fase III: Implementación.

En esta fase se realizará la instalación y la configuración del equipo router Gigabit Omada modelo ER7206 v2, el cual será incorporado al Laboratorio de Redes y conectado a la infraestructura tecnológica actual. Se establecerán parámetros específicos para la captura y el análisis del tráfico.

- Instalación del router ER7206 v2.
- Integración con la infraestructura existente.
- Configuración de monitoreo de tráfico.

Fase IV: Pruebas

Se llevarán a cabo pruebas de monitoreo en tiempo real a partir de la utilización de la plataforma Omada Controller, lo cual permitirá ver el flujo de datos, detectar picos de tráfico y encontrar anomalías por medio de la infraestructura del laboratorio. Además, se ejecutará el script desarrollado en Python para analizar los archivos en formato CSV generado por la plataforma, permitiendo observar el comportamiento del tráfico y generar estadísticas detalladas. Esta fase es importante para validar la eficiencia del entorno controlado y evaluar su rendimiento frente a distintos escenarios de tráfico.

- Recolección de información mediante monitoreo en tiempo real.
- Análisis del comportamiento y patrones de tráfico a partir de archivo CSV.
- Evaluación del funcionamiento de la red ante distintos escenarios.

Fase V: Reporte

Se creará un manual de funcionamiento que documentará los procesos de instalación del equipo, las configuraciones y la ejecución de pruebas orientadas al análisis del tráfico de red. El documento incorporará instrucciones detalladas sobre el uso de herramientas como Omada Controller, facilitando su aplicación en entornos educativos y técnicos. Asimismo, se entregará el script desarrollado en Python para el procesamiento de archivos CSV generados durante el monitoreo.

- Manual de funcionamiento sobre instalación, configuración y pruebas.
- Instrucciones para el uso de herramientas especializadas.

- Entrega del script de análisis en Python.

Este trabajo se enmarca en la línea de investigación de Tecnología y Sistemas, dentro de la sublínea de Ingeniería y Gestión de TSI, conforme a la resolución RCF-FST-SO-09 No. 03-2021.

1.3 Objetivos del proyecto

1.3.1 Objetivo general

Implementar un entorno de monitoreo de tráfico de red mediante el uso de equipo y herramientas tecnológicas que permitan mejorar la seguridad y el rendimiento de la red en el laboratorio de Redes.

1.3.2 Objetivos específicos

- Revisar de manera técnica los equipos de enrutamiento con funciones de monitoreo del tráfico de red, que permitan capturar y analizar datos en tiempo real.
- Analizar resultados obtenidos mediante herramientas de monitoreo de tráfico de red.
- Elaborar un manual de funcionamiento para un entorno controlado de monitoreo del tráfico de red en el que se detallen los procesos de instalación, configuración, pruebas de análisis de tráfico.

1.4 Justificación del proyecto

El diseño de un entorno controlado para monitorear la red se ha convertido en una necesidad estratégica para cualquier organización, al aportar beneficios en términos de seguridad informática, eficiencia operativa y continuidad del servicio [10]. Contar con un sistema de monitoreo continuo permite la detección temprana de fallos, la optimización del rendimiento y la prevención de interrupciones inesperadas. Estos factores no solo garantizan la estabilidad de los procesos, sino que también mejoran la experiencia del usuario, fortaleciendo la confianza y la percepción de calidad en los servicios ofrecidos [10].

En el ámbito académico de la Facultad de Sistemas y Telecomunicaciones (FACSISTEL) de la Universidad Estatal Península de Santa Elena, un sistema de monitoreo de red representa un recurso estratégico para la formación técnica [11].

Un entorno controlado permitirá la aplicación práctica de conocimientos teóricos, fortaleciendo habilidades esenciales en el campo de redes de comunicación y mejorando la calidad del proceso de enseñanza y aprendizaje [11].

Este espacio seguro y realista facilitará la comprensión del funcionamiento de las redes, al permitir la simulación de escenarios reales, el análisis de protocolos de seguridad y la identificación de anomalías en condiciones controladas. Además, promoverá la adopción de medidas preventivas y el diseño de estrategias orientadas a la protección de la infraestructura tecnológica.

La incorporación de herramientas y tecnologías actualizadas convertirá al Laboratorio de Redes en un espacio innovador, alineado con los estándares contemporáneos de educación tecnológica. Esta modernización no solo renovará el entorno físico, sino que permitirá integrar prácticas con dispositivos y sistemas utilizados en entornos profesionales, brindando así una experiencia formativa más completa y pertinente.

El presente proyecto está alineado con el Plan Nacional de Desarrollo Ecuador No Se Detiene 2025-2029, haciendo énfasis en el Eje Ambiente, Agua, Energía y Conectividad, específicamente en el Objetivo 7 y la política 7.1 [12].

Objetivo 7: Impulsar el desarrollo de infraestructuras sostenibles y resilientes; y de la conectividad física y digital, que brinde condiciones de crecimiento y desarrollo económico [12].

Política 7.1: Impulsar el desarrollo digital a través de la mejora en tecnología y la expansión de la conectividad en áreas geográficas no atendidas o con conectividad limitada en el país [12].

1.5 Alcance del proyecto

El presente proyecto tiene como finalidad diseñar un entorno controlado para el monitoreo del tráfico de red en el laboratorio de Redes. Esta iniciativa busca responder a la necesidad de contar con un espacio funcional que permita observar el comportamiento de la red, detectar anomalías y fortalecer el aprendizaje práctico dentro del entorno académico.

El desarrollo se llevará a cabo en las instalaciones del laboratorio, donde se integrará el equipo Router VPN Gigabit Omada modelo ER7206 v2 a la infraestructura tecnológica existente. Este entorno permitirá capturar flujos de datos en tiempo real, analizar patrones de tráfico y evaluar el rendimiento de la red bajo distintos escenarios, brindando una visión técnica y detallada de su funcionamiento.

La metodología aplicada PDCA corresponde al ciclo de Deming, el cual estructura el proyecto en fases: recolección de información, diseño del entorno controlado, implementación, pruebas y elaboración de reporte. Cada fase está diseñada para garantizar una ejecución ordenada, permitiendo validar la eficiencia del entorno y documentar los procedimientos realizados.

Fase de recolección de información:

- Aplicar una encuesta dirigida a estudiantes que realizan prácticas en el laboratorio de Redes.
- Tipo de muestreo no probabilístico por conveniencia estratificada.
- Identificar la percepción sobre la falta de un entorno controlado funcional.
- Análisis de los datos recolectados como insumo para la propuesta de mejora.
- Revisión técnica de equipos de enrutamiento.

Fase de diseño del entorno controlado:

- Se definirá la topología de red, integrando el router Omada.
- Selección de herramientas de monitoreo y análisis para la captura de datos en tiempo real.
- Plataforma Omada Controller y desarrollo de un script en Python para el procesamiento de archivos CSV, facilitando la visualización de estadísticas y patrones de tráfico.

Fase de implementación:

- Instalación y configuración del dispositivo de enrutamiento y monitoreo dentro del laboratorio de Redes.
- Integración del equipo a la infraestructura tecnológica existente.

Fase de pruebas:

- Ejecución de monitoreo en tiempo real del flujo de datos mediante el equipo y herramientas seleccionadas.
- Análisis de patrones de comportamientos de red, detección de anomalías, visualización de estadísticas de tráfico.

Fase de reporte:

- Elaboración de un manual de funcionamiento que documente los procedimientos de instalación, configuración y análisis del entorno de monitoreo.
- Incluir instrucciones detalladas sobre el uso del Router ER7206 v2 y las herramientas de análisis empleadas.

Finalmente, este proyecto se enmarca en un contexto académico orientado a enriquecer el proceso de aprendizaje, brindando a los estudiantes la oportunidad de perfeccionar habilidades técnicas en un entorno supervisado. La propuesta no solo fortalece la formación práctica, sino que también promueve el uso responsable y seguro de tecnologías aplicadas al monitoreo de redes.

CAPÍTULO 2.- MARCO TEÓRICO Y METODOLOGÍA DEL PROYECTO

2.1 Marco conceptual

2.1.1 Redes de comunicación

Las redes de comunicación representan un conjunto estructurado de dispositivos interconectados que permiten la transmisión de datos entre usuarios, sistemas y equipos tecnológicos. Estas redes pueden operar mediante medios físicos como cables de cobre, fibra óptica o a través de tecnologías inalámbricas, tales como Wi-Fi y enlaces satelitales [13]. Su función principal es facilitar el intercambio de información en tiempo real, mejorando la conectividad entre distintos puntos geográficos [13].

Las redes de comunicación son esenciales para garantizar un buen funcionamiento, trabajo colaborativo a distancia y el acceso a recursos compartidos [14]. Su evolución ha dado un giro a la forma como las personas interactúan, aprenden y trabajan en los entornos digitales cada vez más exigentes [14].

2.1.2 Tipos de redes

Las redes informáticas se clasifican principalmente según su alcance geográfico y la cantidad de dispositivos que interconectan. Entre las más comunes se encuentran:

- **LAN (Local Area Network):** Operan en espacios reducidos como oficinas o laboratorios [15].
- **MAN (Metropolitan Area Network):** Cubren áreas urbanas o campus universitarios [15].
- **WAN (Wide Area Network):** Permiten la conexión entre dispositivos ubicados en distintas regiones o países [15].

También existen las PAN (Personal Area Network), diseñadas para conectar dispositivos personales como teléfonos móviles y computadoras mediante tecnologías de corto alcance como Bluetooth [16]. Cada tipo de red responde a requerimientos específicos de conectividad, velocidad, seguridad y escalabilidad, siendo fundamentales para el diseño de infraestructura tecnológica eficiente [16].

2.1.3 Topología de red

La topología de red hace referencia al diseño físico o lógico mediante el cual se organizan los dispositivos y las conexiones dentro de una red informática. Este concepto permite visualizar cómo se distribuyen los nodos, como computadoras, routers o impresoras y cómo se comunican entre sí para transmitir datos [17].

Entre las topologías más comunes se encuentran: estrella, bus, anillo, malla y árbol. La elección de una topología adecuada influye directamente en el rendimiento, la escalabilidad y la tolerancia a fallos de la red [18]. En entornos académicos como laboratorios, seleccionar una estructura eficiente facilita el monitoreo, la administración, la detección de errores y comprender las topologías para diseñar redes funcionales y seguras [18].

2.1.4 Arquitectura de red

La arquitectura de red representa el modelo estructural que define cómo se organizan los componentes físicos y lógicos dentro de una infraestructura de comunicaciones [19]. Este concepto establece las reglas, protocolos y funciones que permiten la interacción entre dispositivos, servidores y usuarios, garantizando la interoperabilidad, la escalabilidad y la seguridad del sistema [20].

2.1.5 Monitoreo de tráfico de red

El monitoreo de tráfico de red es el proceso mediante el cual se supervisa el flujo de datos que circula entre los dispositivos conectados en una red informática [21]. Permitiendo identificar el origen, destino, volumen y tipo de información transmitida, lo cual resulta esencial para detectar anomalías, mejorar el rendimiento y prevenir amenazas [21].

Mediante el uso de herramientas específicas como analizadores de flujo y sistemas de alerta, los administradores pueden observar métricas clave, como el uso de ancho de banda, puertos saturados y actividades sospechosas [22]. En entornos académicos como laboratorios, el monitoreo facilita el aprendizaje práctico al permitir observar el comportamiento real de la infraestructura tecnológica, apoyando la toma de decisiones informadas sobre la configuración, seguridad y escalabilidad [22].

2.1.6 Herramientas de monitoreo

Las herramientas de monitoreo de red son soluciones tecnológicas diseñadas para supervisar el estado, rendimiento y seguridad de los dispositivos conectados a una infraestructura informática [23]. Estas herramientas permiten visualizar métricas en tiempo real, generar alertas ante comportamientos anómalos y analizar el flujo de datos para detectar fallos o vulnerabilidades [23].

Entre las más utilizadas se encuentran: PRTG Network Monitor, Zabbix, Nagios, ManageEngine y OpManager [24]. Estas herramientas facilitan el aprendizaje práctico, ya que permiten a los estudiantes observar el comportamiento de una red bajo diferentes condiciones [24].

2.1.7 Seguridad informática

La seguridad informática comprende el conjunto de prácticas, tecnologías y políticas orientadas a proteger los sistemas digitales, redes y datos frente a accesos no autorizados, ataques maliciosos y fallos operativos [25]. Su propósito es garantizar la confidencialidad, integridad y disponibilidad de la información, considerados fundamentales para el funcionamiento seguro de cualquier infraestructura tecnológica [26].

La seguridad informática permite prevenir incidentes como el robo de datos, la propagación de malware o la interrupción de servicios críticos [26].

2.1.8 Principios de seguridad

Los principios de seguridad informática constituyen la base conceptual para proteger los datos y sistemas frente a amenazas internas y externas [27]. Entre los más reconocidos se encuentran la confidencialidad, la integridad y la disponibilidad, conocidas como el modelo CIA por sus siglas en inglés [27].

- **Confidencialidad:** Permite que la información sea accesible por personas que estén autorizadas, evitando así las filtraciones o accesos indebidos [28].
- **Integridad:** Garantiza que la información no sea codificada de forma no autorizada, asegurando así su exactitud y su confiabilidad en su ciclo de vida [28].

- **Disponibilidad:** Implica que los sistemas y servicios estén operativos cuando se requieran, minimizando interrupciones y asegurando la continuidad de las operaciones [28].

2.1.9 Sistemas de IDS/IPS

Los sistemas de IDS e IPS son mecanismos diseñados para identificar y responder ante actividades sospechosas dentro de una red informática. Mientras los IDS se enfocan en la detección pasiva de intrusiones mediante el análisis de patrones y comportamientos, los IPS actúan de forma preventiva, bloqueando el tráfico malicioso en tiempo real [29].

Estas tecnologías permiten clasificar eventos según su severidad, origen y tipo de amenaza, utilizando bases de datos de firmas y algoritmos de comportamiento [30]. Su integración en equipos de enrutamiento facilita la generación de alertas técnicas, el análisis de tráfico y la comprensión de vulnerabilidades reales [30].

2.1.10 Metodología PDCA

El ciclo PDCA (Plan-Do-Check-Act), también ciclo de mejora continua, es una técnica comúnmente utilizada en el ámbito técnico y educativo para buscar comprobar la calidad y eficiencia de los procesos tratados [31].

La aplicación de esta metodología en proyectos de redes informáticas facilita la estructuración lógica de cada una de las etapas, desde la identificación de necesidades hasta la implementación de las soluciones propuestas, ayudando de esta forma a la toma de decisiones informadas y la mejora progresiva del sistema [31].

- **Planificar:** Se recopila información relevante del entorno, se definen los objetivos del proyecto y se establecen estrategias para alcanzar los resultados esperados [32].
- **Hacer:** Se ejecutan las acciones planificadas, como el diseño de la red, la selección de equipos y la configuración inicial [32].
- **Verificar:** Se analizan los resultados obtenidos, comparándolos con los objetivos planteados para identificar desviaciones y oportunidades de mejora [32].

- **Actuar:** Se introducen ajustes y correcciones con base en los hallazgos, fortaleciendo el rendimiento del sistema y asegurando su sostenibilidad en el tiempo [32].

2.1.11 Visual Studio

Es un entorno de desarrollo integrado (IDE) que permite crear, depurar y desplegar aplicaciones en múltiples lenguajes de programación, tales como C#, Python y JavaScript [33]. Su interfaz intuitiva y sus herramientas integradas lo convierten en una plataforma para el desarrollo de software, especialmente en proyectos que requieren análisis técnicos y estructuración de código [33].

Sirve para modelar arquitecturas, mejorar pruebas y gestionar versiones de manera eficiente. Visual Studio ha evolucionado para integrar funciones avanzadas como inteligencia artificial, destacando el fortalecimiento de competencias digitales en entornos educativos [34].

2.1.12 Python – Lenguaje de programación

Python es un lenguaje de programación de alto nivel, interpretado y de propósito general, diseñado para ser legible, versátil y accesible tanto para desarrolladores como para usuarios con formación técnica [35]. Su sintaxis clara permite escribir código de forma intuitiva, lo que lo convierte en una herramienta ideal para tareas de automatización, desarrollo web, análisis de datos y aprendizaje automático [35]. Su enfoque admite programación orientada a objetos, imperativa y funcional, lo que amplía su aplicabilidad en diversos entornos académicos y profesionales [35].

2.1.13 Router VPN Gigabit ER7206 v2

Es un dispositivo diseñado para entornos profesionales que requieren alta seguridad, rendimiento y gestión centralizada. Su arquitectura basada en Omada SDN permite el monitoreo inteligente, la configuración remota, el balanceo de carga entre múltiples puertos WAN y la segmentación de tráfico [36].

En contextos académicos, el hardware puede ser usado para crear entornos controlados para comprender el análisis de tráfico en tiempo real, fortaleciendo la infraestructura tecnológica y promoviendo la formación práctica en redes y telecomunicaciones [36].

2.1.14 Omada Controller de TP-Link

Plataforma de gestión centralizada que permite administrar routers, switches y puntos de acceso desde una única interfaz. Su arquitectura basada en SDN facilita la configuración remota, el monitoreo en tiempo real y la implementación automatizada de servicios de red [37].

Esta herramienta permite establecer redes seguras, escalables y fácilmente replicables, optimizando la supervisión del tráfico y el rendimiento [38]. Omada Controller mejora la eficiencia operativa al reducir la complejidad de configuración y mantenimiento, destacando su capacidad para gestionar múltiples dispositivos, ideas para laboratorios educativos y redes institucionales [38].

2.1.15 Archivos CSV

Estructuras de datos tabulares representadas en texto plano, donde cada línea corresponde a un registro y los campos se separan mediante comas [39]. Su simplicidad estructural, combinada con la compatibilidad con múltiples lenguajes de programación, los convierte en una herramienta utilizada para el análisis de datos [39].

En proyectos de monitoreo de red, permiten almacenar y procesar grandes volúmenes de información de manera eficiente [40]. Según su formato compacto, facilitan la interoperabilidad entre sistemas, destacando su uso frecuente en entornos de machine learning como fuente de datos para entrenamiento y evaluación de modelos [40].

2.2 Marco teórico

2.2.1 Infraestructura de red y su importancia en entornos académicos

La infraestructura de red en instituciones educativas constituye un componente esencial para el desarrollo de procesos formativos modernos, al permitir la interconexión de dispositivos, el acceso a plataformas digitales y la gestión eficiente de recursos tecnológicos [20]. En entornos académicos, una red bien estructurada facilita la implementación de laboratorios virtuales, aulas híbridas y sistemas de monitoreo que enriquecen la experiencia de aprendizaje [20].

Una infraestructura robusta promueve la inclusión digital, reduce la brecha tecnológica y mejora la productividad tanto de docentes como de estudiantes. La evolución de las redes educativas está marcada por la incorporación de tecnologías emergentes como SDN e IoT, que permiten una gestión más dinámica, segura y escalable de los datos institucionales [41]. El fortalecimiento de estas infraestructuras responde a la necesidad de adaptar los laboratorios universitarios a los nuevos modelos de enseñanza, investigación y preservación digital [41].

2.2.2 Seguridad informática y monitoreo de tráfico

La seguridad informática y el monitoreo de tráfico son elementos esenciales para preservar la integridad de los sistemas de comunicación digital. Mientras que la seguridad se enfoca en proteger los activos de información frente a amenazas internas y externas, el monitoreo permite observar el comportamiento de la red, detectar anomalías y prevenir accesos no autorizados [42].

En redes académicas, donde múltiples usuarios interactúan simultáneamente, estas prácticas adquieren mayor relevancia debido a la exposición constante a riesgos tecnológicos [43]. Algunos protocolos de comunicación fueron diseñados en contextos donde la seguridad no era una prioridad, lo que obliga a proponer mecanismos defensivos y ofensivos que robustezcan la infraestructura y garanticen la confidencialidad, disponibilidad e integridad de los datos [43].

2.2.3 Uso de herramientas tecnológicas para el análisis de datos

En el ámbito académico y tecnológico, el uso de herramientas para el análisis de datos permite procesar grandes volúmenes de información en tiempo real, facilitando la toma de decisiones, la detección de anomalías y la optimización de procesos [44]. Herramientas como Apache Kafka, Flink o Power BI han demostrado ser eficaces para capturar, transformar y visualizar datos en entornos de red donde la actividad es constante y diversa [44].

Las plataformas de big data aplicadas al análisis en tiempo real no solo mejoran la experiencia del usuario, sino que también permiten anticipar riesgos y oportunidades mediante la gestión eficiente de la información [45]. Tecnología como Hadoop, Spark y sistemas de minería de datos ha revolucionado la forma en

que se interpretan los flujos de datos, abriendo nuevas posibilidades para la investigación científica, la educación y la gestión institucional [45].

2.3 Metodología del proyecto

2.3.1 Metodología de investigación

Para el desarrollo de esta propuesta se realizará un enfoque exploratorio, mediante la revisión de trabajos relacionados con entornos controlados y monitoreo de tráfico de redes [5]. Esta revisión permitirá identificar enfoques previos, comprender cómo se han abordado problemas similares y extraer ideas que orienten el diseño del entorno propuesto.

El estudio se enmarca en un enfoque cuantitativo, utilizando la encuesta como técnica para la recolección de información [5]. Esta será aplicada a los estudiantes que realizan prácticas en el laboratorio de Redes, con el fin de conocer su experiencia y percepción sobre la falta de un entorno funcional para prácticas de monitoreo. La selección de los participantes se realizará mediante un muestreo no probabilístico por conveniencia estratificada. (Ver Anexo 1).

2.3.2 Idea a defender

El diseño de un entorno controlado de monitoreo en el Laboratorio de Redes permite fortalecer la formación de gestión de tráfico de red, por medio de la simulación de situaciones reales, la aplicación de configuraciones técnicas y el análisis de comportamiento en tiempo real. Esta propuesta contribuirá a una mejor comprensión de las vulnerabilidades, a la detección de anomalías y a la toma de decisiones para mejorar la seguridad de la infraestructura tecnológica, integrando herramientas como Omada Controller, Python y sistemas IDS.

