CIYA. Ciencias de la Ingeniería y Aplicadas, Vol. 10 Nº 1, enero-junio de 2026, pp. 147-163

Transformación de la infraestructura de red en entornos educativos: Propuesta de estudio en la Unidad Educativa Oxford

Transformation of Network Infrastructure in Educational Environments: A Study Proposal for the Oxford Educational Unit

Verónica Pailiacho-Mena[1], Enrique Garcés-Freire[2], Dennis Chicaiza[3], Francisco Vega[4]

DOI: https://doi.org/10.61236/ciya.v10i1.1241

RESUMEN:

Hoy en día la infraestructura de red es la columna vertebral de la comunicación en las organizaciones y el área de la educación no es la excepción, además tiene un plus añadido, pues si no cuentan con la infraestructura necesaria, no se puede ofrecer acceso a recursos innovadores y educativos que apoyen el proceso de enseñanza aprendizaje. En esta investigación se presenta una propuesta de estudio de la red de comunicaciones de la Unidad Educativa Oxford, ubicada en la provincia de Cotopaxi en Ecuador, este proyecto estuvo centrado en mejorar la escalabilidad y seguridad de la infraestructura existente, mediante el método Kanban se organizaron las actividades a desarrollar. En el análisis se realizó un inventario de equipos activos de la red, determinándose que es una red plana con alto volumen de paquetes broadcast, cuenta con equipos que operan con las configuraciones de fábrica y sin ningún monitoreo, por lo que se propone un rediseño de red con aspectos importantes como: el cumplimiento de las normativas de cableado estructurado, segmentación de la red, implementación de VLANs e InterVLAN, configuración de medidas de seguridad (BPDU Guard, Port Security, DHCP Snooping) y controles adicionales de firewalls y ACLs. Se creó una simulación en GNS3 para la validación de la eficacia del diseño, demostrando su capacidad para optimizar el rendimiento, garantizar la seguridad y adaptación al crecimiento futuro de la institución, así también, la propuesta fue validada por especialistas del área, obteniendo un 100% de satisfacción en criterios como estructura, adaptabilidad y seguridad.

Palabras claves: rediseño de red, VLANs, seguridad de red, GNS3.

[1] Pontificia Universidad Católica del Ecuador Sede Ambato, Ambato, Tungurahua, Ecuador, vpailiacho@pucesa.edu.ec
[2] Pontificia Universidad Católica del Ecuador Sede Ambato, Ambato, Tungurahua, Ecuador, egarces@pucesa.edu.ec
[3] Universidad Técnica de Ambato, Ambato, Tungurahua, Ecuador, dv.chicaiza@uta.edu.ec
[4] Pontificia Universidad Católica del Ecuador Sede Ambato, Ambato, Tungurahua, Ecuador, francisco.e.vega.t@pucesa.edu.ec

ABSTRACT:

Nowadays, network infrastructure is the backbone of communication within organizations, and the education sector is no exception. Moreover, it has an added value, since without adequate infrastructure it is not possible to provide access to innovative and educational resources that support the teaching–learning process. This research presents a proposal for a study of the communications network of the Oxford Educational Unit, located in the province of Cotopaxi, Ecuador. The project focused on improving the scalability and security of the existing infrastructure, and the Kanban method was used to organize the activities to be carried out. During the analysis phase, an inventory of active network devices was conducted, determining that the network is flat, with a high volume of broadcast packets, and includes devices operating with factory-default configurations and without any monitoring mechanisms. Therefore, a network redesign is proposed, incorporating key aspects such as compliance with structured cabling standards, network segmentation, implementation of VLANs and Inter-VLAN routing, configuration of security measures (BPDU Guard, Port Security, DHCP Snooping), and additional controls through firewalls and ACLs. A simulation was developed using GNS3 to validate the effectiveness of the proposed design, demonstrating its ability to optimize performance, ensure security, and adapt to the institution's future growth. Additionally, the proposal was validated by field specialists, achieving 100% satisfaction in criteria such as structure, adaptability, and security.

Keywords*: Network redesign, VLANs, Network security, GNS3.*

Recibido 18 de noviembre de 2025; **revisión aceptada** 12 de enero de 2026

1. INTRODUCCIÓN

Las redes de comunicación son sistemas fundamentales para el intercambio de información, que permite la conectividad entre dispositivos y el acceso a recursos digitales[1], hoy en día las redes de computadoras se usan en todas las áreas, generando múltiples conexiones entre instituciones comerciales y educativas. En el ámbito educativo existe una gran cantidad de recursos educativos innovadores e informativos en el internet [2], que deben estar al alcance de los educandos, en consecuencia, las instituciones educativas necesitan de una red estable, escalable y disponible, lastimosamente en muchas instituciones de nivel medio, la red va creciendo en base a necesidades de momento, sin un verdadero análisis y diseño de las necesidades presentes y futuras, mientras tanto, la demanda de ancho de banda y servicios en red crece constantemente [3], una infraestructura mal diseñada puede afectar directamente la eficiencia operativa, la experiencia de usuarios como docentes, estudiantes y personal

administrativo, y la seguridad de los datos, pues los métodos de ataque evolucionan día a día y la infraestructura de red debe tener la capacidad de mitigar estos ataques, a través del monitoreo de red y medidas de seguridad[4], entonces surge la necesidad de un rediseño de la red de computadoras [5].