2.3.3 Variable

Porcentaje de registro de tráfico que presentan comportamientos anómalos identificados por el sistema de monitoreo en el entorno controlado. Esta métrica permite evaluar la capacidad del sistema para analizar el tráfico en tiempo real e identificar posibles amenazas. El análisis se basa en los datos exportados en formato CSV que se recogieron durante las sesiones prácticas.

2.3.4 Técnicas e instrumentos de recolección de datos

La recolección de datos se llevará a cabo mediante una encuesta estructurada, aplicada a estudiantes que cruzan asignaturas prácticas en el Laboratorio de Redes de la Facultad. Este instrumento permitirá obtener información directa y detallada sobre aspectos como la percepción del aprendizaje práctico, el uso de herramientas tecnológicas y la importancia del monitoreo de red (Ver Anexo N°1).

Se identificaron los semestres académicos que utilizan el laboratorio, seleccionando el 50% de los estudiantes de cada uno de los cuales se obtuvo una muestra total de 111 estudiantes encuestados (Tabla N°1).

Asimismo, se emplearán datos en tiempo real dentro de un entorno de pruebas con el objetivo de validar el funcionamiento del sistema propuesto. Esto permitirá observar el comportamiento del tráfico sin comprometer la infraestructura.

Semestre	**Materia**	**N° estudiantes**	**Porcentaje 50%**
Tercero	Fundamentos de redes	24	12
Cuarto	Comunicación y enrutamiento de datos	28	14
Cuarto	Ingeniería de software	44	22
Sexto	Ethical hacking	27	14
Sexto	Internet de las cosas	28	14
Sexto	Arquitectura y plataforma TI	23	12
Séptimo	Computación forense	25	12
Séptimo	Seguridad de TI	22	11
Total		221	**111**

Tabla 1. Selección de estudiantes por semestres.

2.3.5 Análisis de encuestas

Pregunta N°1: ¿Has tenido alguna experiencia práctica en el laboratorio de Redes relacionada con redes informáticas?

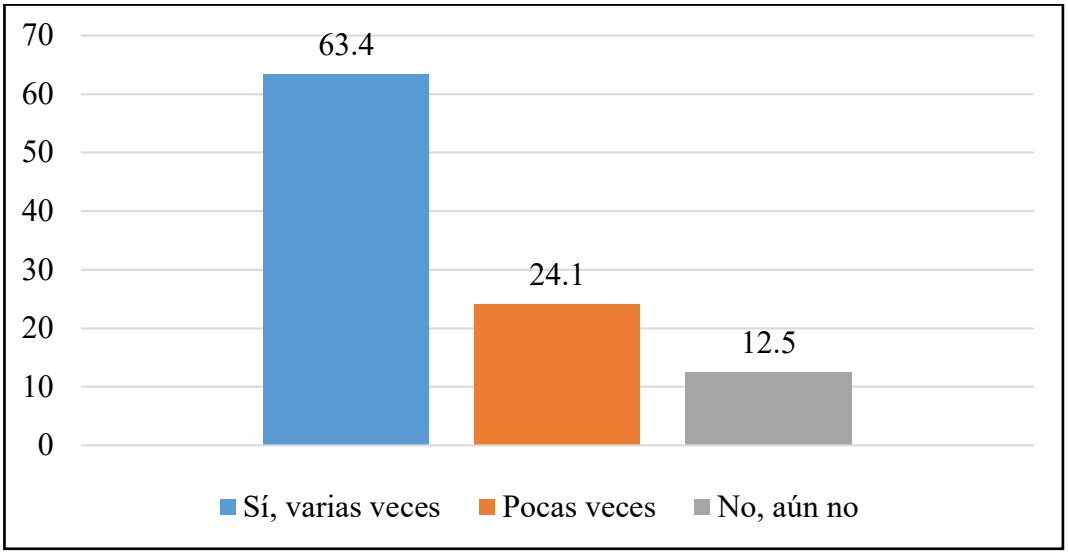


Figura 1. Experiencia práctica en el Laboratorio de Redes.

Respuesta	Votos	Porcentaje
Sí, varias veces	71	63.4%
Pocas veces	27	24.1%
No, aún no	14	12.5%
Total	112	100%

Tabla 2. Experiencia práctica en el Laboratorio de Redes.

Interpretación: El (63,4%) de los estudiantes manifestó haber tenido experiencias prácticas en el laboratorio de Redes, lo que evidencia un nivel de participación técnica (Figura Nº1). Sin embargo, un (24,1%) indicó haber participado solo pocas veces y un (12,5%) aún no ha tenido oportunidad de realizar prácticas (Tabla Nº2).

Conclusión: Tales resultados apuntan a que, si bien existe una base sólida de participación, aún hay que ampliar el acceso y la frecuencia de actividades prácticas, sobre todo para aquellos estudiantes que no han relacionado con equipos o simuladores.

Pregunta N°2: ¿Crees que el laboratorio de Redes debería incluir más actividades prácticas para reforzar lo aprendido?

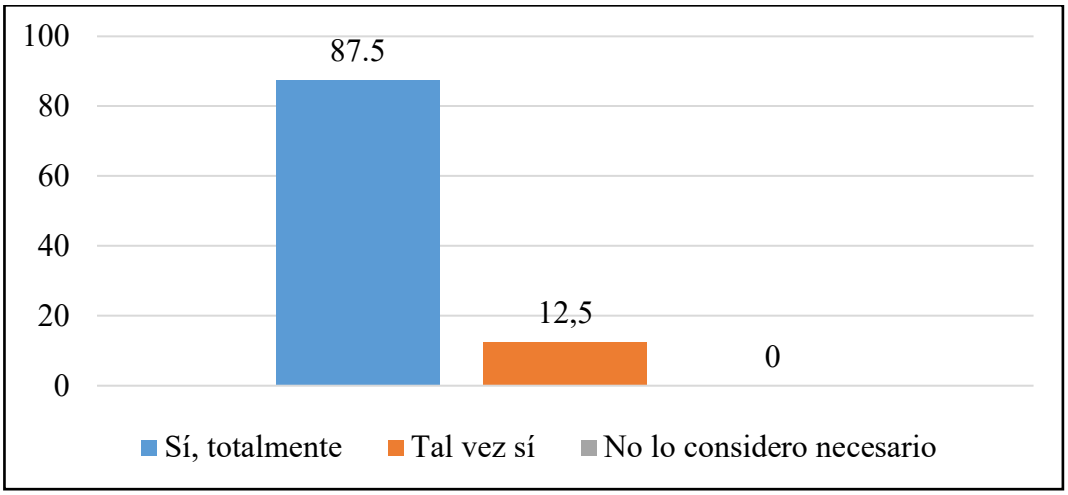


Figura 2. Incluir actividades prácticas.

Respuesta	Votos	Porcentaje
Sí, totalmente	98	87.5%
Tal vez sí	14	12.5%
No lo considero necesario	0	0%
Total	112	100%

Tabla 3. Incluir actividades prácticas.

Interpretación: El (87,5%) de los encuestados considera que el laboratorio debería incorporar más actividades prácticas para reforzar lo aprendido (Figura Nº2). Esto demuestra que los estudiantes valoran el trabajo aplicado como parte esencial de su formación. Aunque un (12,5%) respondió un tal vez sí y ningún estudiante indicó que no lo considera necesario (Tabla Nº3).

Conclusión: Los resultados nos indican una necesidad clara de mejorar el componente práctico en el laboratorio de Redes. Es importante ampliar las oportunidades de practicar, ya que los estudiantes reconocen que practicar les ayuda a entender mejor la parte teórica y a prepararse para situaciones reales.

Pregunta N°3: ¿Qué tan importante consideras practicar configuraciones de red en un entorno controlado antes de aplicarlas en redes reales?

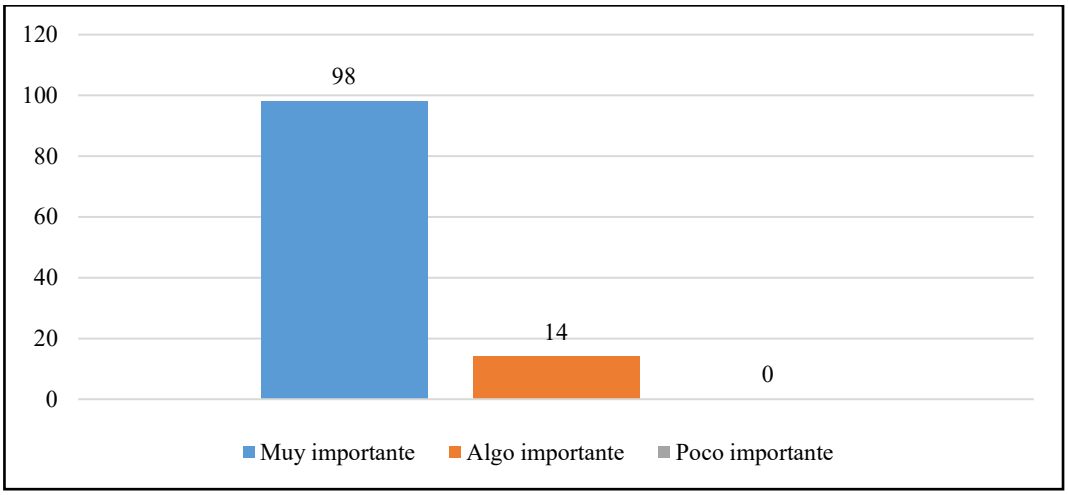


Figura 3. Practicar configuraciones de red en un entorno controlado.

Respuesta	Votos	Porcentaje
Muy importante	98	87.5%
Algo importante	14	12.5%
Poco importante	0	0%
Total	112	100%

Tabla 4. Practicar configuraciones de red en un entorno controlado.

Interpretación: El (87,5%) de los estudiantes considera que practicar configuraciones de red en un entorno controlado es muy importante antes de aplicarlas en redes reales (Figura Nº3). Un (12,5%) considera algo importante, mientras que ningún estudiante lo percibe como poco relevante (Tabla Nº4).

Conclusión: Los resultados reflejan que los estudiantes necesitan un entorno controlado como herramienta para el aprendizaje técnico. Fundamentando seguir promoviendo espacios de simulación y práctica guiada, ya que permite reducir errores, mejorar conocimientos y preparar al estudiante para situaciones reales con mayor seguridad.

Pregunta N°4: ¿Has utilizado algún programa para simular redes informáticas como Packet Tracer durante clases?

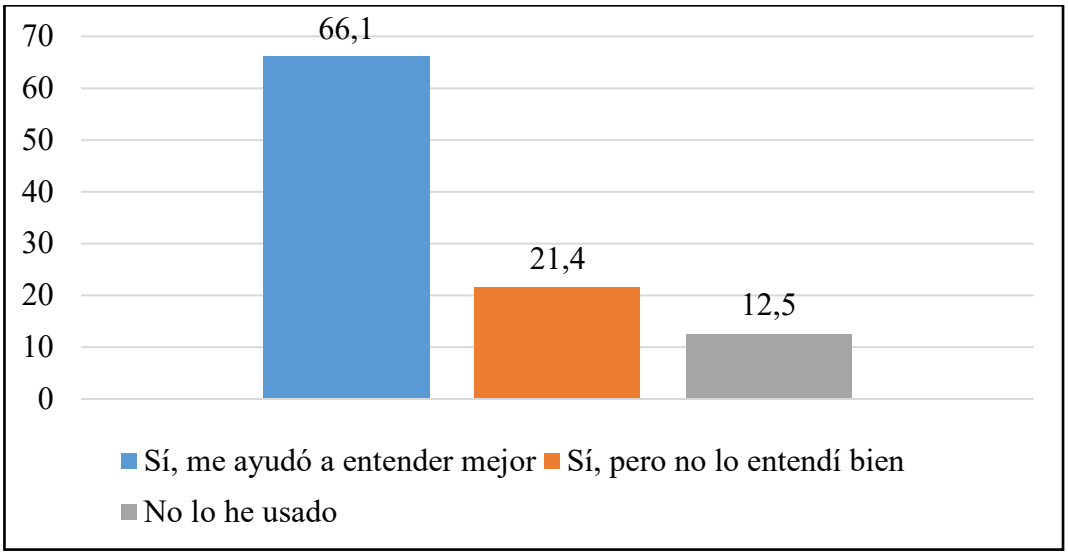


Figura 4. Programas para simular redes informáticas.

Respuesta	Votos	Porcentaje
Sí, me ayudó a entender mejor	74	66.1%
Sí, pero no lo entendí bien	24	21.4%
No lo he usado	14	12.5%
Total	112	100%

Tabla 5. Programas para simular redes informáticas.

Interpretación: El (66,1%) de estudiantes encuestados ha utilizado simuladores como Packet Tracer y considera que le ayudaron a comprender mejor los contenidos (Figura Nº4). Un (21,4%) también los ha usado, pero no logró entenderlos, lo que podría indicar la necesidad de mayor guía del docente. Por otro lado, un (12,5%) no ha tenido contacto con este tipo de herramientas (Tabla Nº5).

Conclusión: Los resultados muestran que los simuladores son útiles para el aprendizaje práctico. Sin embargo, es importante reforzar su uso con explicaciones y ejercicios guiados, para que todos los estudiantes puedan aprovechar su potencial.

Pregunta N°5: ¿Crees que el uso de simuladores en el laboratorio de Redes puede mejorar el aprendizaje práctico?

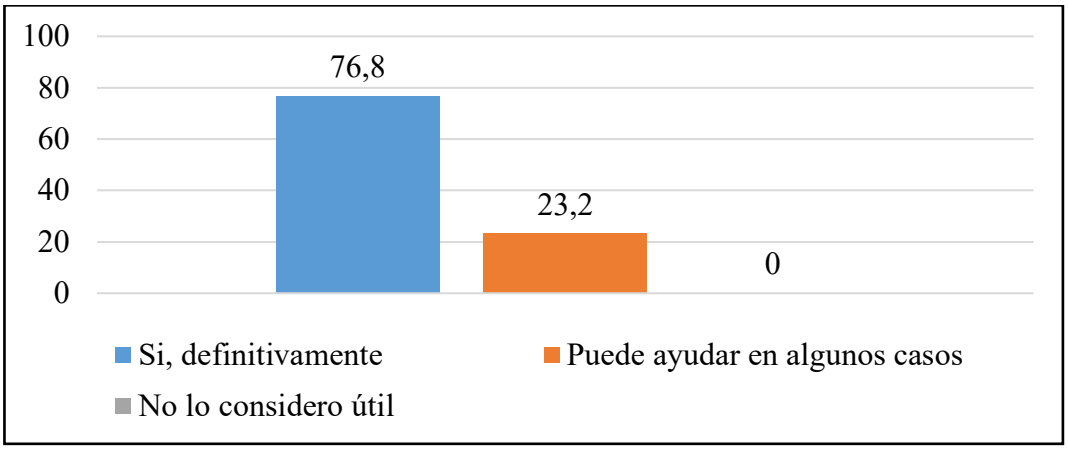


Figura 5. Uso de simuladores en el Laboratorio de Redes.

Respuesta	Votos	Porcentaje
Si, definitivamente	86	76.8%
Puede ayudar en algunos casos	26	23.2%
No lo considero útil	0	0%
Total	112	100%

Tabla 6. Uso de simuladores en el Laboratorio de Redes.

Interpretación: El (76.8%) considera que el uso de simuladores en el laboratorio de Redes mejora el aprendizaje práctico (Figura Nº5). Un (23,2%) piensa que pueden ser útiles en algunos casos, mientras que ningún estudiante los considera innecesarios (Tabla Nº6). Señalando que hay una opinión generalizada del uso de simuladores como herramientas de enseñanza.

Conclusión: Los resultados indican que los simuladores son herramientas clave para reforzar el aprendizaje técnico, por ello es recomendable seguir incorporándolos en las prácticas, ya que permiten experimentar configuraciones, visualizar procesos y entender el funcionamiento de redes, sin comprometer entornos reales.

Pregunta N°6: ¿Crees importante aprender a proteger tu información personal frente a riesgos de seguridad informática?

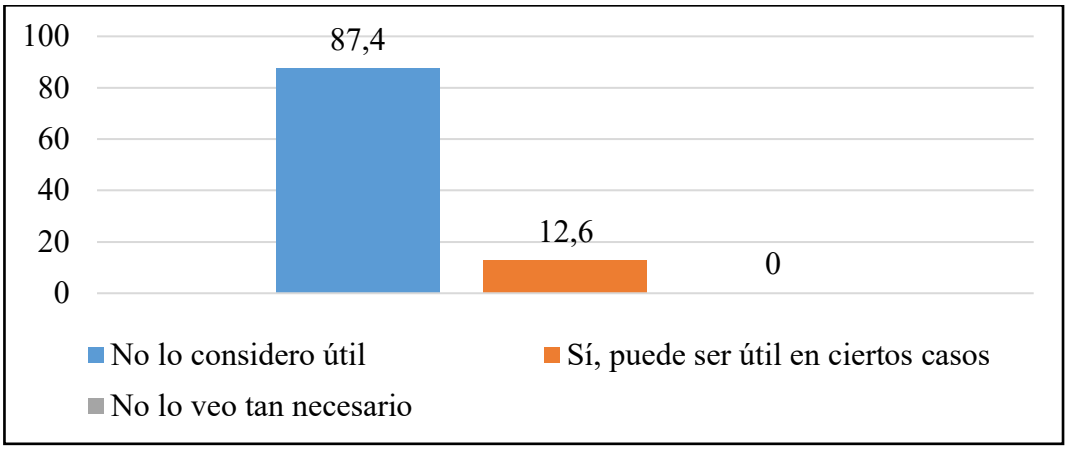


Figura 6. Aprender a proteger tu información.

Respuesta	Votos	Porcentaje
Sí, me parece muy importante	97	87.4%
Sí, puede ser útil en ciertos casos	14	12.6%
No lo veo tan necesario	0	0%
Total	112	100%

Tabla 7. Aprender a proteger tu información.

Interpretación: El (87,4%) indica que aprender a proteger la información personal frente a riesgos de seguridad informática es muy importante (Figura Nº6). Un (12,6%) cree que puede ser útil en ciertos casos, mientras que ningún estudiante lo considera innecesario (Tabla Nº7). Esto muestra que existe una consideración sobre la importancia de la seguridad en entornos académicos y personales.

Conclusión: Los resultados reflejan que los estudiantes reconocen la importancia de adquirir conocimientos sobre protección de datos. Es recomendable incluir contenidos relacionados con seguridad informática en las prácticas del laboratorio, ya que esto contribuirá a que los estudiantes tomen conciencia frente a amenazas digitales.

Pregunta N°7: ¿Consideras importante aprender a identificar problemas de red mediante el monitoreo del tráfico?

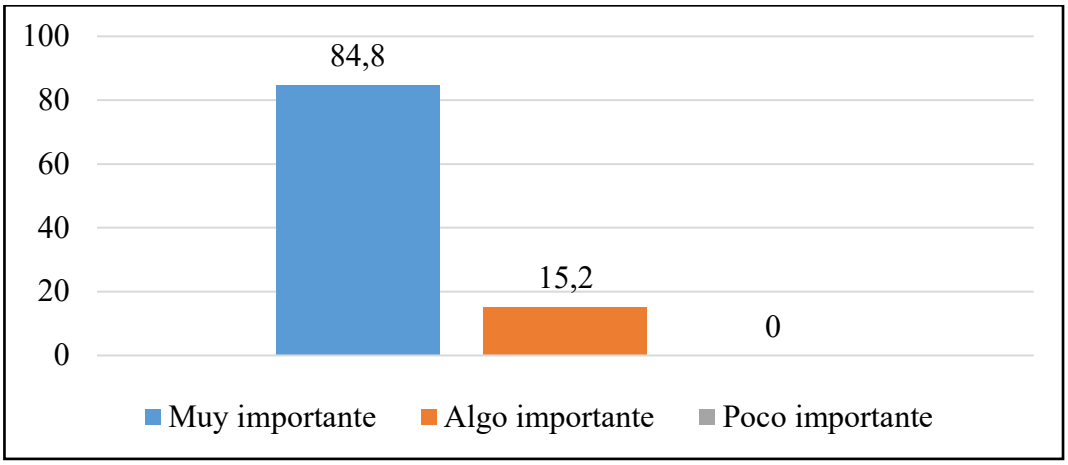


Figura 7. Identificar problemas de red.

Respuesta	Votos	Porcentaje
Muy importante	95	84.8%
Algo importante	17	15.2%
Poco importante	0	0%
Total	112	100%

Tabla 8. Identificar problemas de red.

Interpretación: El (84,8%) de los estudiantes encuestados considera que lograr aprender a identificar problemas mediante el tráfico de la red es muy importante (Figura Nº7). Un (15,2%) dice que es algo importante, mientras que ningún estudiante lo considera como poco relevante (Tabla Nº8). Esto refleja que el uso de herramientas de monitoreo es importante para el diagnóstico y la gestión eficiente de redes.

Conclusión: El monitoreo de tráfico debe incorporarse en las prácticas del laboratorio de Redes, ya que permite observar el comportamiento de la red en tiempo real, interpretar datos y detectar anomalías. Estas actividades fortalecen la capacidad de análisis técnico y la resolución de problemas en entornos reales.

Pregunta N°8: ¿Qué aspecto de infraestructura te gustaría que se mejore en el laboratorio de Redes para facilitar el aprendizaje?