Este replanteo de la red es pertinente, cuando esta ha crecido sin una planificación establecida, cuando existe un excesivo tráfico de broadcast que satura los equipos y reduce el rendimiento general de la red, otro parámetro a considerar son los equipos obsoletos o cableado de red sin cumplir las normas de cableado estructurado. Este rediseño de la red debe permitir optimizar los recursos, mejorar la gestión y monitoreo del tráfico de la red y garantizar la seguridad de la información [6]. Así se pueden evitar ataques como suplantación de direcciones MAC (MAC Flooding), ataques de denegación de servicio (DHCP Spoofing), captura de datos, entre otros[7], que ponen en riesgo a la institución.

La Unidad Educativa Oxford está ubicada en Salcedo, Ecuador, ofrece educación inicial y preparatoria, elemental y media, superior y bachillerato general unificado [8], existen alrededor de 1300 estudiantes, con una proyección de crecimiento anual del 15%, trabajan alrededor de 86 personas entre administrativos y profesores, la institución cuenta con una red que en general está funcional, pero presenta problemas de lentitud, no abastece a todos los edificios, no se han configurado seguridades en la red, lo que les hace vulnerables a ataques informáticos y limita su capacidad de adaptación a futuras necesidades tecnológicas, por lo que es necesario rediseñar la red de comunicaciones para toda la institución, este reporte de investigación está basado en la tesis titulada Rediseño de la red de comunicaciones de la Unidad Educativa Oxford [9] desarrollada en la Pontificia Universidad Católica del Ecuador Sede Ambato.

La propuesta planteada usó como método de trabajo a Kanban, para así garantizar un seguimiento y monitoreo permanente del proyecto. Fueron varios los aspectos que se consideraron en el rediseño como: la segmentación lógica de la red implementando *Virtual Local Area Network* (VLANs), para decrementar el tráfico de broadcast en la red [10], la disponibilidad, configuraciones en los dispositivos activos de la red para controlar ataques cibernéticos [11]. Estos elementos no solo resuelven las limitaciones actuales, sino que también preparan la red para futuras expansiones. Para una mejor visualización del rediseño se generó una simulación en GNS3 (*Graphical Network Simulator*-3), una herramienta ampliamente utilizada en la planificación de redes [12] [13], lo que permitió evaluar escenarios de funcionamiento de la red, simulación de ataques y la eficiencia de los controles de seguridad implementados. Adicionalmente, el proyecto fue validado por especialistas en telecomunicaciones, quienes aprobaron satisfactoriamente el rediseño considerando criterios

como escalabilidad, adaptabilidad y seguridad. Este enfoque integral asegura que la propuesta no solo sea teóricamente sólida, sino también aplicable en entornos reales.

2. METODOLOGÍA

El estudio se desarrolló bajo un enfoque cualitativo, que permitió analizar de manera integral las necesidades técnicas y operativas de la red de la Unidad Educativa Oxford. La planificación del trabajo se la realizó bajo el método Kanban, utilizando un tablero visual para gestionar las tareas y actividades[14], organizadas en las columnas "Por hacer", "En progreso" y "Realizadas", fue un acierto aplicar este método de trabajo, por su facilidad de adaptación, planificación y seguimiento ágil, si bien Kanban ha sido utilizado más en proyectos de desarrollo de software[15], se puede evidenciar que Kanban también se puede adaptar a proyectos técnicos de telecomunicaciones, pues dentro del tablero se organizaron las 3 fases principales del rediseño de red y cada fase tiene descrito las tareas a desarrollar, el tablero permitió ir avanzando en cascada hasta el cumplimiento del proyecto, en la Tabla 1 se puede observar el listado de actividades realizadas.

Tabla 1. Tablero de actividades Kanban.

Por hacer	En proceso	Realizadas
Análisis de la situación actual: - Recolección de información técnica - Análisis de la red de area local (LAN) actual - Requisitos funcionales		
Diseño de la solución **-** Rediseño de la infraestructura LAN - Distribución de configuraciones - Seguridad de la red - Servicios		
Validación de la propuesta - Simulación - Selección de especialistas - Matriz de validación por especialistas - Análisis de los resultados de validación		

2.1. Análisis de la situación actual

La recopilación de datos se la realizó mediante entrevistas semiestructuradas al personal del departamento de TI (Tecnologías de la Información) de la Unidad Educativa y a través de la observación directa se puede determinar que actualmente se cuenta con cuatro edificios, un laboratorio con red en cada edificio y no hay interconexión entre todos los edificios, trabajan con dos proveedores de internet Speedy en el edificio del colegio (bachillerato) e iniciales, mientras que la conexión de CNT (Corporación Nacional de Telecomunicaciones) está en el

edificio administrativo y escuela. Ambos planes de internet tienen una velocidad de 100 megabits por segundo (Mbps).

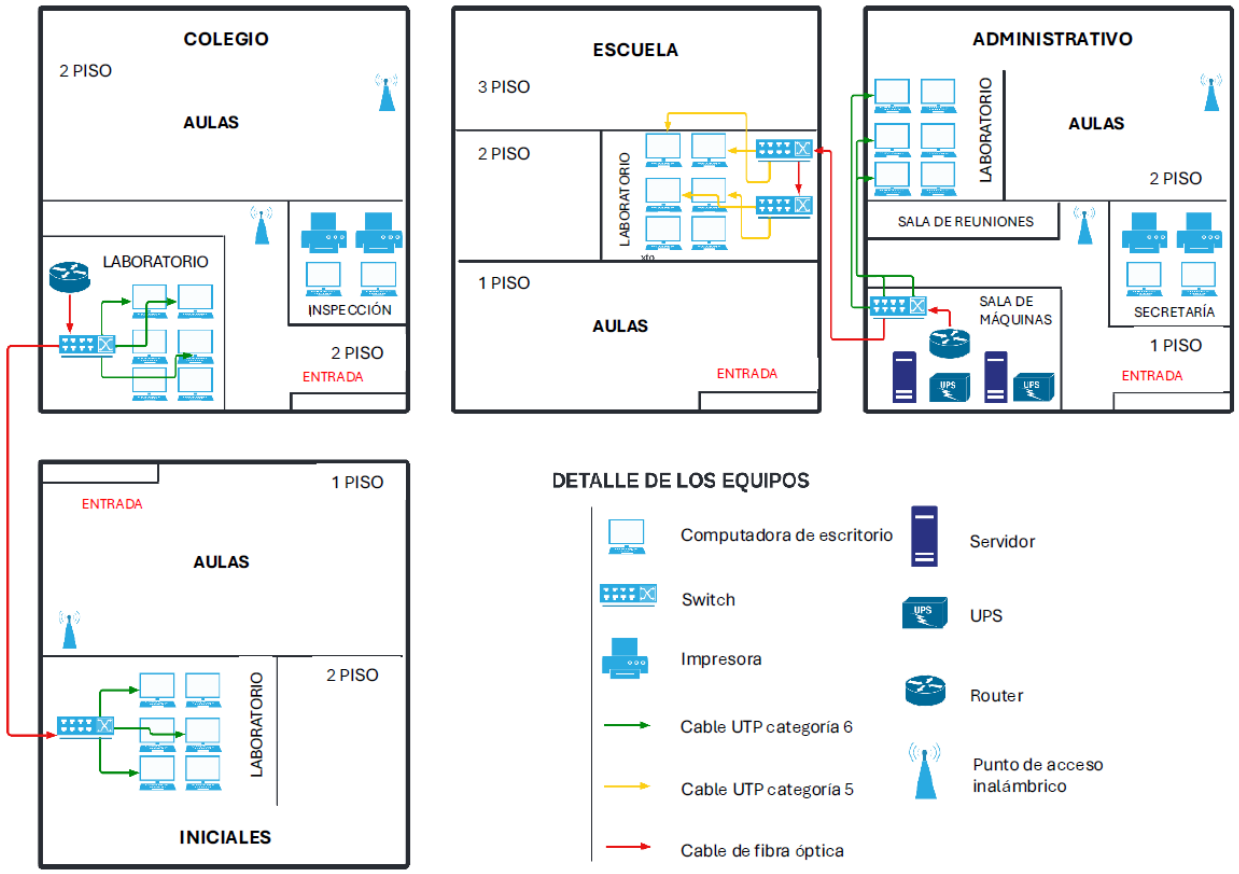

Figura 1. Infraestructura LAN actual

Las entrevistas al personal de TI de la Unidad Educativa se basaron en un guion predefinido, donde se abordaron temas como el estado de los equipos, topología de red, protocolos utilizados y problemas recurrentes. Adicionalmente, se realizó un diagnóstico físico de los dispositivos de red (switchs, routers, puntos de acceso) para identificar limitaciones en capacidad, configuración y seguridad, el inventario detallado de los equipos de red, se muestra un resumen en la Tabla 2.