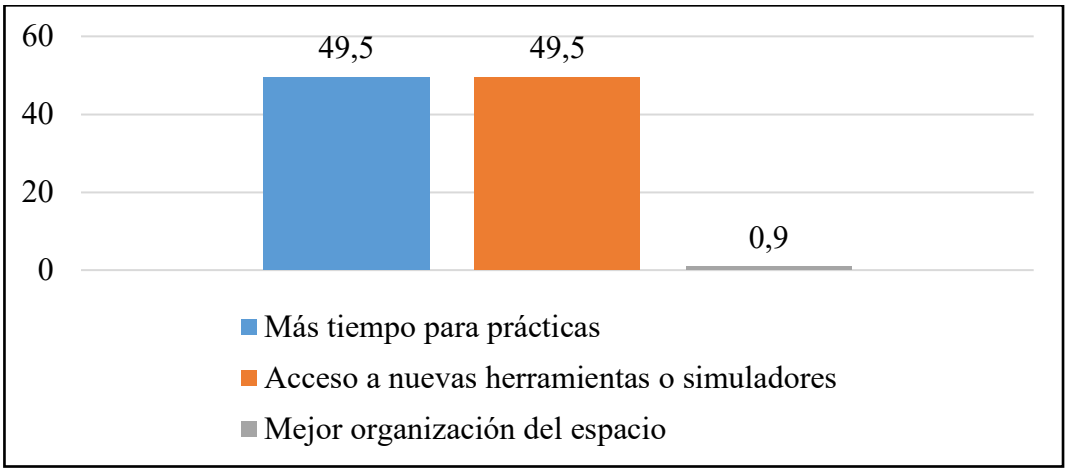


Figura 8. Mejoras en el Laboratorio de Redes.

Respuesta	Votos	Porcentaje
Más tiempo para prácticas	55	49.5%
Acceso a nuevas herramientas o simuladores	55	49.5%
Mejor organización del espacio	1	0.9%
Total	112	100%

Tabla 9. Mejoras en el Laboratorio de Redes.

Interpretación: Los estudiantes encuestados se dividen entre dos necesidades principales el (49,5%) considera que debe ampliar el tiempo a prácticas, mientras que el (49,5%) sugiere mejorar el acceso a nuevas herramientas o simuladores (Figura Nº8). Solo un (0.9%) menciona la organización del espacio físico como un aspecto a mejorar (Tabla Nº9).

Conclusión: Los resultados reflejan que los estudiantes toman en cuenta tanto el tiempo disponible para aplicar conocimiento como el acceso a herramientas. Es recomendable revisar la planificación de las sesiones prácticas y explorar nuevas plataformas o simuladores que complementen el aprendizaje. Aunque la infraestructura física no fue necesaria, su mejora también puede contribuir a una experiencia más cómoda.

2.3.6 Metodología de desarrollo

Para llevar a cabo el proyecto se utilizará la metodología PDCA, conocida como ciclo de mejora continua o ciclo de Deming, ya que se ajusta a proyectos de simulación e implementación de infraestructura de red [46]. Aunque esta metodología se compone de cuatro etapas, en este caso se ha ajustado a cinco fases que responden a las necesidades del desarrollo del entorno controlado (Figura N°9). Las fases consideradas son: recolección de información, diseño del entorno controlado, implementación, pruebas y elaboración de reporte.

Figura 9. Metodología PDCA.

Fase I: Recolección de información

Se aplicará una encuesta a los estudiantes que reciben clases en el laboratorio de Redes, utilizando un muestreo no probabilístico por conveniencia estratificada con el fin de obtener información sobre el estado actual del monitoreo de tráfico en el entorno académico y establecer una base diagnóstica para justificar la propuesta de mejoras (Ver Anexo 1). Además, se llevará a cabo una revisión técnica de los equipos de enrutamiento con el propósito de seleccionar el dispositivo que ofrezca capacidades de captura y análisis de datos en tiempo real.

Fase II: Diseño del entorno controlado

Se elaborará una topología de red que incorpore el router Omada ER7206 v2 como elemento central de la infraestructura. Se seleccionarán herramientas de análisis

como Omada Controller y se desarrollará un script en Python para procesar archivos en formato CSV, permitiendo extraer estadísticas, identificar patrones de tráfico y alertas relevantes.

Fase III: Implementación

Se llevará a cabo la instalación y configuración del equipo que se integrará en el laboratorio de Redes y conectado a la infraestructura tecnológica existente. Se establecerán parámetros para la captura y el análisis del tráfico.

Fase IV: Pruebas

Se procederá a realizar pruebas de monitoreo en tiempo real utilizando la plataforma Omada Controller junto al análisis de archivos CSV mediante el script desarrollado en Python, lo que permitirá visualizar el comportamiento del tráfico, validar la eficiencia del entorno implementado y evaluar su rendimiento frente a distintos escenarios simulados.

Fase V: Reporte

Se desarrollará un manual de funcionamiento que documente los procesos de instalación, configuración y pruebas de análisis de tráfico. El documento incorporará instrucciones detalladas para el uso de herramientas de monitoreo y el script utilizado para el procesamiento de datos, sirviendo como guía técnica.

CAPÍTULO 3. PROPUESTA

3.1 Requerimientos

3.1.1 Requerimientos funcionales

Requerimiento	Descripción del requerimiento
RF1	El sistema debe capturar tráfico de red en tiempo real mediante el Router Gigabit Omada, instalado en el laboratorio de Redes, garantizando la recolección continua de datos para su posterior análisis.
RF2	El sistema debe permitir la visualización del flujo de datos a través de la plataforma Omada Controller, mostrando picos de tráfico, dispositivos conectados, topología de red y generando alertas ante anomalías detectadas en la infraestructura.
RF3	Generar archivos en formato CSV que contengan el registro del tráfico de red, tales como: nombre del dispositivo, dirección MAC, dirección IP, hora de inicio, volumen de descarga, alertas y eventos asociados.
RF4	Procesar los archivos CSV mediante un script desarrollado en lenguaje de Python con el fin de extraer estadísticas, identificar patrones de comportamiento y detectar anomalías en el uso de la red.
RF5	Permitir la evaluación del rendimiento de la red bajo distintos escenarios simulados, facilitando la toma de decisiones técnicas orientadas a ajustes, mejoras o intervenciones preventivas.
RF6	Documentar los procesamientos de instalación, configuración y pruebas en un manual técnico de funcionamiento accesible para estudiantes y docentes como guía de uso.

Requerimiento	Descripción del requerimiento
RF7	El sistema debe operar dentro de un entorno académico controlado, sin comprometer la infraestructura institucional ni interferir con el funcionamiento de otros servicios de red existentes.

Tabla 10. Requerimientos funcionales.

3.1.2 Requerimientos no funcionales

Requerimiento	Descripción del requerimiento
RF1	El sistema debe operar de forma continua durante sesiones de prácticas en el Laboratorio de Redes, sin interrupciones que comprometan la captura ni el monitoreo del tráfico de red.
RF2	El procesamiento de datos debe ser en tiempo real, permitiendo una visualización continua del comportamiento de la red con baja latencia.
RF3	La plataforma de monitoreo debe contar con una interfaz gráfica que facilite la interpretación por parte de estudiantes y docentes.
RF4	El sistema debe permitir ajustes en la configuración, incorporación de nuevas reglas de análisis y mejoras en el script Python sin afectar la operatividad del entorno.
RF5	Permitir la integración de nuevos dispositivos o herramientas sin requerir una reestructuración de la infraestructura existente.
RF6	El entorno debe asegurar la seguridad de los datos recolectados, cuidando de no filtrar información sensible y asegurar que el monitoreo se realice bajo parámetros éticos y académicos.

Requerimiento	Descripción del requerimiento
RF7	El sistema debe ser replicable en espacios académicos, facilitando su adopción como recurso didáctico en procesos de formación técnica.

Tabla 11. Requerimientos no funcionales.

3.1.3 Requerimientos de hardware

Dispositivo	Especificaciones técnicas	Descripción funcional
Router VPN Gigabit Omada ER7206 v2	Procesador de alto rendimiento, múltiples puertos WAN, soporte para protocolos VPN (IPSec, OpenVPN, L2TP).	Dispositivo principal para el monitoreo del tráfico de red. Permite capturar y analizar el comportamiento de los usuarios conectados.
Router TP-Link Archer C50	Doble banda (2.4 GHz / 5 GHz), 4 puertos LAN, compatible con IEEE 802.11ac.	Funciona como punto de acceso para los usuarios. Su tráfico es redirigido al router Omada para su análisis y visualización.
Televisión de 45 pulgadas	Entrada HDMI, resolución mínima full HD.	Pantalla principal para visualización de estadísticas, gráficos y paneles de monitoreo generados por el sistema.
Laptop para administración y análisis	Procesador Intel Core i5, 8 GB RAM, conexión Wi-Fi y Ethernet.	Equipo destinado a la configuración del router, ejecución de scripts en Python y análisis de datos.

Dispositivo	Especificaciones técnicas	Descripción funcional
Cable de red (Ethernet)	Categoría 6, longitud ajustable	Permite la conexión física entre los dispositivos de red, asegurando estabilidad en la transmisión de datos.
Mouse y teclado estándar	Conexión USB	Facilitan la interacción directa con la laptop durante la configuración, monitoreo y análisis técnico.

Tabla 12. Requerimiento de hardware.

3.1.4 Requerimientos de software

Software	Descripción funcional
Python	Lenguaje de programación utilizado para desarrollar el script que analiza los archivos CSV generados por el sistema de monitoreo. Permite extraer estadísticas, identificar patrones de tráfico y detectar anomalías.
Omada Controller	Plataforma de gestión centralizada que permite visualizar en tiempo real el comportamiento de la red, gestionar dispositivos conectados y exportar registros para su análisis técnico.
Tp-Link Omada	Aplicación disponible en Google Play que permite conocer el estado de la red desde dispositivos móviles. Facilita el acceso remoto a estadísticas, alertas y configuración básica del sistema.

Software	Descripción funcional
Sistema operativo Windows	Entorno instalado en la laptop utilizada para ejecutar el script en Python, almacenar los archivos CSV y administrar la infraestructura de red.
Archivo CSV	Formato de salida generado por Omada Controller. Contiene registro del tráfico de red que será procesado para su análisis técnico.
Visual Studio Code	Entorno de desarrollo utilizado para escribir, depurar y ejecutar el script en Python. Facilita la organización del código y la integración de librerías necesarias para el análisis.
Librerías de Python (Pandas, Dash, Plotly)	Conjunto de herramientas que permite manipular datos, generar gráficos estadísticos y realizar cálculos sobre registros de tráfico almacenados en formato CSV.

Tabla 13. Requerimiento de software.

3.2 Propuesta tecnológica

La propuesta tecnológica desarrollada en este proyecto tiene como finalidad proponer un entorno controlado para el monitoreo del tráfico de red en el laboratorio de Redes de (FACSISTEL). Este entorno responde a la necesidad de contar con un espacio funcional que facilite la observación del comportamiento de la red, la detección de anomalías y el fortalecimiento del aprendizaje práctico en el ámbito académico.

El diseño incluye la integración del equipo router VPN Gigabit Omada como componente central de la infraestructura, acompañado por la plataforma de gestión Omada Controller, que permite visualizar el flujo de datos en tiempo real, identificar picos de tráfico y generar alertas ante comportamientos inusuales. Se desarrolló un script en lenguaje Python orientado al procesamiento de archivos

CSV, con el propósito de extraer estadísticas, patrones y evidencias para el análisis técnico.

La propuesta se estructura en cinco fases, alineadas a la metodología PDCA, reconocida por su carácter sistemático y su aplicación en procesos de mejora continua. Estas fases permiten organizar de forma ordenada el desarrollo del sistema, así como la validación de cada fase, así como la documentación de los procedimientos realizados. Las fases se dividen de la siguiente manera:

- Fase de recolección de información.
- Fase de diseño del entorno controlado.
- Fase de implementación.
- Fase de pruebas.
- Fase de reporte.

3.3 Fase de recolección de información

3.3.1 Objetivo de la encuesta

La encuesta tiene como objetivo recolectar datos importantes que permitan conocer las condiciones actuales del laboratorio de Redes, así como también su infraestructura tecnológica y el entorno de monitoreo. Las respuestas a la encuesta permitirán identificar oportunidades de mejora que favorezcan a las prácticas académicas. La información que se recolecte será utilizada con fines investigativos y educativos, asegurando la confidencialidad de los estudiantes.

3.3.2 Levantamiento de información

Mediante un muestreo no probabilístico por conveniencia estratificada, se aplicó la encuesta a estudiantes que realizan prácticas en el laboratorio. Los resultados evidenciaron la necesidad de contar con un entorno controlado funcional para el desarrollo de actividades prácticas.

3.3.3 Cuadro comparativo de equipos

Comparativo de routers según capacidades de monitoreo, exportación, configuración e integración IDS/IPS (Tabla N°14).

Marca /Modelo	Monitoreo en tiempo real		Exportación de datos		Configuración		IDS/IPS integrado		Descripción técnica en el entorno controlado	
TP-Link Omada ER7206 v2	Compatible con Omada Controller para visualizar tráfico, dispositivos y protocolos en tiempo real.	✓	Permite exportar registros en formato CSV para análisis externo.	✓	Mediante interfaz web, app móvil y controlador SDN.	✓	Incluye IDS/IPS nativo, permite integración con sistemas externos.	✓	Ideal para entornos educativos por su gestión centralizada, soporte VPN, segmentación por VLAN y compatibilidad con múltiples protocolos [36].	✓
MikroTik RB4011	Ofrece monitoreo detallado mediante RouterOS con herramientas como Torch y gráficos de tráfico.	✓	Exportación posible vía Syslog, SNMP o scripts personalizados.	✓	Requiere conocimientos técnicos en RouterOS.	X	No incluye IDS/IPS integrado, pero permite con Snort o Suricata.	X	Alto en rendimiento y personalización, requiere un aprendizaje elevado para usuarios sin experiencia, por lo tanto, no es recomendable para entornos educativos [47].	X

Marca /Modelo	Monitoreo en tiempo real		Exportación de datos		Configuración		IDS/IPS integrado		Descripción técnica en el entorno controlado	
Cisco RV345	Monitoreo en tiempo real desde interfaz web con estadísticas de tráfico, QoS y dispositivos.	✓	Exportación de datos mediante Syslog, SNMP y registros internos.	✓	Interfaz intuitiva y asistente de configuración.	✓	Incluye IDS/IPS, firewall SPI, filtrado de contenido y control de aplicaciones.	✓	Recomendado para entornos que requieren seguridad avanzada, aunque su costo y enfoque empresarial pueden limitar su adopción académica [48].	X
Ubiquiti EdgeRouter 4	Monitoreo en tiempo real mediante EdgeOS y Deep Packet Inspection (DPI).	✓	Exportación mediante CLI, Syslog, integración con servidores externos.	X	Requiere configuración por CLI o interfaz avanzada.	X	IDS/IPS disponible en modelos UniFi con suscripción CyberSecure, EdgeRouter requiere integración externa.	X	No es recomendable para entornos académicos debido a su enfoque más técnico, ideal para usuarios avanzados [49].	X

Tabla 14. Cuadro comparativo de equipos de enrutamiento.

3.3.4 Selección de equipo de enrutamiento

Tras el análisis técnico comparativo de los equipos de enrutamiento (Tabla N°14), se seleccionó el TP-Link Omada ER7206 v2 (Figura N°10) como dispositivo principal para la propuesta del entorno controlado de monitoreo en el Laboratorio de Redes. Esta elección responde a su capacidad para capturar tráfico en tiempo real, exportar registros en formato CSV y administrar la red.

Su integración nativa con la plataforma Omada Controller permite una gestión eficiente del entorno, visualización detallada del comportamiento de los dispositivos conectados y la posibilidad de realizar configuraciones remotas desde distintos dispositivos. Adicionalmente, el ER7206 v2 se distingue frente a otros equipos por su interfaz amigable, permite que sea compatible con herramientas de análisis y facilidad de replicación.

Figura 10. Router Omada ER7206.

3.4 Fase de diseño del entorno controlado

3.4.1 Arquitectura de red

La arquitectura de red implementada en el entorno controlado del Laboratorio de Redes se basa en un modelo jerárquico funcional, que permite organizar los dispositivos según su rol técnico, facilitando la gestión del tráfico, la segmentación de servicios y la supervisión en tiempo real (Figura N°11).

En la capa central, se ubica el Router Omada ER7206, conectado al switch del rack de comunicaciones, el cual recibe conectividad desde el proveedor institucional. La

capa de distribución incorpora un punto de acceso TP-Link Archer C50s, encargado de extender la conectividad inalámbrica a los dispositivos de usuario.

La capa de transición incluye un router MikroTik, destinado a pruebas de conectividad local en IPv6, mientras que la capa de almacenamiento integra un NAS para el resguardo de registros de monitoreo. En la capa de acceso, se encuentran los dispositivos utilizados por estudiantes, como portátiles y dispositivos móviles. Finalmente, la capa de monitoreo centraliza la gestión mediante un PC controlador con Omada Controller, accesible desde navegador web, aplicación móvil y controlador en la nube.

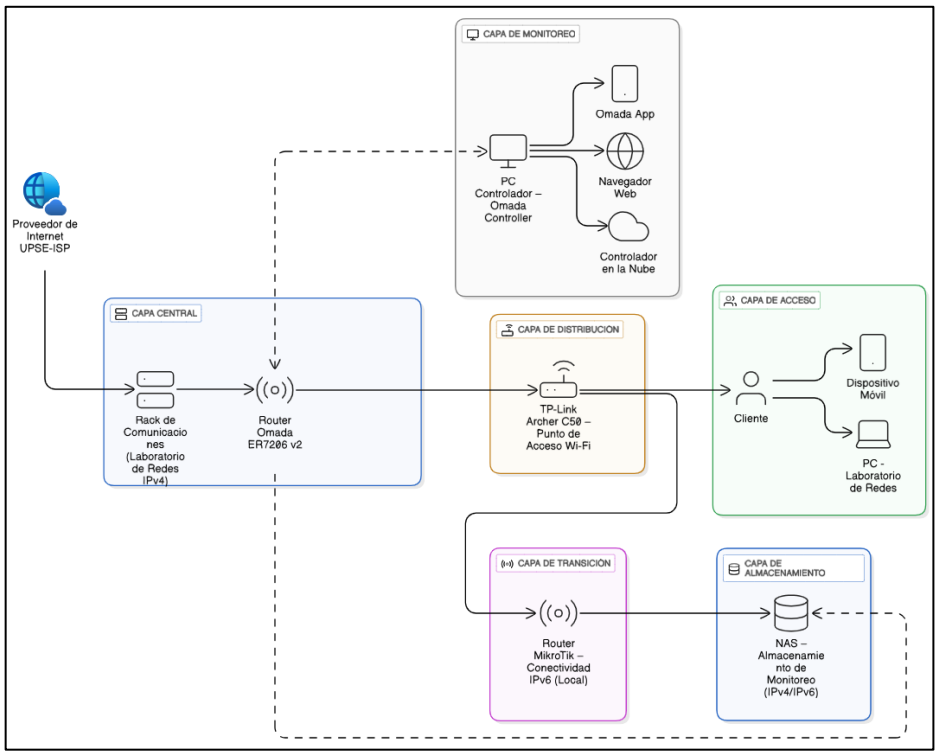


Figura 11. Arquitectura de red.

3.4.2 Topología de red

La topología de red responde a un modelo jerárquico mixto, que combina conectividad cableada e inalámbrica para facilitar la gestión, el monitoreo y el almacenamiento de tráfico en tiempo real. Esta disposición permite simular y gestionar escenarios reales, cada uno de sus componentes con su función dentro del entorno de monitoreo, lo que favorece el análisis técnico y la comprensión estructural de la infraestructura (Figura N°12).

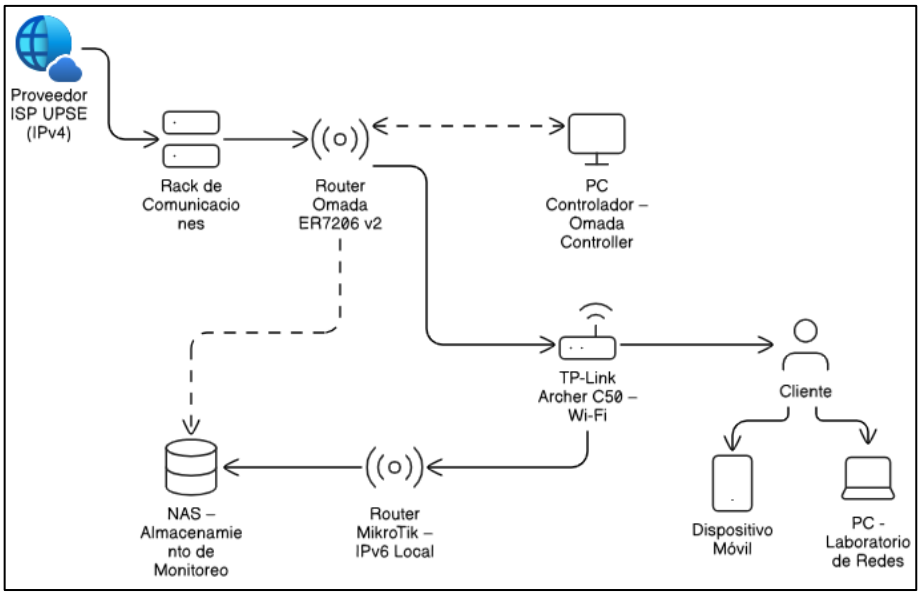


Figura 12. Topología de red.

3.4.3 Implementación del área de monitoreo

Se incorporó una televisión de 45 pulgadas en el área de trabajo del Laboratorio, con el propósito de facilitar la visualización de la interfaz gráfica del sistema de monitoreo (Figura N°13). Esta pantalla permite acceder en tiempo real a las estadísticas, alertas y comportamiento del tráfico de red, tanto desde el navegador web. Al tratarse de un televisor con sistema operativo Android, se optimiza su uso como herramienta de apoyo visual, fortaleciendo el aprendizaje práctico y la comprensión técnica de los estudiantes durante sesiones académicas.

Figura 13. Incorporación del área de monitoreo.