Tabla 2. Equipos existentes

Edificio	Equipos	Cantidad	Marca
Iniciales	Switch 48 puertos	1	Aruba
	Punto de acceso	1	Aruba
Escuela	Switch 16 puertos	1	Aruba
Colegio	Switch 48 puertos	1	Aruba
	Impresora	3	HP
	Copiadora	1	HP

Edificio	Equipos	Cantidad	Marca
	Router	1	TP-Link
	Punto de acceso	2	Aruba
Administrativo	Switch 48 puertos	1	Aruba
	Impresora	2	HP
	UPS	2	Forza
	Punto de acceso	2	Aruba
	Router	1	TP-Link
	Servidor Contable y Académico	1	Dell
	Servidor DHCP y Active Directory	1	Dell

En este análisis se identificó que los dispositivos operaban con las configuraciones de fábrica, nunca habían sido monitoreados, la red es plana sin segmentación lógica, mediante Wireshark, se detectó un alto volumen de tráfico de broadcast, existen puertos abiertos sin ninguna autenticación. Estos hallazgos se correlacionaron con las entrevistas al personal de TI, quienes reportaron problemas recurrentes de lentitud y caídas de conexión durante horas pico, el análisis también evaluó el cableado de red, revelando una falta de cumplimiento a las normas de cableado estructurado, una mezcla de UTP categoría 5 y 6. Esto incrementa los cuellos de botella en la transmisión de datos, especialmente en el edificio de la escuela, donde el cableado es de categoría 5 y el ancho de banda es limitado, Adicionalmente, poseen servidores de *Active Directory* y el protocolo dinámico de configuración de host (DHCP). En el servidor situado en el área administrativa se alojan el software contable denominado Fénix y el software para el registro de notas, Odoo, el acceso a estos programas está protegido mediante inicios de sesión con credenciales, no se han implementado controles de seguridad adicionales en la infraestructura de red, no cuentan con políticas de backup, ni de seguridad.

2.2. Diseño de la solución

Con los problemas detectados es urgente un rediseño de la red, donde se diseñó una topología estrella extendida con redundancia, con un *backbone* de fibra óptica que interconectará los switches de todos los edificios para garantizar alta disponibilidad, la propuesta integra una sola red institucional.

Para cada edificio (inicial, escuela, colegio, administrativo) se segmentó la red y se crearon 16 VLANs independientes, asignando rangos de direcciones IP (*Internet Protocol*) en base al

número de ips requeridas, mediante VLSM (*Variable Length Subnet Masking*) para optimizar el espacio de direccionamiento, ver el resultado en la Tabla 3.

Tabla 3. Direccionamiento IP.

Edificio	Subred	Requerimientos de IPs	Id de Red	Notación CIDR (*Classless Inter-Domain Routing*)
Iniciales	Wi-Fi Oxford	65	172.x.1.128	/25
	Laboratorios	20	172.x.2.96	/27
	Docentes	10	172.x.3.0	/28
	Administrativo	3	172.x.3.32	/29
Escuela	Wi-Fi Oxford	84	172.x.0.128	/25
	Docentes	28	172.x.2.128	/27
	Laboratorios	20	172.x.2.64	/27
	Administrativo	3	172.x.3.40	/29
Colegio	Wi-Fi Oxford	90	172.x.0.0	/25
	Docentes	31	172.x.2.0	/26
	Laboratorios	20	172.x.2.160	/27
	Administrativo	8	172.x.3.16	/28
Administrativo	Wi-Fi Oxford	70	172.x.1.0	/25
	Laboratorios	20	172.x.2.192	/27
	Administrativo	16	172.x.2.224	/27
	Docentes	3	172.x.3.48	/29

Las VLANs se intercomunicarán a través del router principal, en cuanto a seguridad, se diseñaron medidas en las capas del modelo TCP/IP, en la capa de enlace de datos se configuró Port Security para limitar el acceso a los puertos del switch por las direcciones MAC y BPDU Guard para prevenir ataques al protocolo STP, así también se deshabilitaron los puertos no utilizados. En la capa de red, se aplicaron ACLs (listas de control de acceso) extendidas para filtrar tráfico no autorizado hacia servicios críticos, como el sistema contable. Adicionalmente, se desplegará un firewall Fortinet en la periferia de la red, configurado para permitir solo tráfico HTTPS, SSH e ICMP, con reglas establecidas para el control de contenidos. Estos controles se complementaron con los servicios centralizados como DHCP, Active Directory y DNS, alojados en un servidor Windows Server 2019. Cada configuración fue documentada en scripts reproducibles, facilitando su implementación.

Además, se sugiere contratar un solo proveedor de servicio de internet, considerar la configuración de un software de monitoreo de red, el desarrollo de políticas de seguridad, por costos estos servicios no fueron desarrollados en el rediseño de la red.

3. RESULTADOS

3.1. Infraestructura propuesta

El rediseño de la red de la Unidad Educativa Oxford soluciona los requerimientos actuales, y contempla un crecimiento de la misma, todos los edificios están interconectados para lo cual se propone la creación de 4 cuartos de equipos donde se alojaran los racks, patch panel, switch, cada uno en el mismo piso del laboratorio de computación del edificio y un DataCenter que será el núcleo de la infraestructura de red en el edificio administrativo, la red tiene un enlace redundante lo que proporciona disponibilidad y garantía de comunicación, el diseño físico se lo puede visualizar en la figura 2.

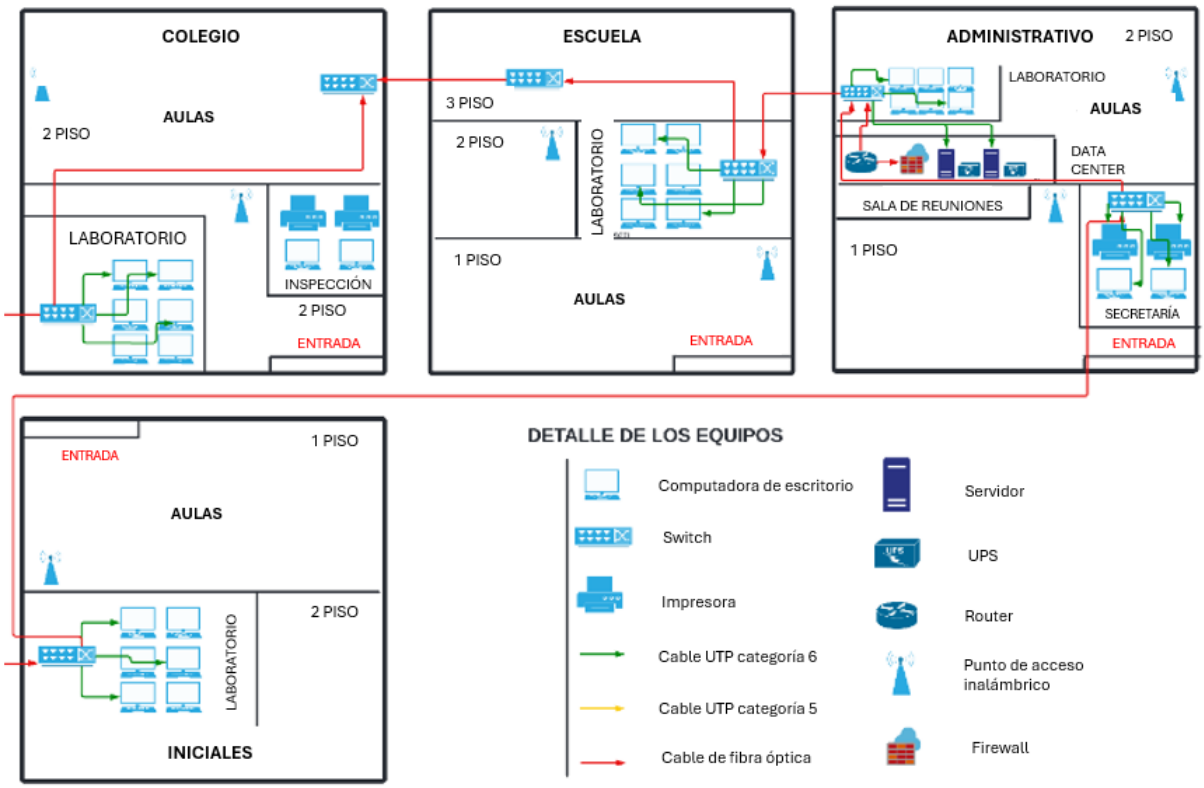

Figura 2. Diseño de red propuesto.

La propuesta incluyó la adquisición e instalación de nuevos equipos para modernizar la infraestructura existente, se incorporan 2 switches Aruba de 48 puertos para reemplazar los equipos obsoletos en los edificios de la escuela y el colegio, así como 2 puntos de acceso adicionales para mejorar la cobertura inalámbrica.

La topología en estrella extendida se diseñó mediante conexiones de fibra óptica (500 metros, marca Corning) entre switches, lo que permitió alcanzar velocidades de hasta 1 Gbps y el cambio de cableado a UTP Cat 6 en toda la institución. Adicionalmente, es necesario un firewall, para lo cual se sugiere Fortinet en el edificio administrativo para filtrar el tráfico

entrante y saliente, configurado para permitir únicamente protocolos esenciales como HTTPS, SSH e ICMP.