3.4.4 Selección de herramientas de análisis

Para el monitoreo de tráfico de red, se seleccionó la plataforma Omada Controller como herramienta principal. Esta solución permite visualizar en tiempo real el comportamiento de los dispositivos conectados, generar estadísticas de uso, identificar picos de tráfico y exportar registros en formatos CSV. Su integración nativa con el router Omada garantiza una gestión centralizada, accesible desde el navegador web, lo que facilita la propuesta para entornos académicos.

Asimismo, se definió el uso de Python como lenguaje de programación para el desarrollo de un script orientado al análisis de los archivos CSV generados por el sistema. Se incorporan librerías como pandas, dash y plotly, las cuales ofrecen herramientas para el análisis estadístico y representación gráfica interactiva.

3.4.5 Plan de pruebas y procedimientos

Este plan contempla procedimientos para evaluar el rendimiento del sistema, estabilidad de la conexión, capacidad de monitoreo en tiempo real y la exportación de datos para análisis (Tabla N°15).

Prueba	Objetivo	Procedimiento	Indicador
Monitoreo en tiempo real	Validar que el sistema muestre estadísticas del tráfico y dispositivos conectados.	Acceder al panel de Omada Controller, observar el flujo de datos y verificar actualizaciones constantes.	Las estadísticas deben reflejar el comportamiento actual de la red en tiempo real.
Visualización de topología de red	Comprobar que la estructura lógica de la red se represente al conectar nuevos dispositivos.	Ingresar al apartado de Mapa en Omada Controller, conectar un nuevo dispositivo y verificar su aparición.	La topología debe actualizarse automáticamente, mostrando nodos activos y relaciones.

Prueba	Objetivo	Procedimiento	Indicador
Aplicaciones y tráfico por usuario	Evaluar la capacidad del sistema para identificar aplicaciones utilizadas y tráfico generado.	Acceder a estadísticas, seleccionar un usuario y revisar categorías de aplicaciones y tráfico.	El sistema debe mostrar las aplicaciones activas y el tráfico asociado por usuario.
Conectividad por usuarios	Verificar que el sistema identifique correctamente los datos de conexión de cada usuario.	Acceder al panel de clientes, revisar nombre, tipo de conexión, MAC e IP asignada.	Todos los campos deben mostrarse y actualizarse por dispositivo conectado.
Detección de anomalías	Registrar eventos inusuales y generar alertas con información detallada.	Simular comportamientos anómalos y verificar fecha, hora, descripción, gravedad y clasificación.	El sistema debe generar alertas con campos de registro.
Exportación de registros CSV	Comprobar que los datos monitoreados puedan ser exportados para análisis.	Ejecutar la función de exportación en Omada Controller, guardar y verificar la estructura del archivo.	El archivo debe generarse correctamente, con datos legibles y organizados.

Prueba	Objetivo	Procedimiento	Indicador
Acceso desde la web	Validar que la interfaz gráfica del sistema sea accesible.	Ingresar al controlador desde un navegador, verificar navegación y acceso a funciones.	La interfaz debe ser accesible y funcional desde la web.
Ejecución del script en Python	Analizar datos exportados mediante el script desarrollado.	Ejecutar el script sobre un archivo CSV y generar estadísticas con librerías como pandas, dash y plotly.	El script debe ejecutarse sin errores y generar resultados interpretables.

Tabla 15. Plan de pruebas técnicas.

3.5 Fase de implementación

3.5.1 Integración del router Omada al Laboratorio de Redes

Se realizó la instalación en una ubicación estratégica, utilizando un rack para su montaje físico y la visualización de la interfaz gráfica (Figura 14). Se verificó la conectividad, asegurando su reconocimiento dentro del esquema IP institucional.

Figura 14. Integración del Router Omada al Laboratorio de Redes.

3.5.2 Adopción y configuración del router Omada

Las configuraciones iniciales se realizaron desde el apartado Visión global, donde se despliega el estado general del sistema y los dispositivos disponibles para adopción (Figura Nº15).

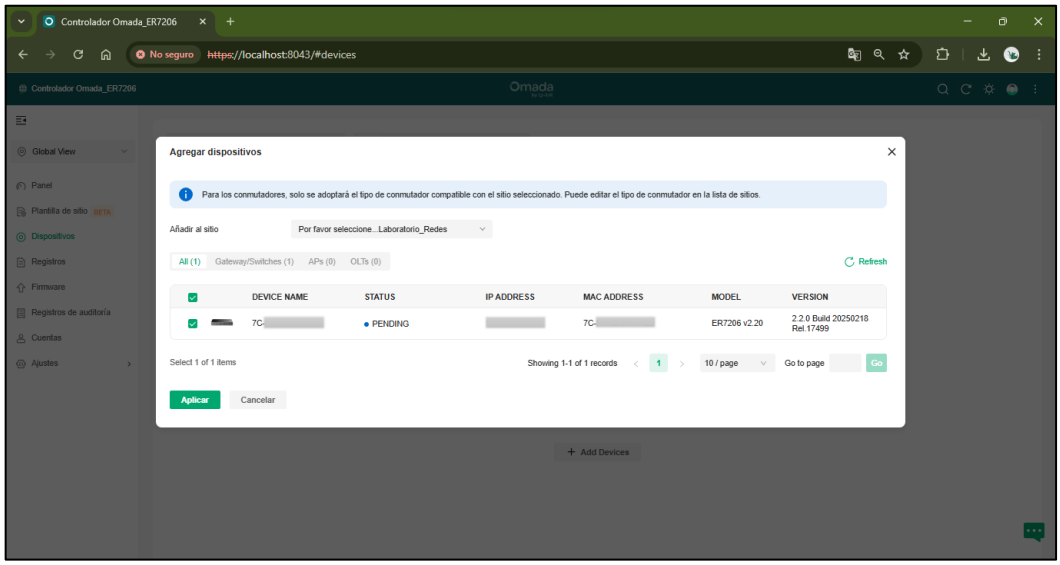


Figura 15. Agregar dispositivo para su adopción.

Este módulo permite que el sistema reconozca el equipo como pendiente, es decir, listo para ser adoptado. Al seleccionar el sitio correspondiente, el sistema solicitará las credenciales previamente creadas para autorizar la adopción (Figura Nº16).

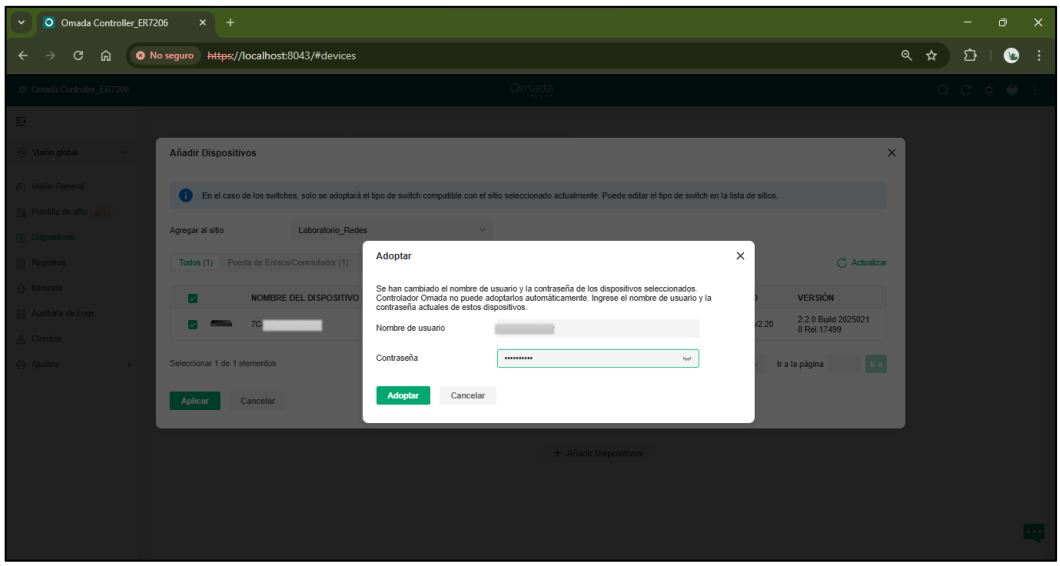


Figura 16. Reconocimiento y autorización para la adopción.

Una vez adoptado, el dispositivo queda vinculado al sitio definido y se habilita su gestión desde la plataforma. Desde el apartado Cuenta, es posible administrar los usuarios registrados por el administrador principal. Cada cuenta puede configurarse con distintos niveles de acceso, funciones específicas y privilegios sobre los sitios disponibles (Figura Nº17).

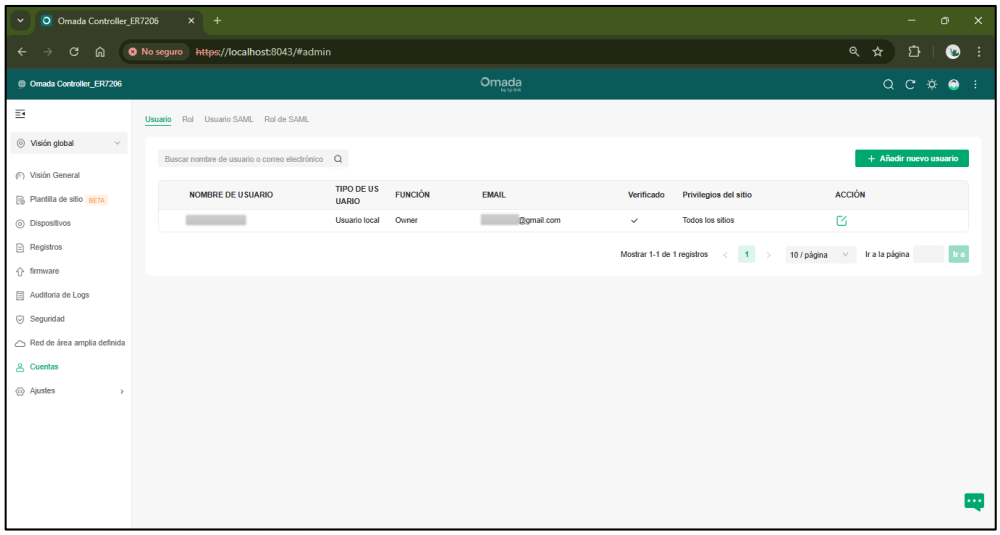


Figura 17. Agregar nueva cuenta para administrar el equipo.

Se procedió a añadir un nuevo usuario con acceso a la nube, funcionalidad que permite ingresar al controlador desde el navegador web (Figura Nº18). En este paso se habilitan los permisos de acceso remoto y se vincula una cuenta de correo electrónico.

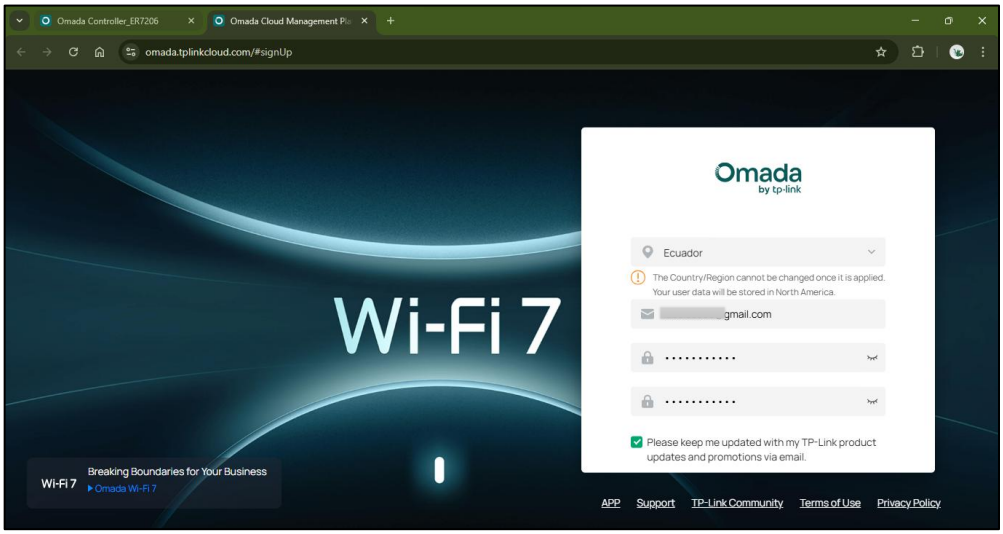


Figura 18. Creación de credenciales para plataforma web.

Una vez verificada la cuenta, se accede al apartado Acceso a la nube, donde se define el correo electrónico y las acciones permitidas para el usuario (Figura N°19). Esta configuración habilita la gestión remota, facilitando el monitoreo y la administración desde cualquier ubicación con acceso a internet.

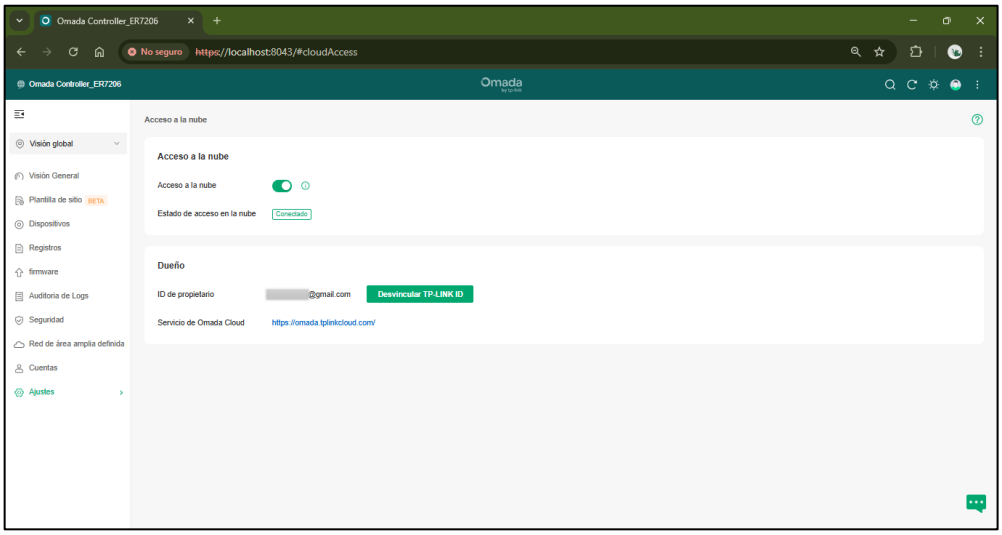


Figura 19. Acceso a la nube.

Desde el apartado Rol, se accede a la gestión de perfiles vinculados al controlador Omada. Los roles disponibles incluyen: Dueño, Super Administrador, Administrador y Visitante, cada uno con distintos niveles de acceso (Figura N°20). Es posible definir acciones tanto para vista global como para los sitios creados, incluyendo permisos de modificación, solo lectura o bloqueo.

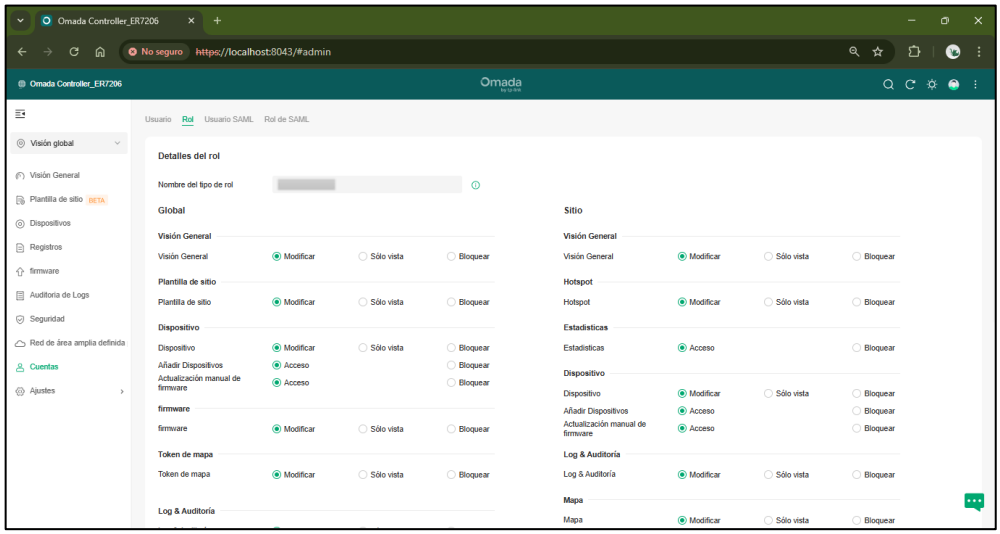


Figura 20. Rol para vista global y sitio.

El módulo de Retención de datos permite almacenar información relacionada con los clientes, el tráfico y anomalías detectadas en la red (Figura N°21). Esta configuración fue ajustada para permitir la utilización de los datos almacenados mediante un script en Python desarrollado para su análisis.

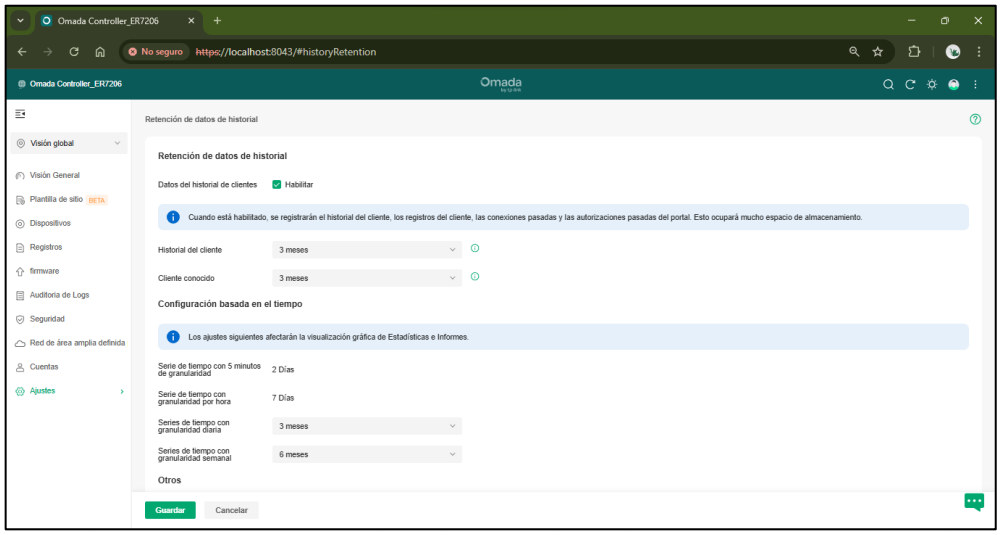


Figura 21. Retención de datos almacenados para pruebas.

Las siguientes configuraciones se realizaron dentro del sitio Laboratorio Redes. Desde el apartado Visión general, se habilitó una vista panorámica del estado de la red, los clientes y el tráfico generado. El sistema permite seleccionar distintos tipos de visualización, incluyendo gráficas de carga, alertas, clientes, tiempo de actividad, aplicaciones por categoría y distribución del tráfico (Figura N°22).

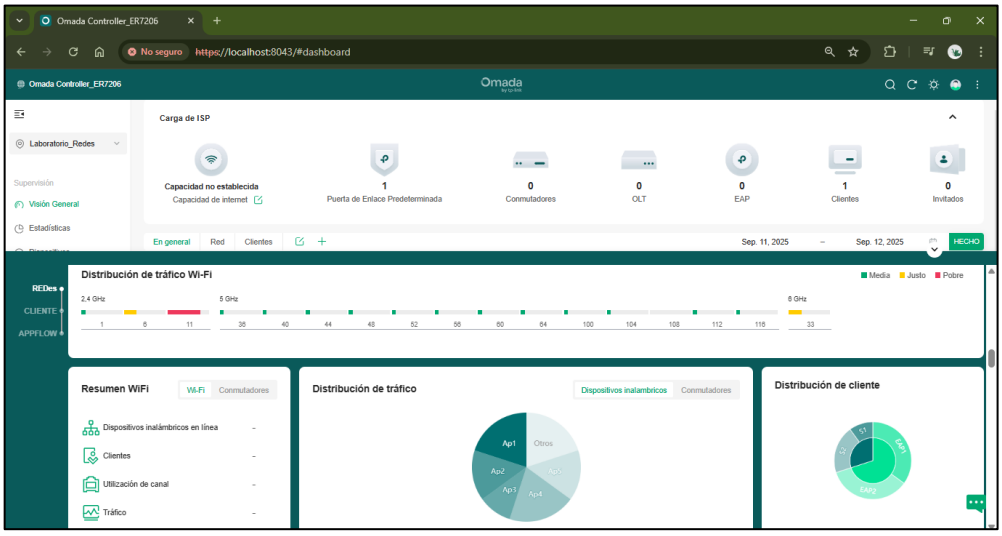


Figura 22. Visualización para dashboard.

Se configuró el mecanismo de detección en línea del router/firewall, el cual verifica la conexión a internet mediante él envió de paquetes de prueba (Figura N°23). Se personalizó el intervalo de verificación a 10 segundos, lo que permite una respuesta rápida ante fallos de conexión, ya sea mediante la reactivación del enlace o la redistribución de la carga entre los enlaces disponibles.

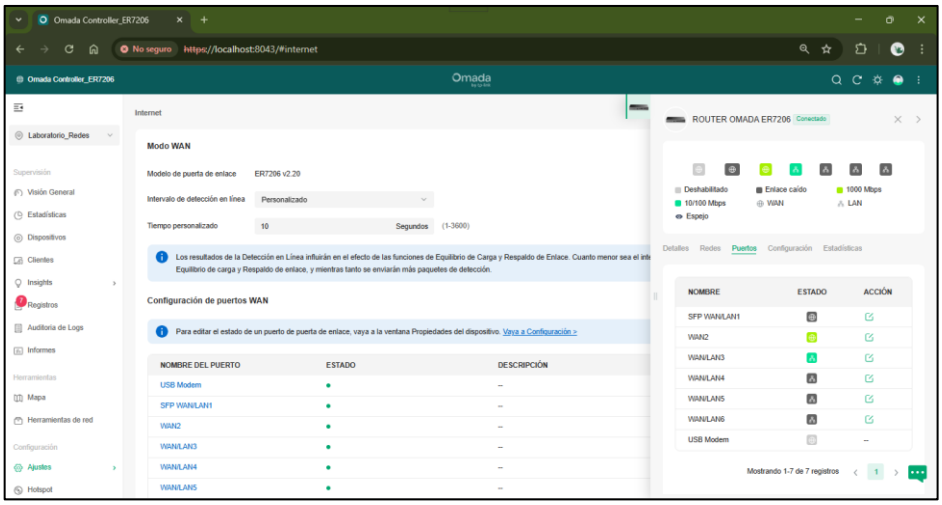


Figura 23. Mecanismo de detección en línea.

Dentro de la configuración de seguridad, se accede a Defensa ante inundación y a Defensa ante paquetes anómalos, que permiten proteger la red frente a tráfico malicioso (Figura N°24). Estas funciones permiten observar el comportamiento del sistema e incluso analizar su respuesta ante eventos anómalos.

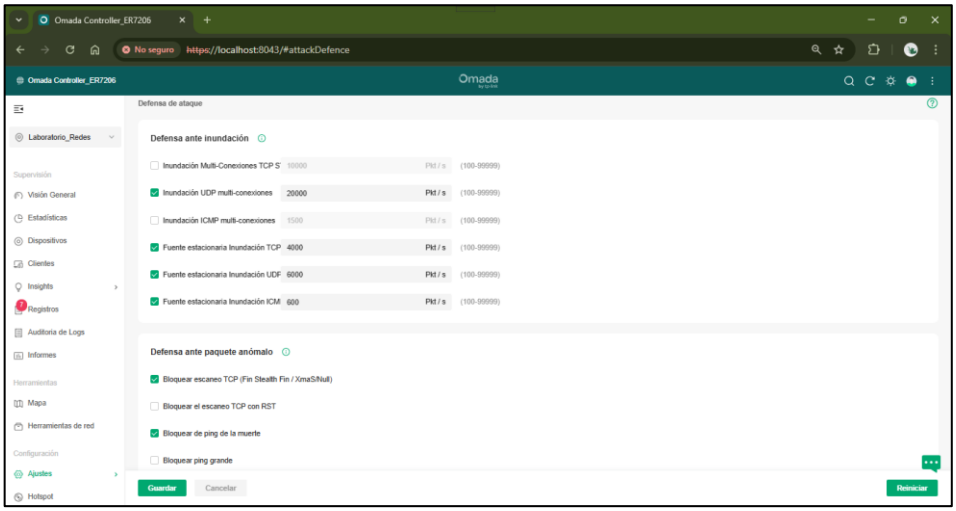


Figura 24. Defensa ante inundación y defensa ante paquetes anómalos.

En el módulo IDS/IPS, se configuró el modo IDS, dado que el entorno controlado del laboratorio requiere observar sin intervenir. Esta configuración permite detectar anomalías sin bloquear el tráfico, facilitando el análisis técnico (Figura N°25). Se definió un nivel de seguridad que abarca categorías como virus, malware y tráfico sospechoso.

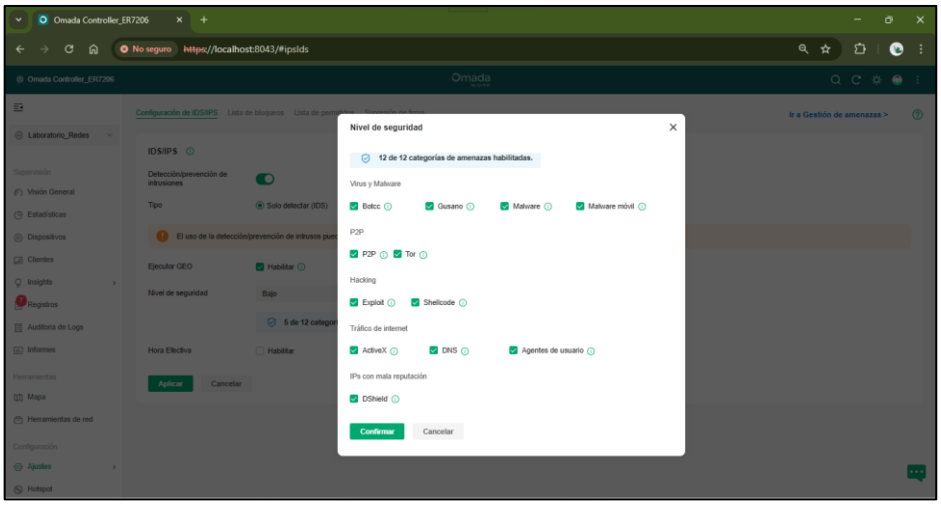


Figura 25. Nivel de seguridad por categoría.

Para complementar el monitoreo, se habilitó la función de inspección profunda de paquetes y el registro de tráfico, permitiendo visualizar el comportamiento de las aplicaciones utilizadas por cada usuario. Esta visualización incluye datos como nombre de la aplicación, categoría, tráfico de subida y bajada y usuarios activos (Figura N°26).

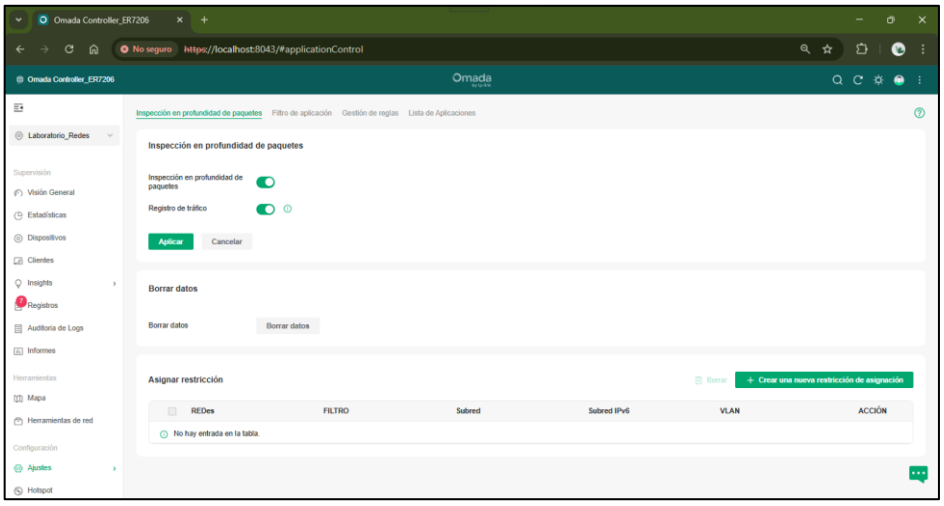


Figura 26. Inspección de paquetes y registro de tráfico.

3.6 Fase de pruebas

Se accedió al apartado Visión general del sistema Omada Controller para observar el flujo de datos en tiempo real (Figura N°27). Las estadísticas de tráfico y los dispositivos conectados se presentaron mediante visualizaciones dinámicas, lo que facilita el monitoreo continuo y permite a los estudiantes interpretar el comportamiento de la red durante las secciones prácticas.

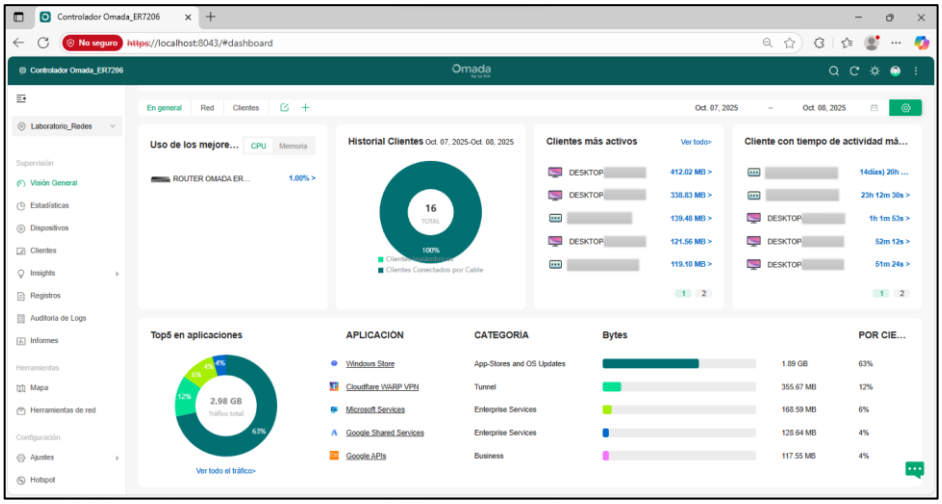


Figura 27. Visualización gráfica en tiempo real.

Cuando los usuarios se conectan al punto de acceso, los dispositivos aparecen automáticamente en el entorno gráfico. El mapa de red muestra los nodos activos y sus relaciones como router, controlador, grupo de usuarios conectados (Figura N°28). Esta representación gráfica refuerza la representación de la arquitectura de red y promueve el aprendizaje técnico.

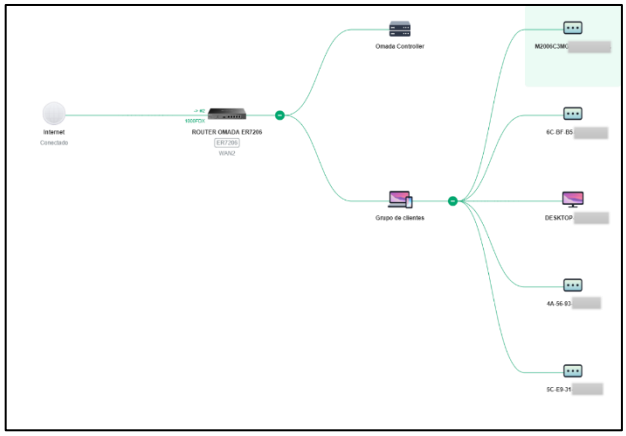


Figura 28. Topología de red generada por el sistema.

Desde el apartado Estadísticas, se accedió al análisis por aplicaciones, donde se identifican los nombres de las aplicaciones utilizadas, su categoría, el tráfico ascendente y descendente, así como los usuarios activos (Figura N°29). Esta información permite evaluar el uso de recursos, detectar patrones y comprender la distribución del tráfico.

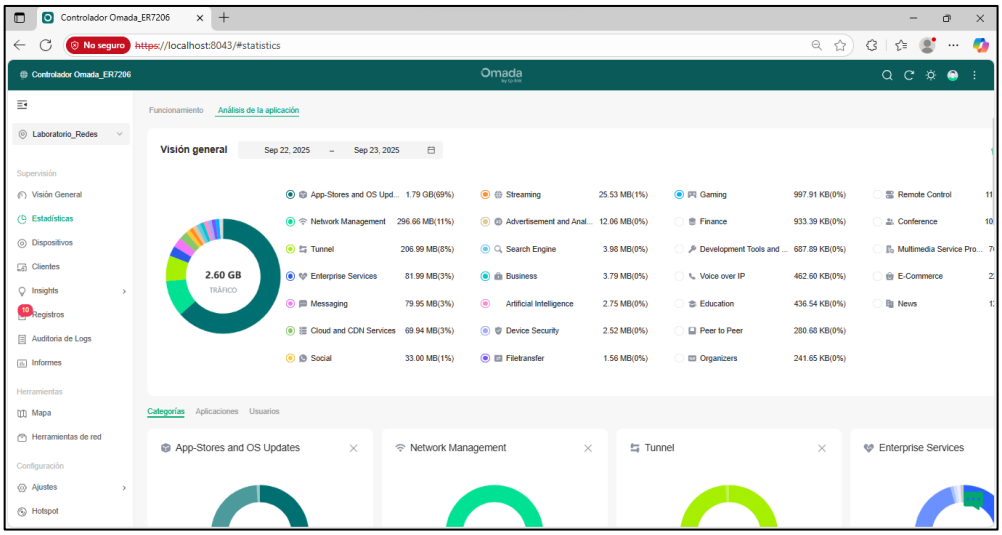


Figura 29. Tráfico generado por aplicaciones.

El sistema emite datos de conexión individual por usuario, con información como nombre, dirección IP, velocidad de descarga, tráfico de subida y tiempo de actividad (Figura N°30). Esta funcionalidad permite un seguimiento personalizado de los dispositivos conectados, facilitando la gestión técnica del entorno.

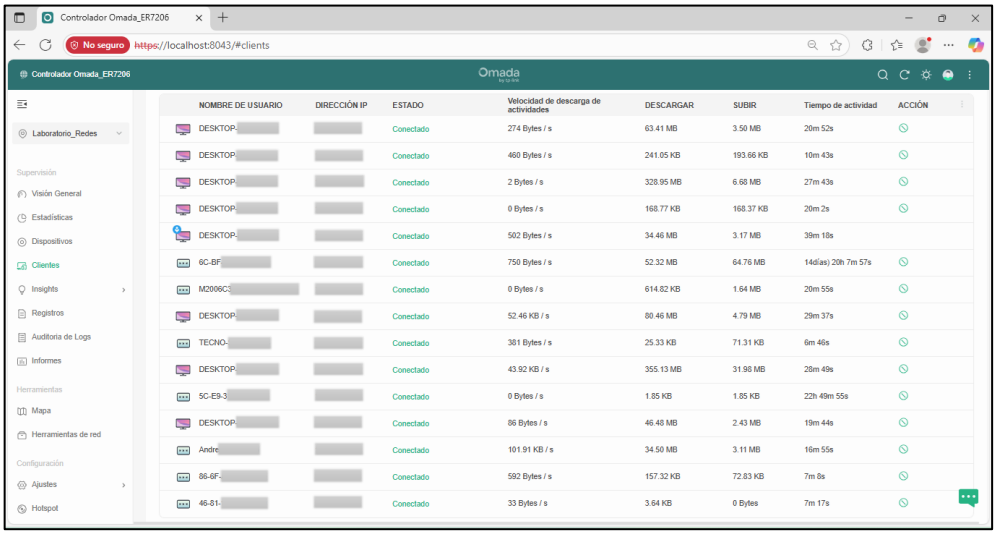


Figura 30. Panel de conectividad por usuario.

Se verificó la capacidad del sistema para generar alertas ante comportamientos anómalos. Los eventos fueron registrados con información geográfica, fecha, hora, descripción, nivel de gravedad y clasificación de la amenaza (Figura N°31). Esta funcionalidad fortalece la seguridad del entorno, permitiendo detectar y documentar incidentes que podrían comprometer la red.

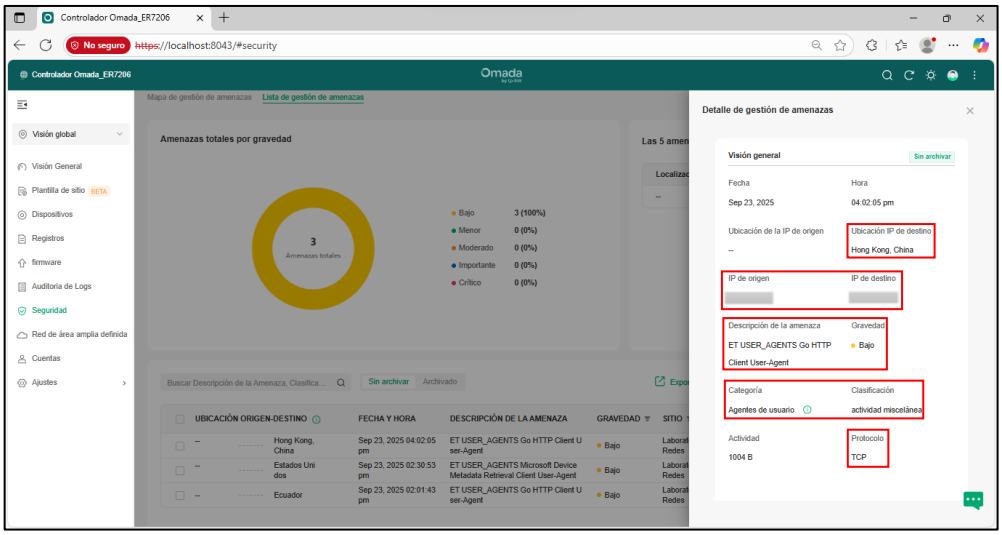


Figura 31. Detección de anomalías.

Se validó el acceso remoto al sistema mediante interfaz gráfica desde otro dispositivo. La navegación fue fluida y las funciones operativas estuvieron disponibles, lo que facilitó la gestión remota por parte del docente o administrador sin necesidad de presencia física en el laboratorio (Figura N°32)

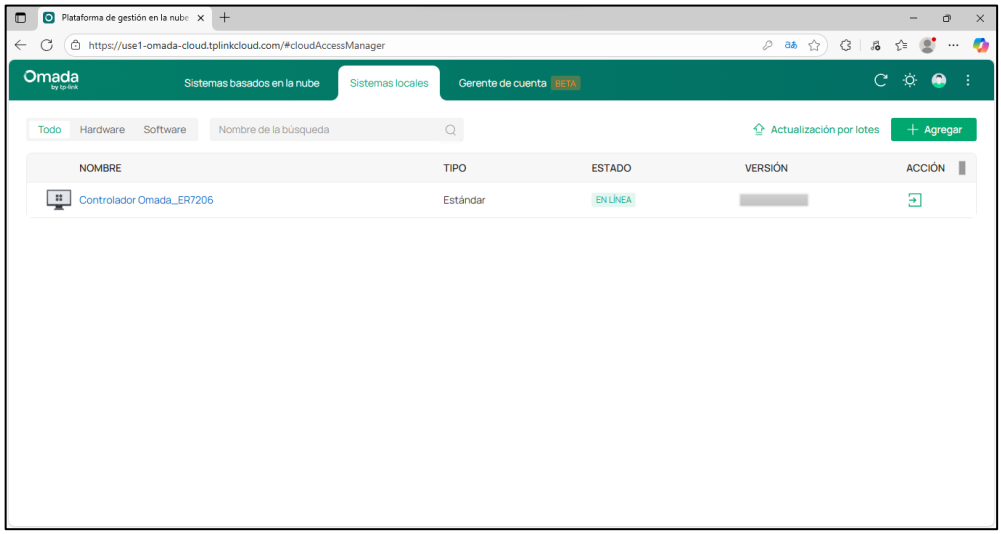


Figura 32. Acceso remoto al sistema.

Finalmente, se aplicó el script desarrollado en Python sobre los archivos CSV exportados por el sistema. El código se ejecutó, generando estadísticas e interpretaciones visuales mediante las librerías pandas, dash y plotly. Esta práctica demuestra que los datos generados por el equipo de enrutamiento pueden ser procesados con herramientas externas, fortaleciendo la capacidad de análisis técnico por parte de los estudiantes (Figura N°33).

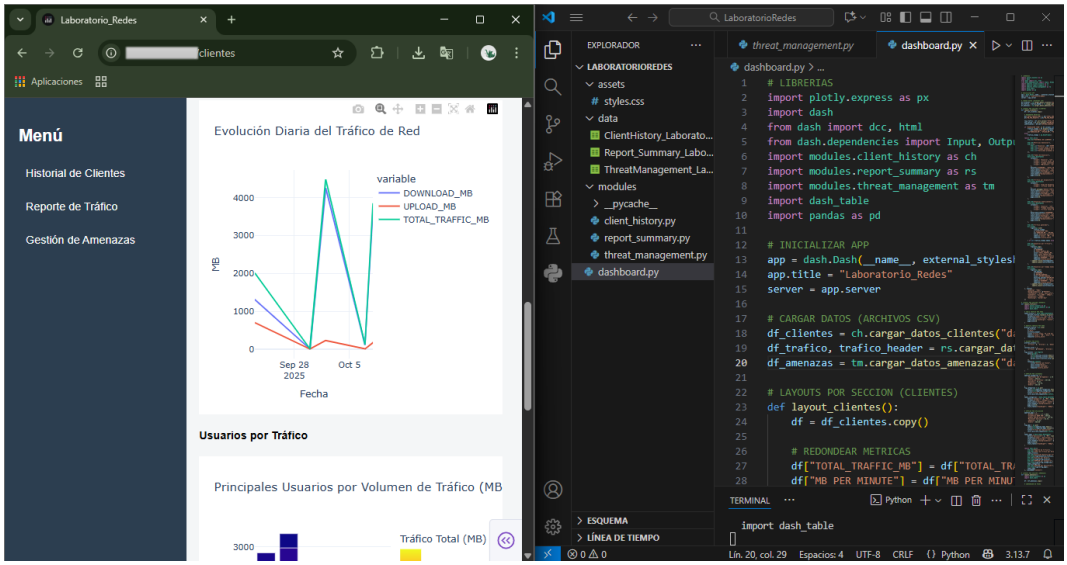


Figura 33. Desarrollo con herramientas externas.

3.7 Fase de reporte

La elaboración del manual de funcionamiento tiene como propósito documentar los procedimientos de instalación, configuración y ejecución de pruebas dentro del entorno de monitoreo. El documento incorpora instrucciones detalladas sobre el uso del router ER7206 v2, la plataforma Omada Controller y el script desarrollado en Python para el análisis de tráfico generado a partir de archivos en formato CSV (Ver Anexo 2).

CONCLUSIONES

- En consecuencia, se realizó una revisión técnica detallada de los equipos de enrutamiento con capacidad de monitoreo de tráfico de red, identificando que el Router Gigabit Omada ER7206 v2 cumple con los requerimientos para capturar y analizar datos en tiempo real. Su integración con la plataforma Omada Controller permitió validar su eficiencia en entornos controlados, ofreciendo visualización dinámica del comportamiento de la red, generación de estadísticas y detección de anomalías. La propuesta responde a la necesidad de recrear situaciones reales y aprender a gestionar el tráfico de red de manera segura, permitiendo prácticas académicas en escenarios simulados de riesgo y supervisión.