El costo total de la implementación en Ecuador ascendió a $14.000 USD, incluyendo equipos, cableado estructurado categoría 6 (300 metros) y accesorios como patch panels, cajetines, Jack conector, canaletas, patch cord, entre otros y configuraciones de red y seguridad. Un aspecto crítico fue la ubicación del Data Center en el segundo piso y no el improvisado que había en el primer piso, con una inversión de $3,500 USD en equipos complementarios como aire acondicionado, sensores de temperatura, deshumidificadores, sistema antincendios, sistemas de vigilancia y controles de acceso. Esta medida no solo protege a los servidores de posibles inundaciones, sino que también se centraliza la gestión de la red. Para comprender mejor la relación del costo, se menciona que el salario mínimo vital en el país es de $470, con lo que se puede comprender que la inversión para el rediseño es relativamente alta, sin embargo, los beneficios alcanzados a corto y largo plazo, justifican la inversión.

3.2. Simulación en GS3

La propuesta del rediseño de red fue simulada en GNS3 que es una herramienta de software libre que permite la simulación de redes de comunicaciones que integra diferentes dispositivos virtuales para el diseño, prueba y verificación de infraestructuras de red [16].

Se replicó la topología completa, incluyendo switches, routers, VLANs y el firewall, para evaluar escenarios realistas, la segmentación de la red se logró mediante la creación de 16 VLANs ver figura 3., cada una asociada a un grupo específico de usuarios los cuales se detallaron en la Tabla 3.

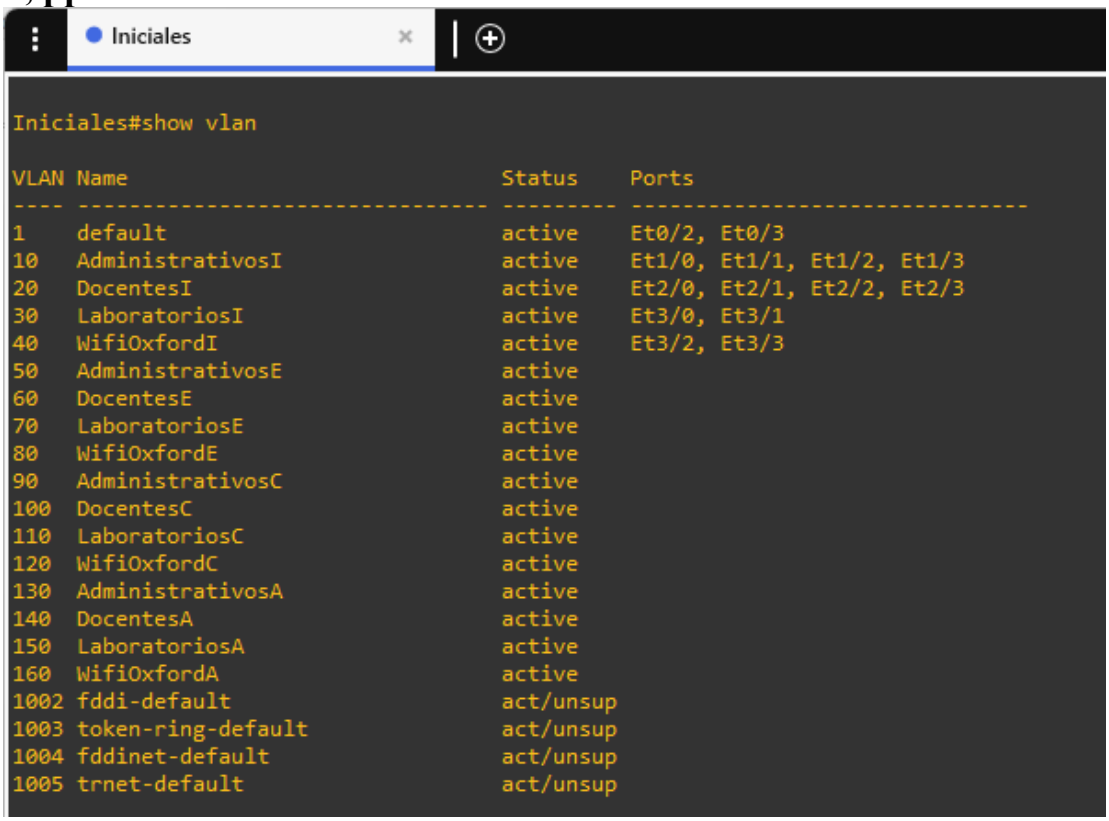

Figura 3. VLAN creadas

Para habilitar la comunicación entre VLANs, se configuraron subinterfaces en el router principal, ver figura 4.