- En cuanto al análisis de los resultados obtenidos a través de las herramientas de monitoreo, se evidenciaron mejoras en la supervisión del tráfico de red. La visualización en tiempo real, el registro de eventos y el procesamiento de datos en formato CSV mediante Python permitieron identificar patrones de uso, evaluar el rendimiento de la red y detectar anomalías. Durante el periodo de pruebas de un mes, se analizaron 310 registros de conexión, con un tráfico total superior a 882 GB y se identificaron 35 amenazas clasificadas como de baja severidad, asociadas principalmente a actividades de tipo agentes de usuario. Las categorías más frecuentes fueron actividades misceláneas, violación de políticas y actividad de tipo troyano, lo que evidenció la capacidad del entorno para detectar comportamientos anómalos y consolidar métricas de comportamiento.

- Se elaboró un manual técnico de funcionamiento que documenta de forma clara y estructurada los procesos de instalación, configuración, pruebas y análisis del entorno controlado de monitoreo. Este recurso facilita la replicabilidad del proyecto, promueve el uso autónomo de las herramientas implementadas y fortalece la formación práctica de los estudiantes en el área de redes. El manual es un instrumento para la sostenibilidad del entorno dentro del laboratorio de FACSISTEL.

RECOMENDACIONES

- Una vez concluido el presente ensayo de titulación, se recomienda continuar con la evaluación técnica de equipos de enrutamiento que integren funciones avanzadas de seguridad, como segmentación mediante VLANs, control de acceso por MAC y reglas de tráfico personalizadas. Estas medidas permitirán mejorar la protección de los datos y el rendimiento de la red en entornos controlados. Se sugiere considerar la implementación de firewalls complementarios y sistemas de detección de intrusos IPS para robustecer la seguridad informática del laboratorio.

- Antes de finalizar, dado que el entorno fue configurado bajo el protocolo IPv4, se recomienda que futuras investigaciones contemplen la incorporación de IPv6, con el fin de adaptarse a las nuevas exigencias de direccionamiento y compatibilidad en redes modernas. Asimismo, se sugiere integrar módulos de análisis más avanzados que permitan correlacionar eventos, aplicar técnicas de machine learning para detección de anomalías y generar reportes automatizados que faciliten la toma de decisiones en tiempo real.

- Por último, se recomienda mantener el manual técnico actualizado conforme se realicen mejoras en el entorno de monitoreo, incluyendo nuevas versiones de software, cambios en la topología de red o incorporación de nuevas herramientas. Se sugiere utilizar el manual como recurso pedagógico, promoviendo su uso en prácticas de laboratorio y proyectos integrados, con el fin de fortalecer la formación técnica en el área de redes.

Referencias

[1] B. Brito Acosta, D. A. Cruz Bermúdez y M. Denis Márquez, «La comunicación: valiosa herramienta en la gestión organizacional,» *Revista Científica,* vol. 1, nº 36, p. 66–73, 15 Octubre 2023.

[2] O. Foundation, «owasp.org,» Tecnored, 10 Noviembre 2021. [En línea]. Available: https://owasp.org/Top10/es/A09_2021-Security_Logging_and_Monitoring_Failures/. [Último acceso: 22 Agosto 2025].

[3] A. Pickford y G. Thoss, «RNO/ITS – PIARC,» Octubre 2025. [En línea]. Available: https://rno-its.piarc.org/es/monitoreo-de-la-red/tecnologias-de-monitoreo. [Último acceso: 1 Abril 2025].

[4] Universidad Estatal Peninsula de Santa Elena, «Facultad de Sistemas UPSE,» Universidad Estatal Península de Santa Elena, 8 Enero 2016. [En línea]. Available: https://www.upse.edu.ec/facsistel/index.php. [Último acceso: 1 Abril 2025].

[5] R. Hernandez Sampieri, C. Fernandez Collado y P. Baptista Lucio, Metodologia de la investigacion, Mexico: McGraw-Hill Interamericana, 2014.

[6] L. C. Lituma Briones, «Laboratorio virtual de análisis y comportamiento de malware basado en técnicas y métodos de seguridad informática para los laboratorios en la Facultad de Sistemas y Telecomunicaciones,» Universidad Estatal Península de Santa Elena (UPSE), La Libertad, Ecuador, 2020.

[7] M. J. Mendoza Mendoza, «Análisis de vulnerabilidades de seguridad en redes LAN mediante la herramienta NESSUS en la Facultad de Sistemas y Telecomunicaciones de la UPSE,» Universidad Estatal Península de Santa Elena (UPSE), La Libertad, Ecuador, 2023.

[8] F. d. B. Echeverría Sierralta, «Implementación y evaluación de sistema de monitoreo de seguridad basado en flujos de paquetes IP,» Universidad de Chile, Facultad de Ciencias Físicas y Matemáticas, Santiago, Chile, 2008.

[9] Dirección de Desarrollo Estratégico, «Aplicación del Ciclo de Deming o PDCA para la gestión de la calidad en la educación superior: una introducción,» Universidad de Concepción, Concepción, Chile, 2020.

[10] E. Velazquez, «Cybolt LATAM,» Cybolt, 30 Abril 2024. [En línea]. Available: https://cybolt.com/latam/conoce-los-10-beneficios-del-monitoreo-de-red/. [Último acceso: 14 Abril 2025].

[11] Beyond Technology, «Beyond Technology,» Beyond Technology, 09 Diciembre 2024. [En línea]. Available: https://beyondtechnology.net/es/5-beneficios-clave-del-monitoreo-de-red-para-empresas/. [Último acceso: 14 Abril 2025].

[12] Secretaría Nacional de Planificación, «Plan Nacional de Desarrollo 2025–2029: Ecuador no se detiene,» Gobierno del Ecuador, Quito, Ecuador, 2025.

[13] Andrew S. Tanenbaum y David J. Wetherall, Redes de computadoras, Madrid: Pearson Educación, 2011.

[14] Yosen, «Salud Vital,» SaludVital.cl, 14 Septiembre 2024. [En línea]. Available: https://saludvital.cl/comunicacion/que-son-y-como-funcionan-las-redes-de-comunicacion/. [Último acceso: 04 Agosto 2025].

[15] Equipo editorial de IONOS, «IONOS Digital Guide,» IONOS.mx, 06 Septiembre 2019. [En línea]. Available: https://www.ionos.mx/digitalguide/servidores/know-how/los-tipos-de-redes-mas-conocidos/. [Último acceso: 01 Agosto 2025].

[16] B. León, «Guru99,» Guru99.com, 14 Mayo 2025. [En línea]. Available: https://www.guru99.com/es/types-of-computer-network.html. [Último acceso: 04 Agosto 2025].

[17] C. Helmut Sy, «Lifeder,» Lifeder.com, 06 Septiembre 2024. [En línea]. Available: https://www.lifeder.com/topologias-de-red/. [Último acceso: 04 Agosto 2025].

[18] A. V. Figueroa Sánchez y S. A. Herrera Hernández, «Propuesta en educación ambiental no formal para la construcción de conocimiento en torno a los componentes de formación dentro del programa de servicio social ambiental del Jardín Botánico José Celestino Mutis mediante la estrategia de enfoque intercultur,» Universidad Distrital Francisco José de Caldas, Bogotá, Colombia, 2016.

[19] Redacción RedesTelecom, «RedesTelecom.es,» 22 Abril 2024. [En línea]. Available: https://www.redestelecom.es/especiales/arquitectura-de-red-caracteristicas-importancia-y-funcionalidades/. [Último acceso: 31 Octubre 2025].

[20] J. D. Rodríguez Vizuete, R. A. Macías Lara, M. F. Bone Andrade, S. M. Sosa Calero y J. C. Santillan Lima, «Perspectivas y futuro de las infraestructuras de redes en instituciones educativas,» *Dominio de las Ciencias,* vol. Vol. 7, nº 1225–1242, p. 1225–1242, 2021.

[21] IBM, «IBM Mexico,» IBM, Octubre 2024. [En línea]. Available: https://www.ibm.com/mx-es/topics/network-monitoring. [Último acceso: 05 Agosto 2025].

[22] Site24x7, «Site24x7,» Zoho Corporation, Octubre 2024. [En línea]. Available: https://www.site24x7.com/es/network-traffic-monitoring.html. [Último acceso: 05 Agosto 2025].

[23] Network Startup Resource Center (NSRC), «NSRC – Network Startup Resource Center,» Sentrio, 24 Octubre 2016. [En línea]. Available: https://nsrc.org/workshops/2016/walc/gestion/presentations/gestion-de-redes.pdf. [Último acceso: 05 Agosto 2025].

[24] Reef Recovery, «Reef Recovery,» Pandora FMS, 14 Diciembre 2021. [En línea]. Available: https://reefrecovery.org/es/11-mejores-herramientas-de-monitoreo-de-infraestructura-ti-para-2021/. [Último acceso: 05 Agosto 2025].

[25] IBM, «IBM Mexico,» IBM, Octubre 2024. [En línea]. Available: https://www.ibm.com/mx-es/topics/it-security. [Último acceso: 05 Agosto 2025].

[26] ConceptoABC, «ConceptoABC,» ConceptoABC.com, Octubre 2024. [En línea]. Available: https://conceptoabc.com/seguridad-informatica/. [Último acceso: 05 Agosto 2025].

[27] UNIR FP, «UNIR FP,» Universidad Internacional de La Rioja – Formación Profesional (UNIR FP), 04 Enero 2023. [En línea]. Available: https://unirfp.unir.net/revista/ingenieria-y-tecnologia/principios-seguridad-informatica/. [Último acceso: 2025 Agosto 2025].

[28] Fortinet, «Fortinet,» CiberseguridadTips.com, 03 Mayo 2024. [En línea]. Available: https://www.fortinet.com/lat/resources/cyberglossary/cia-triad. [Último acceso: 05 Agosto 2025].

[29] C. Inc., «corelight.com,» [En línea]. Available: https://corelight.com/resources/glossary/ids-vs-ips. [Último acceso: 04 Agosto 2025].

[30] EC-Council, «eccouncil.org,» 15 Diciembre 2023. [En línea]. Available: https://www.eccouncil.org/cybersecurity-exchange/network-security/ids-and-ips-differences/. [Último acceso: 04 Agosto 2025].

[31] ServerNet, «ServerNet,» ServerNet, [En línea]. Available: https://servernet.com.ar/ciclo-pdca-seguridad-informatica/. [Último acceso: 22 Agosto 2025].

[32] B. Diego Fernando, «Ingenio Empresa,» IngenioEmpresa, 02 Agosto 2018. [En línea]. Available: https://www.ingenioempresa.com/ciclo-pdca/. [Último acceso: 22 Agosto 2025].

[33] Microsoft, «Microsoft Learn,» Microsoft Corporation, 09 Septiembre 2025. [En línea]. Available: https://learn.microsoft.com/es-es/visualstudio/get-started/visual-studio-ide?view=vs-2022. [Último acceso: 05 Agosto 2025].

[34] F. Tejera Martínez, D. Aguilera y J. M. Vilchez González, «Lenguajes de programación y desarrollo de competencias clave: revisión sistemática,» *Revista Electrónica de Investigación Educativa (REDIE),* vol. Vol. 22, nº 1, p. e27, 2020.

[35] Coursera Staff, «Coursera,» Coursera.org, 29 Noviembre 2023. [En línea]. Available: https://www.coursera.org/mx/articles/what-is-python-used-for-a-beginners-guide-to-using-python. [Último acceso: 05 Agosto 2025].

[36] TP-Link, «TP-Link España,» TP-Link Technologies Co., Ltd., 31 Enero 2025. [En línea]. Available: https://www.tp-link.com/es/business-networking/omada-sdn-controller/omada-software-controller/v5/. [Último acceso: 07 Abril 2025].

[37] Omada Networks, «Omada Networks,» TP-Link Technologies Co., Ltd., Julio 2025. [En línea]. Available: https://www.omadanetworks.com/es/business-networking/omada-router-wired-router/er7206/. [Último acceso: 01 Agosto 2025].

[38] TP-Link, «TP-Link España,» TP-Link Argentina, 2025. [En línea]. Available: https://www.tp-link.com/es/business-networking/management-platform/omada-software-controller/v1/. [Último acceso: 05 Agosto 2025].

[39] Beatriz Soto, «ADSLZone,» ADSLZone, 31 Enero 2025. [En línea]. Available: https://www.adslzone.net/reportajes/software/csv-que-es/. [Último acceso: 2025 Agosto 2025].

[40] Python Software Foundation, «Documentación oficial de Python,» Academia Desarrollo Web, 22 Octubre 2025. [En línea]. Available: https://docs.python.org/es/3/library/csv.html. [Último acceso: 05 Agosto 2025].

[41] C. Banco de Desarrollo de América Latina, «CAF,» CAF.com, 2016 Octubre 4. [En línea]. Available: https://www.caf.com/es/actualidad/noticias/la-importancia-de-tener-una-buena-infraestructura-escolar/. [Último acceso: 05 Agosto 2025].

[42] Fortinet, «Fortinet Cyberglossary LATAM,» [En línea]. Available: https://www.fortinet.com/lat/resources/cyberglossary/network-traffic. [Último acceso: 05 Agosto 2025].

[43] M. D. S. Pacheco, «Seguridad en redes de comunicaciones: Perspectivas y desafíos,» *Ingeniare. Revista chilena de ingeniería,* Vols. %1 de %2Vol. 30, Núm. 2, nº 2, p. 215–226, 2022.

[44] E. G. Mita Arancibia, «Revisión sistemática sobre análisis de datos en tiempo real: Herramientas para tomar decisiones estratégicas,» *Panel – Revista de Administración,* vol. 6, nº 2, Julio 2024.

[45] E. J. Hernández Leal, N. D. Duque Méndez y J. Moreno Cadavid, «Big Data: una exploración de investigaciones, tecnologías y casos de aplicación,» *TecnoLógicas,* vol. 20, nº 39, p. 15–38, 2017.

[46] J. Martins, «Asana,» Asana, 04 Octubre 2024. [En línea]. Available: https://asana.com/es/resources/pdca-cycle. [Último acceso: 22 Agosto 2025].

[47] MikroTik, «MikroTik Help Center,» MikroTikls SIA, 02 Junio 2025. [En línea]. Available: https://help.mikrotik.com/docs/spaces/UM/pages/19136528/RB4011iGS+RM. [Último acceso: 30 Agosto 2025].

[48] Cisco Systems, «Cisco Support,» Cisco Systems, 24 Abril 2018. [En línea]. Available: https://www.cisco.com/c/es_mx/support/docs/smb/routers/cisco-rv-series-small-business-routers/smb5520-get-to-know-the-rv345-dual-wan-gigabit-vpn-router-and-the-rv.html. [Último acceso: 30 Agosto 2025].

[49] Inc. Ubiquiti, «Ubiquiti Quick Start Guides,» Ubiquiti Networks, [En línea]. Available: https://dl.ubnt.com/qsg/ER-4/ER-4_ES.html. [Último acceso: 30 Agosto 2025].

ANEXOS

Anexo 1. Encuesta dirigida a estudiantes de FACSISTEL.

UPSE	**UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA** **FACULTAD DE SISTEMAS Y TELECOMUNICACIONES** **TECNOLOGÍAS DE LA INFORMACIÓN**
ENCUESTA DIRIGIDA A ESTUDIANTES DE FACSISTEL	
Ensayo:	Diseño de un entorno controlado para el análisis y monitoreo de tráfico de red en el laboratorio de redes de FACSISTEL
Objetivo:	La presente encuesta forma parte del trabajo de titulación "Diseño de un entorno controlado para el análisis y monitoreo de tráfico de red en el laboratorio de redes de FACSISTEL". Y tiene como objetivo recopilar información que permita evaluar las condiciones actuales del laboratorio de Redes.
1. ¿Has tenido alguna experiencia práctica en el laboratorio de Redes relacionada con redes informáticas?	
a). Sí, varias veces	
b). Pocas veces	
c). No, aún no	
2. ¿Crees que el laboratorio de Redes debería incluir más actividades prácticas para reforzar lo aprendido?	
a). Sí, totalmente	
b). Tal vez sí	
c). No lo considero necesario	
3. ¿Qué tan importante consideras practicar configuraciones de red en un entorno controlado antes de aplicarlas en redes reales?	
a). Muy importante	
b). Algo importante	
c). Poco importante	

4. ¿Has utilizado algún programa para simular redes informáticas como Packet Tracer durante clases?		
a). Sí, me ayudó a entender mejor		
b). Sí, pero no lo entendí bien		
c). No lo he usado		
5. ¿Crees que el uso de simuladores en el laboratorio de Redes puede mejorar el aprendizaje práctico?		
a). Si, definitivamente		
b). Puede ayudar en algunos casos		
c). No lo considero útil		
6. ¿Crees importante aprender a proteger tu información personal frente a riesgos de seguridad informática?		
a). Sí, me parece muy importante		
b). Sí, puede ser útil en ciertos casos		
c). No lo veo tan necesario		
7. ¿Consideras importante aprender a identificar problemas de red mediante el monitoreo del tráfico?		
a). Muy importante		
b). Algo importante		
c). Poco importante		
8. ¿Qué aspecto de infraestructura te gustaría que se mejore en el laboratorio de Redes para facilitar el aprendizaje?		
a). Más tiempo para prácticas		
b). Acceso a nuevas herramientas o simuladores		
c). Mejor organización del espacio		

Anexo 2. Manual de funcionamiento.

UNIVERSIDAD ESTATAL PENÍNSULA
DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

MANUAL DE FUNCIONAMIENTO PARA EL ENTORNO CONTROLADO

AUTOR

Carcelén Tomalá, Miguel Ángel

TUTOR

Lsi. Quirumbay Yagual Daniel Iván, MSIA.

Santa Elena, Ecuador

Año 2025

Acceso y configuración inicial del router Omada

Para iniciar el proceso de configuración del router TP-Link Omada ER7206, se estableció una conexión física directa entre el equipo de administración y uno de los puertos LAN del dispositivo. Esta conexión permitió acceder a la interfaz de gestión local mediante la dirección IP predeterminada.

Al introducir esta dirección en el navegador, se desplegó la interfaz principal del sistema, solicitando la creación de una cuenta de administrador (Figura N°34). Este paso resulta fundamental, ya que las credenciales definidas en esta etapa serán requeridas tanto para el acceso posterior al router como para su integración con el sistema de gestión centralizada Omada Controller.

Figura 34. Interfaz de creación para cuenta de administrador.

Una vez finalizado el registro y verificada la autenticación, se procedió a ingresar nuevamente con las credenciales definidas (Figura N°35). Al acceder al panel principal, se visualizaron distintas secciones de configuraciones disponibles: Estado, Red, USB, Preferencias, Transmisión, Cortafuegos, Control de conducta, VPN, VPN SSL, Autenticación, Servicios y Herramientas del sistema (Figura N°36). Esta estructura permite una administración detallada de cada componente de red, facilitando la configuración técnica como la documentación del entorno.

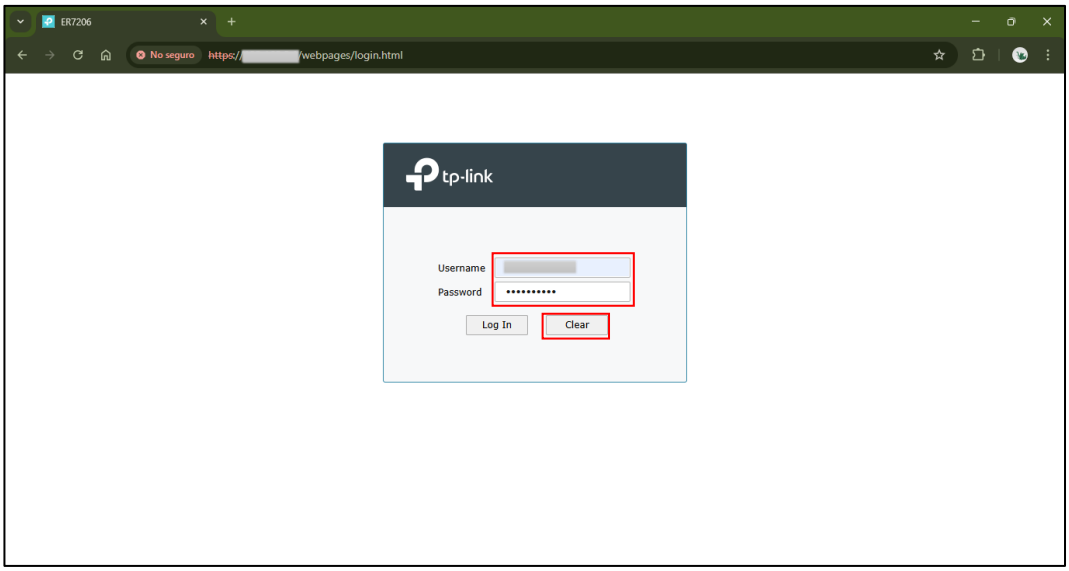


Figura 35. Ingreso de credenciales de administrador.

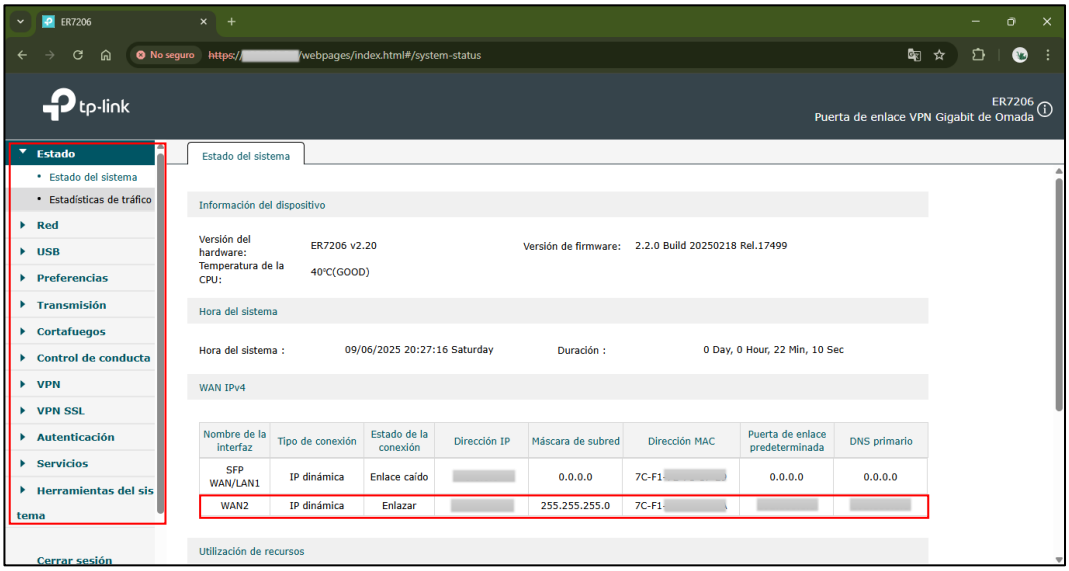


Figura 36. Interfaz principal del router Omada.

Instalación del software Omada Controller

Para iniciar la gestión centralizada del entorno de red, se procedió con la instalación del software Omada Controller en el equipo de administración del laboratorio (Figura N°37). El proceso comenzó accediendo al sitio oficial de TP-Link, donde se seleccionó el modelo correspondiente y se filtró el tipo de descarga según el sistema operativo, en este caso Windows.

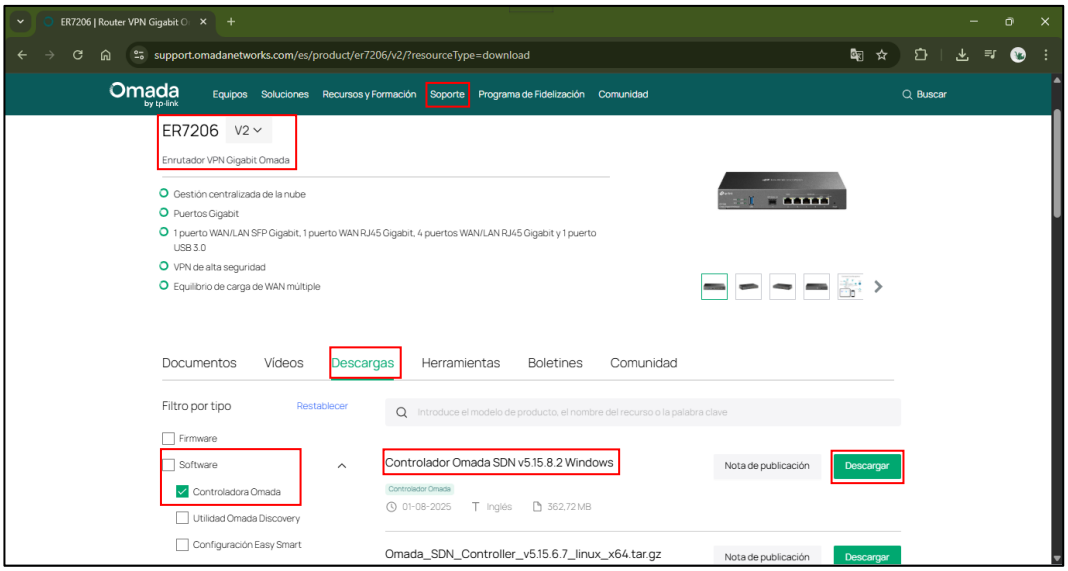


Figura 37. Página oficial de descarga del software Omada Controller.

Una vez descargado el paquete de instalación, se procedió a extraer los archivos incluidos: el ejecutable del instalador, los términos de licencia y la nota técnica correspondiente a la versión utilizada (Figura N°38).

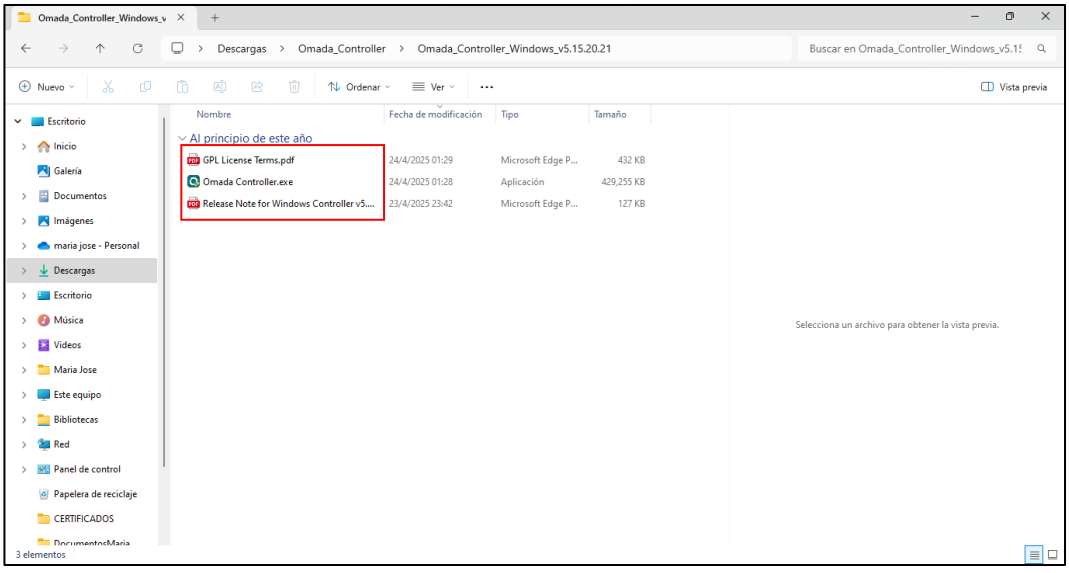


Figura 38. Carpeta con los archivos extraídos.

Antes de ejecutar el instalador, se verificó la presencia del entorno Java Runtime Environment (JRE), requisito indispensable para el funcionamiento del controlador. Se instaló la versión compatible de Java 8, asegurando la correcta ejecución del software (Figura N°39).

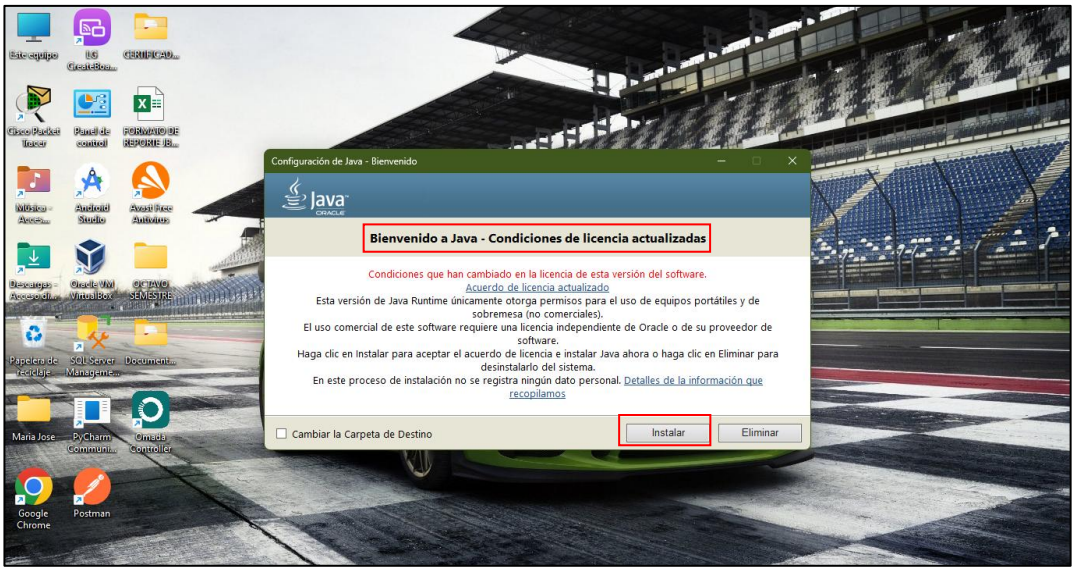


Figura 39. Instalación de Java Runtime Environment.

Posteriormente, se ejecutó el archivo de instalación siguiendo las instrucciones del asistente hasta completar el proceso (Figura N°40). Es importante considerar que, al instalar en el directorio c:\Program Files, el sistema operativo puede restringir la escritura en carpetas internas del controlador, como data\db. Por ello, se recomienda validar permisos de acceso antes de iniciar la configuración.

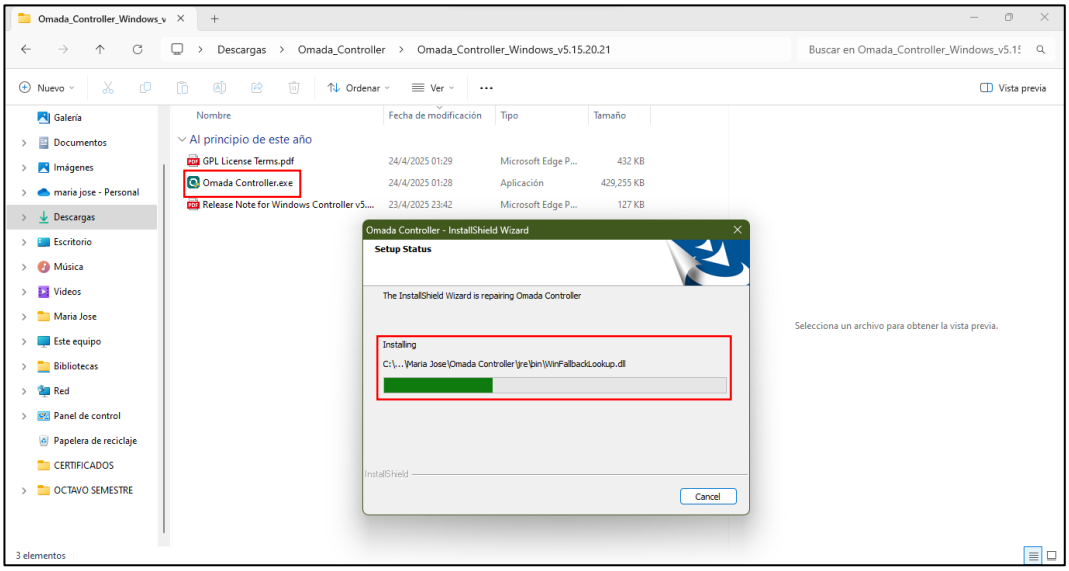


Figura 40. Inicio del instalador del software Omada Controller.

Ejecución del controlador y configuración inicial

Una vez completada la instalación, se ejecutará el controlador, el cual redirigió automáticamente al navegador local, desplegando el asistente de configuración inicial (Figura N°41). Este entorno permite la monitorización del estado de la red, ofreciendo visualización en tiempo real, distribución del tráfico y generación de alertas ante eventos anómalos.

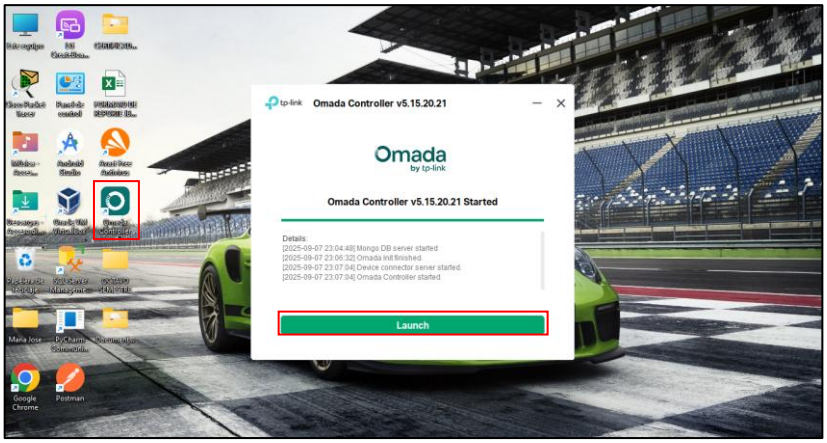


Figura 41. Inicio del controlador.

Durante esta etapa, se solicitó la creación de una cuenta de administración local, que incluye nombre de usuario, correo electrónico y contraseña (Figura N°42). Estos datos son esenciales para acceder al panel de gestión del controlador y vincular sesiones futuras de administración.

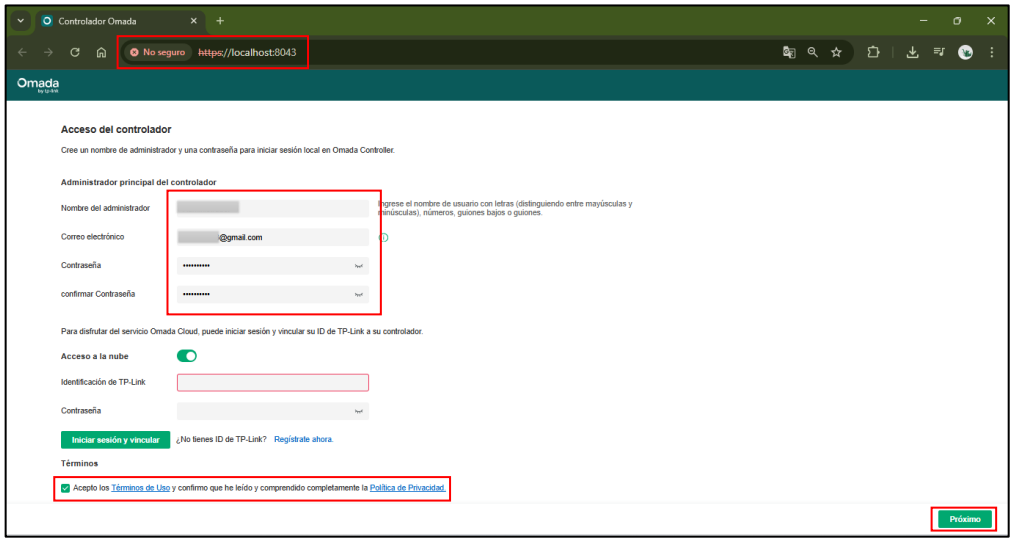


Figura 42. Acceso al controlador.

El asistente de configuración del sitio constituye un apartado clave que permite segmentar entornos dentro del controlador. La creación del sitio facilita la adopción del router Omada sin interferir con otros equipos que pudieran estar gestionados en el mismo sistema (Figura N°43).

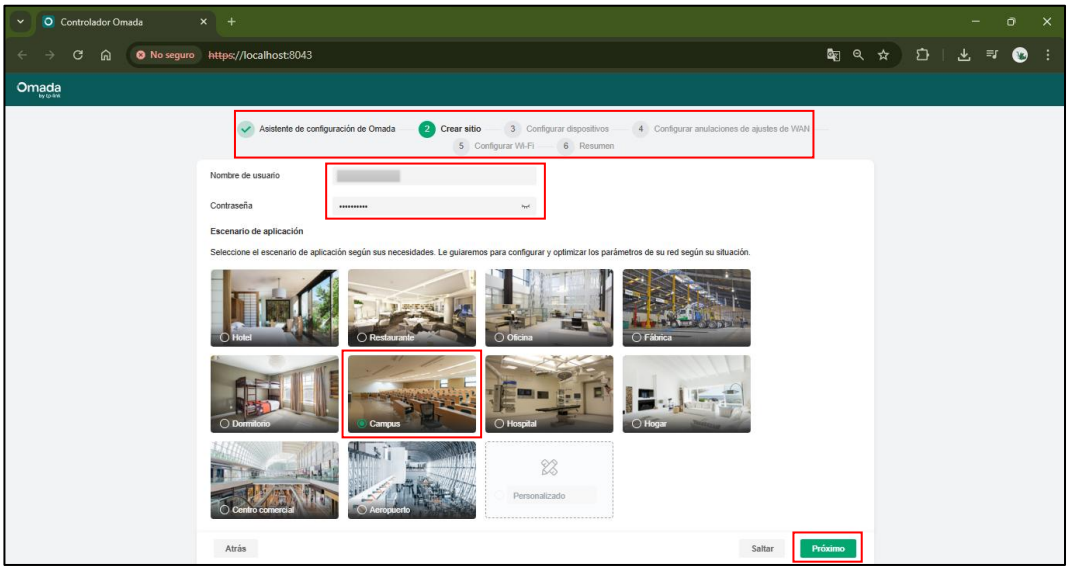


Figura 43. Creación del sitio.

Durante este proceso, se definió un escenario que simula un laboratorio académico orientado a prácticas de red. Asimismo, se asignaron credenciales específicas al dispositivo, permitiendo su incorporación al entorno previamente configurado (Figura N°44).

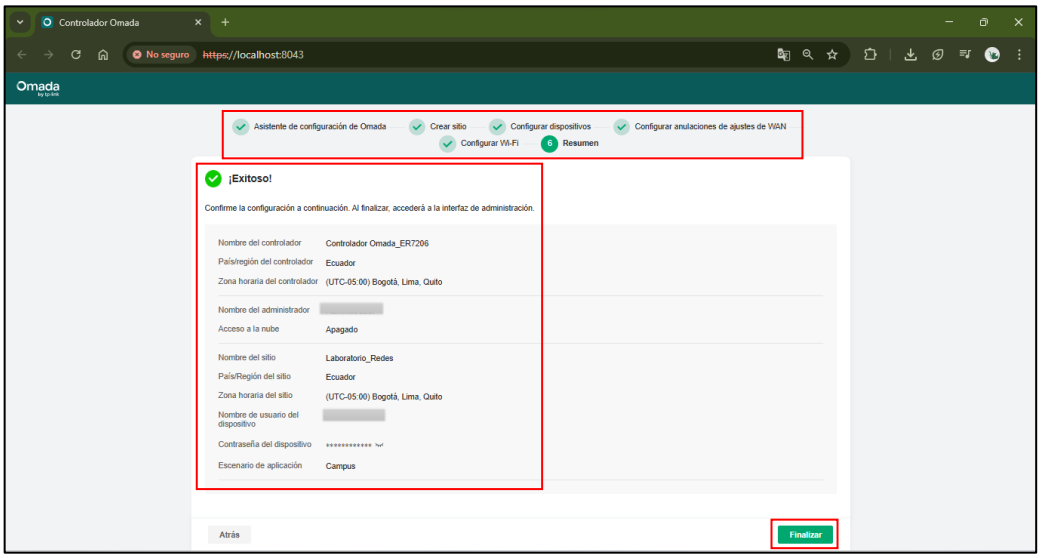


Figura 44. Resumen del asistente configurado.

Una vez finalizado el asistente de configuración, el sistema solicitó el ingreso de las credenciales creadas. Este acceso permite al usuario autenticarse como administrador local y desplegar el entorno de gestión del controlador (Figura N°45).

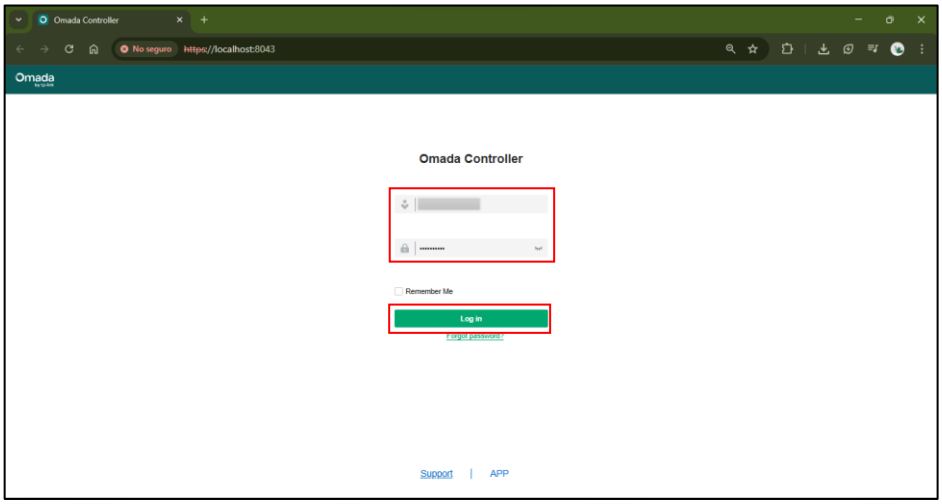


Figura 45. Ingreso de credenciales al controlador.

Al ingresar, se habilita la interfaz global del Omada Controller, diseñada para ofrecer una visión integral del estado de la red (Figura N°46). El administrador puede supervisar múltiples sitios, visualizar estadísticas en tiempo real, acceder al mapa de topología, gestionar dispositivos conectados y consultar registros de actividad mediante una navegación intuitiva y una administración eficiente.

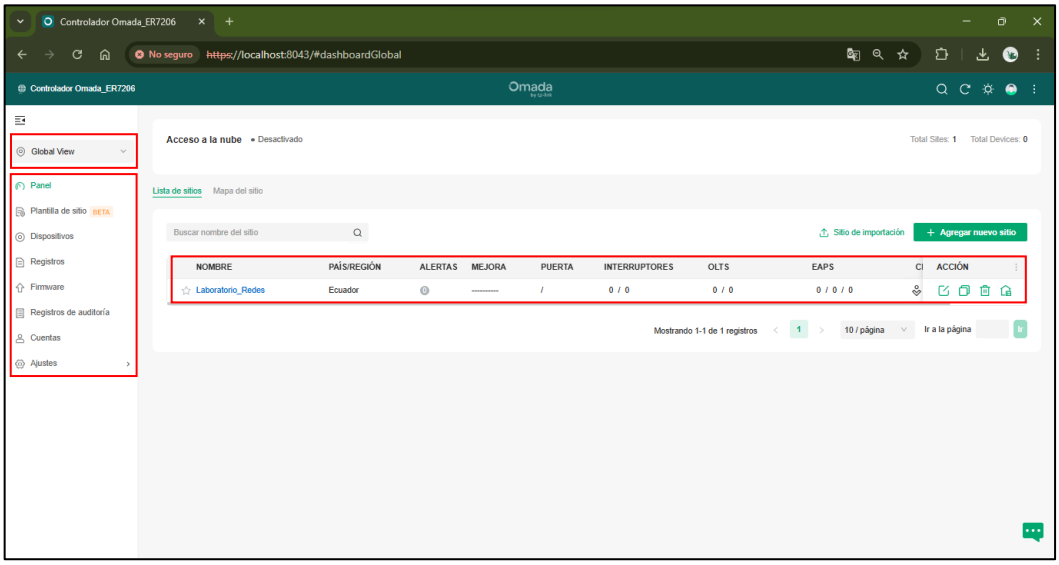


Figura 46. Interfaz global del controlador.