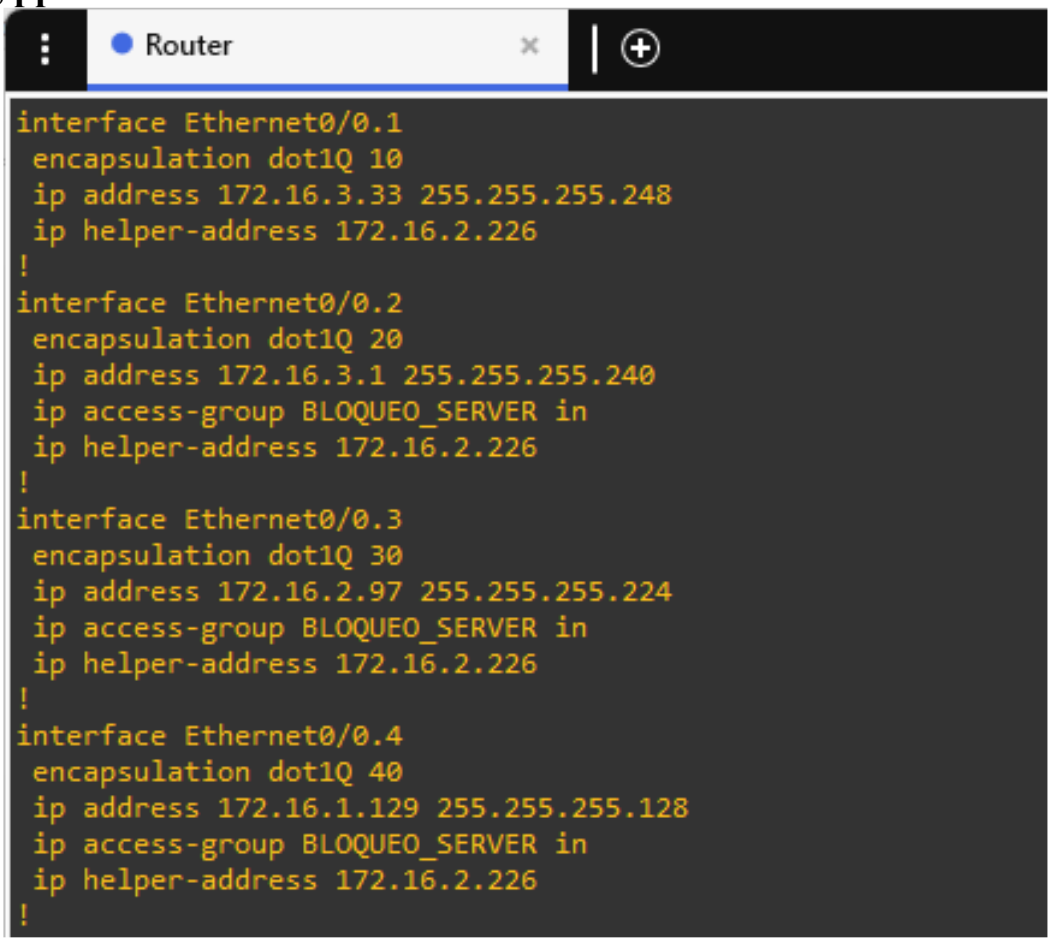

Figura 4. InterVLAN en el router

En materia de seguridad, se configuraron varios protocolos y controles de seguridad en los dispositivos de red. En los switches, se activó Port Security para limitar el acceso por puerto a dos direcciones MAC, ver Figura 5, si un dispositivo con otra dirección MAC intenta comunicarse a través de ese puerto, Port Security deshabilitará el puerto.