Restauración de fábrica del equipo

El proceso de restauración de fábrica puede realizarse mediante dos métodos. El primero consiste en utilizar el botón físico ubicado en la parte frontal del router. Para ello, se debe insertar un clip en el orificio correspondiente y mantenerlo presionado durante aproximadamente cinco segundos, hasta que el equipo se reinicie (Figura N°47).

Figura 47. Restauración física mediante botón frontal.

El segundo método se ejecuta desde la interfaz web, accediendo a la dirección IP predeterminada. Una vez ingresadas las credenciales, se accede al panel de configuración del dispositivo. Si el equipo ya ha sido adoptado por el controlador, se mostrará una advertencia indicando que puede ser restablecido para administrarlo como puerta de enlace independiente (Figura N°48).

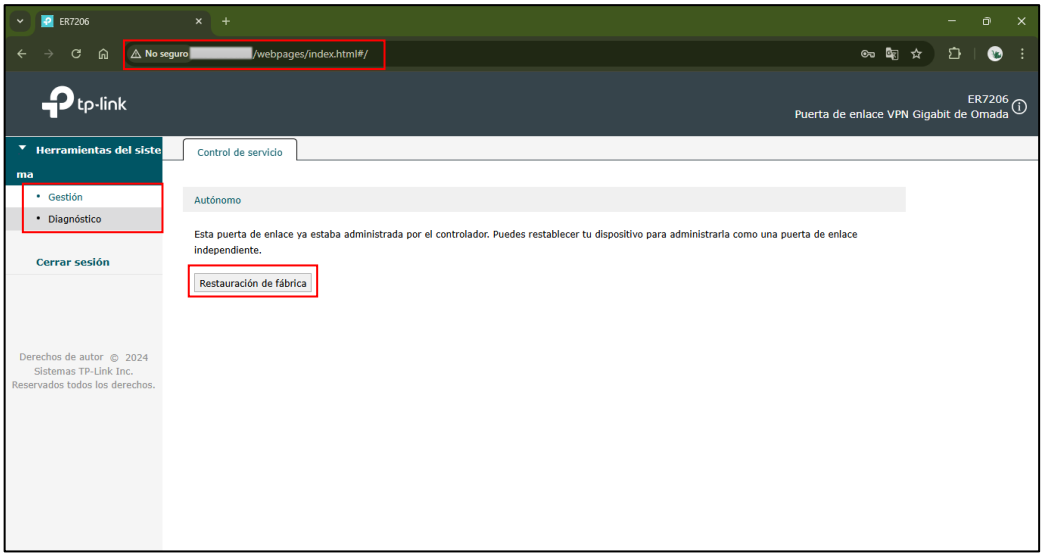


Figura 48. Restauración desde interfaz web del router.

Elaboración y funcionamiento del script en Python

Estructura del proyecto

La carpeta assets contiene la hoja de estilos CSS que define la apariencia visual del dashboard. En data se almacenan archivos CSV con historial de clientes, resumen de tráfico y gestión de amenazas. Los módulos de procesamiento se encuentran en la carpeta modules, mientras que el archivo principal dashboard.py integra todos los componentes y genera la interfaz interactiva (Figura N°49).

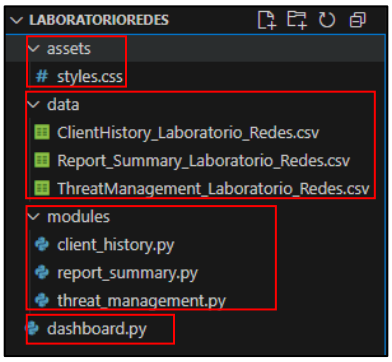


Figura 49. Estructura del proyecto.

Archivos CSV procesados

El primero corresponde al historial de conexión por usuario, registrando el tiempo de actividad y volumen de tráfico. El segundo archivo presenta un resumen general del tráfico, lo que permite analizar patrones de uso y detectar picos de actividad. Finalmente, el tercer archivo contiene los registros de amenazas detectadas, incluyendo detalles como el tipo de riesgo, lo que facilita la evaluación de la seguridad en el entorno de red (Figura N°50).

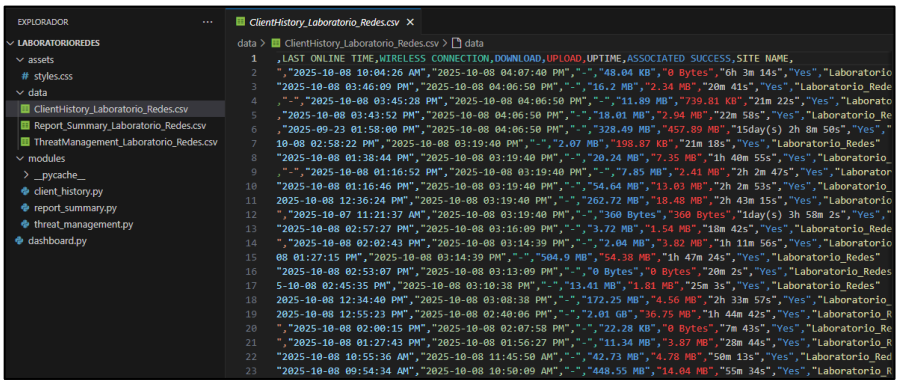


Figura 50. Archivos CSV del proyecto.

Funcionamiento de los módulos de procesamiento

El módulo client_history.py realiza el procesamiento del historial de conexión de los usuarios. Convierte las unidades de tráfico a megabytes, calculando el tiempo total de conexión en minutos y formatea en horas y minutos. Además, genera métricas como el tráfico total, la velocidad promedio de transferencia, normaliza los nombres de usuario y prepara los datos para su visualización en el dashboard (Figura N°51).

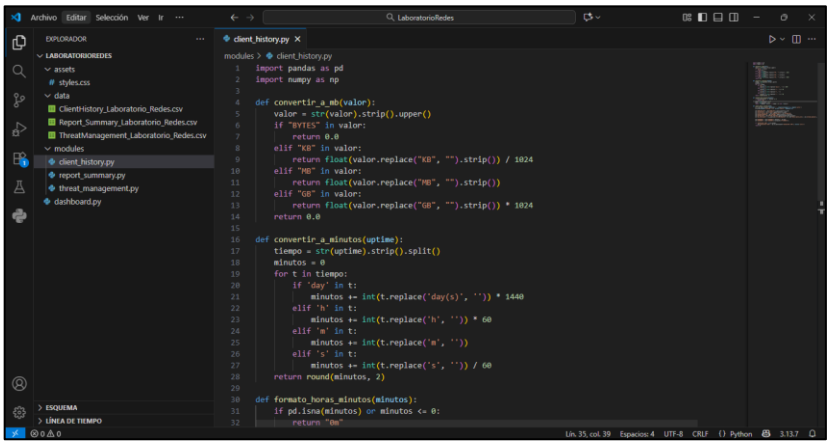


Figura 51. Modulo client_history.py.

El módulo report_summary.py se encarga de procesar el resumen de tráfico registrado por hora. Convierte las unidades de tráfico a megabytes y organiza la información en un DataFrame estructurado, filtra los registros nulos y transforma las horas en formatos datetime. Esta estructura permite visualizar patrones de uso y detectar variaciones en el comportamiento de la red (Figura N°52).

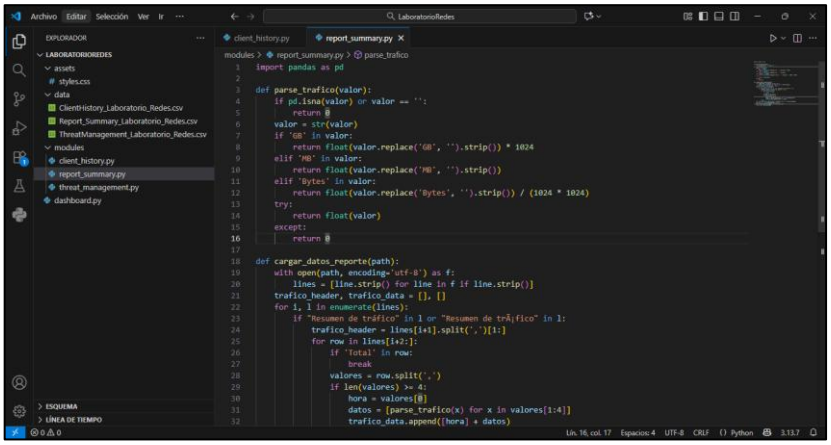


Figura 52. Modulo client_history.py.

El módulo threat_management.py procesa los registros de amenazas detectadas en la red. Convierte las fechas a formato datetime, extrae la fecha individual y organiza los datos para su análisis. Además, genera resúmenes por clasificación, categoría y nivel de severidad, lo que permite identificar patrones de riesgo y evaluar el comportamiento de seguridad en el entorno del laboratorio (Figura N°53).

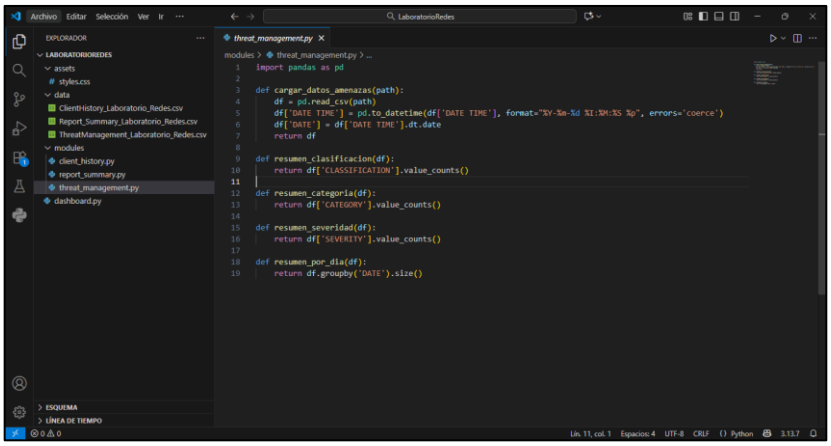


Figura 53. Modulo threat_management.py.

Visualización dashboard principal

Dashboard.py utiliza las librerías pandas, dash y plotly para generar gráficos interactivos, tablas dinámicas y métricas clave. Cada sección se construye mediante funciones específicas (layout_clientes(), layout_tráfico() y layout_amenazas()), lo que permite mantener una estructura modular. Asimismo, se aplican estilos personalizados desde el archivo CSS, asegurando una presentación visual (Figura N°54).

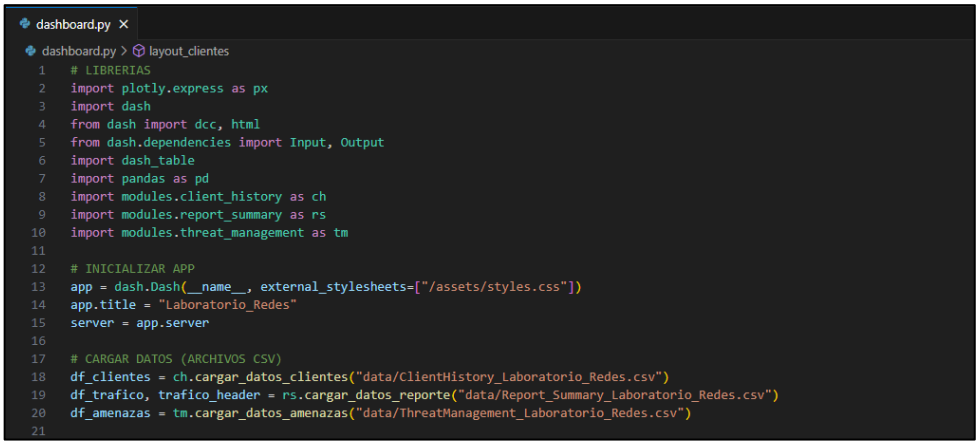


Figura 54. Librerías para el dashboard.

La función layout_clientes() construye la sección del dashboard dedicada al historial de usuarios. Presenta métricas generales, tablas interactivas y gráficos que analizan el tráfico total, tiempo de conexión y la eficiencia por usuario. También identifica los casos ineficientes, muestra la evolución del tráfico de red y permite interpretar el comportamiento de los clientes para detectar patrones (Figura N°55).

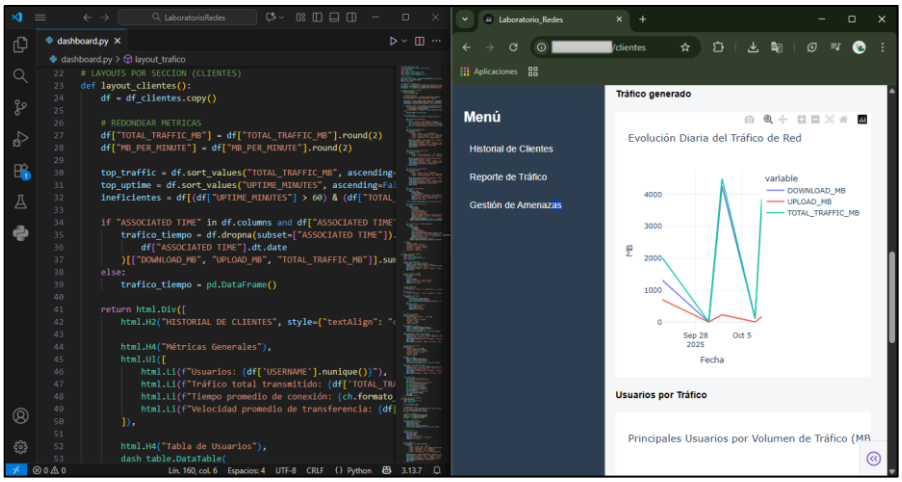


Figura 55. Visualización de clientes en el dashboard.

La función layout_tráfico() organiza la sección del dashboard dedicada al análisis de tráfico por nivel de alerta, categoría y aplicación. Presenta una tabla interactiva y gráficos que muestran la evolución horaria del tráfico, la distribución de alertas y el consumo generado por aplicaciones específicas, permitiendo evaluar el comportamiento de la red (Figura N°56).

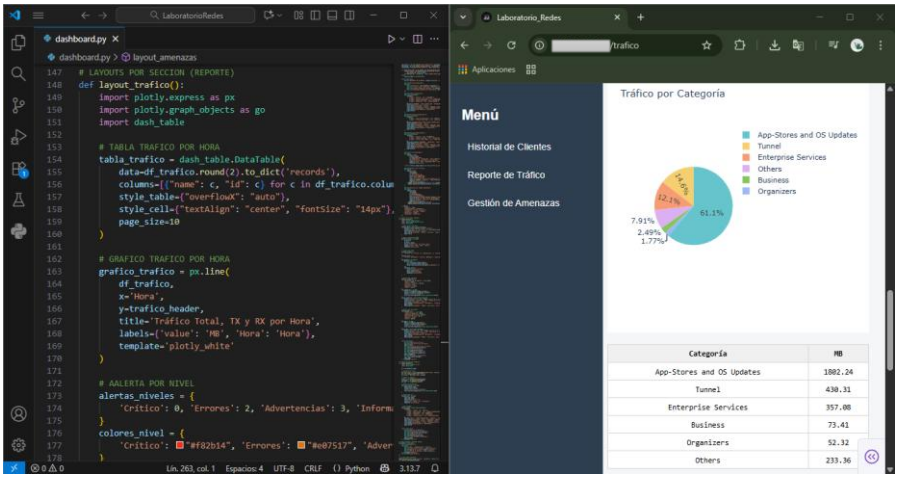


Figura 56. Visualización del tráfico de red en el dashboard.

La función layout_amenazas() construye la sección del dashboard enfocada en la gestión de riesgos y eventos de seguridad. Muestra resúmenes por clasificación, categoría, severidad y frecuencia diaria. Utiliza tablas interactivas y gráficas para visualizar la distribución de amenazas detectadas en la red (Figura N°57).

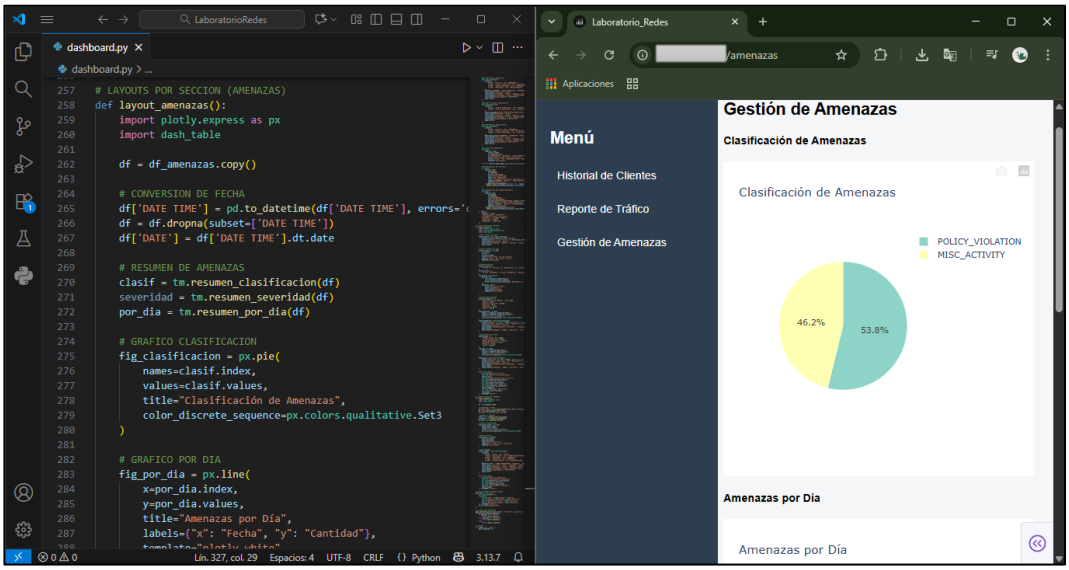


Figura 57. Visualización de amenazas en el dashboard.

Anexo 3. Autorización de uso del Laboratorio de Redes.

FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

DECANATO

Oficio n°. UPSE-FST-2025-302-OF

La Libertad, junio 20 de 2025

Asunto: Uso de laboratorio

Señor Licenciado
Daniel Quirumbay Yagual, MSIA.
DOCENTE DE LA FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
En su despacho.

De mi consideración:

En atención al oficio sin número suscrito por su digna persona, me permito comunicar que se autoriza el uso del Laboratorio de Redes, debiendo coordinar las actividades prácticas del trabajo de titulación de los estudiantes James Carvajal Núñez, Miguel Carcelén Tomalá y Jorge Soledispa Saltos, en función al horario de clases correspondientes al período académico 2025-1, donde el Laboratorio es usado por los estudiantes de las Carreras de la Facultad.

Cabe destacar, que el uso de los equipos debe ser bajo responsabilidad exclusiva del Docente Tutor.

Particular que comunico a usted para los fines consiguientes.

Atentamente

Firmado electrónicamente por:
WASHINGTON DANIEL TORRES GUIN

Ing. Washington Torres Guin, Mgt.
DECANO DE LA FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

WTG/lquimi

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
UPSE
DECANATO
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

Campus matriz, La Libertad - Santa Elena - ECUADOR
Código Postal: 240204 - Teléfono: (04) 781 - 732

UPSE ¡crece SIN LÍMITES!
www.upse.edu.ec

Anexo 4. Uso del Laboratorio de Redes.

FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

DECANATO

Oficio n°. UPSE-FST-2025-421-OF

La Libertad, agosto 26 de 2025

Asunto: Uso de laboratorios

Señor Licenciado
Daniel Quirumbay Yagual, MSIA.
DOCENTE DE LA FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
En su despacho.

De mi consideración:

En atención al oficio sin número suscrito por su digna persona, me permito comunicar que se autoriza el uso del Laboratorio de Redes, debiendo coordinar las actividades prácticas del trabajo de titulación de los siguientes estudiantes con el Ing. Enrique Montenegro Romero, en función al horario de clases correspondientes al período académico 2025-2, donde el Laboratorio es usado por los estudiantes de las Carreras de la Facultad.

TRABAJO DE TITULACIÓN	ESTUDIANTES
Modelo de almacenamiento distribuido seguro mediante miniNAS y conexión VPN para entornos de protección de información crítica.	James Carvajal Núñez
Diseño de un entorno controlado para el análisis y monitoreo de tráfico de red en el laboratorio de redes de FACSISTEL.	Miguel Carcelén Tomalá
Modelo experimental de migración progresiva de IPv4 a IPv6 utilizando mecanismos de túnel y traducción aplicado al laboratorio de redes de FACSISTEL	Jorge Soledispa Saltos

Cabe destacar, que el uso de los equipos debe ser bajo responsabilidad exclusiva del Docente Tutor.

Particular que comunico a usted para los fines consiguientes.

Atentamente

Firmado electrónicamente por: WASHINGTON DANIEL TORRES GUIN
Validar únicamente con FirmaEC

Ing. Washington Torres Guin, Mgt.
DECANO DE LA FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

cc Ing. Enrique Montenegro Romero

WTG/lquimi

Campus matriz, La Libertad - Santa Elena - ECUADOR
Código Postal: 240204 - Teléfono: (04) 781 - 732

www.upse.edu.ec