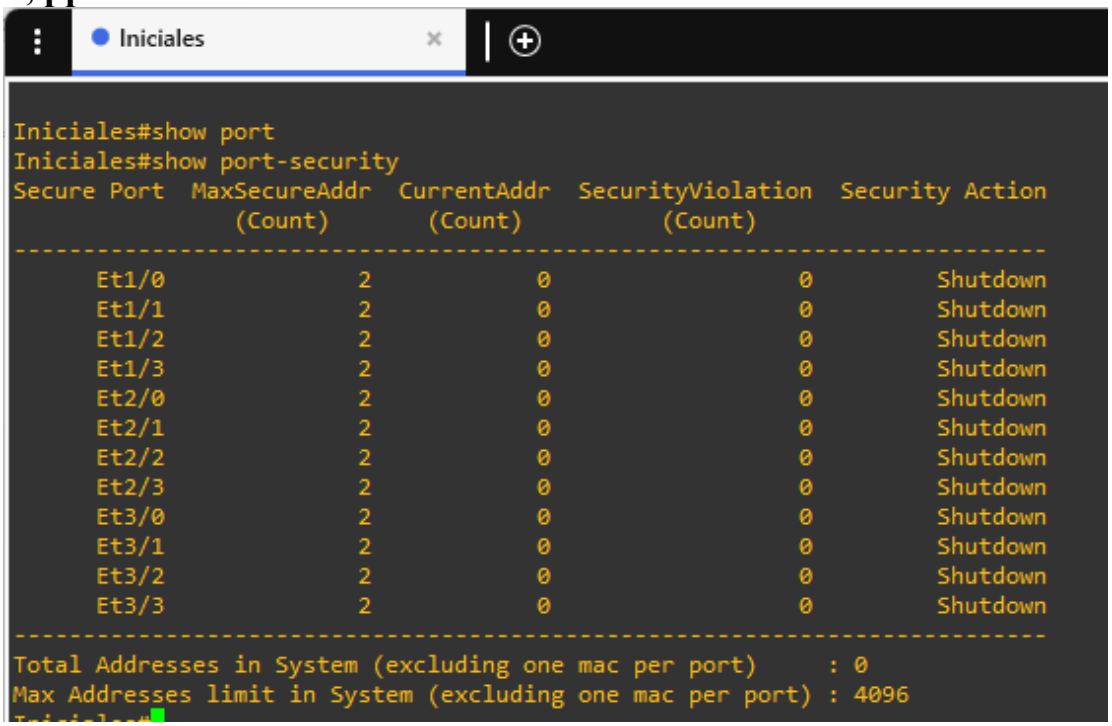

Figura 5. Seguridad en el switch

Al ser una red redundante se habilita por defecto el protocolo STP y es necesario configurar el BPDU (*Bridge Protocol Data Unit) Guard* para prevenir ataques al protocolo en los puertos de acceso; si detecta tráfico de control de switches (BPDUs) en un puerto que debería estar conectado solo a un host, lo bloquea inmediatamente para proteger la red, ver Figura 6.

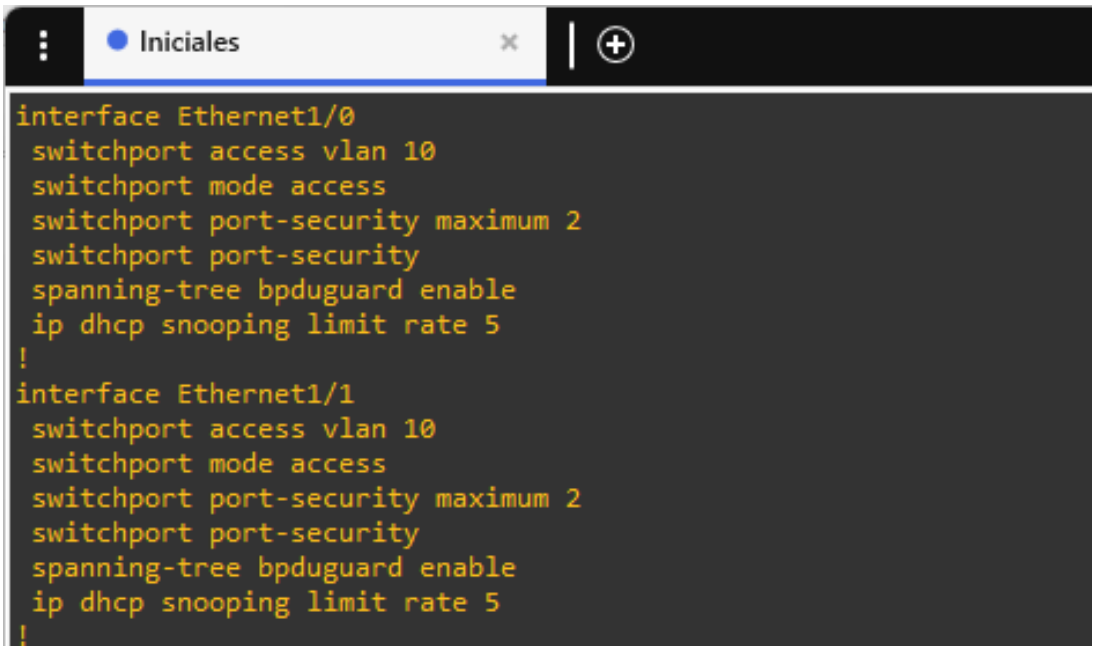

Figura 6. Seguridad BPDU Guard

Se configuró DHCP *Snooping* en los puertos no confiables, bloqueando mensajes DHCP no autorizados después de cinco solicitudes, con esta medida de seguridad se evita el ataque DHCP *Starvation,* ver Figura 7.

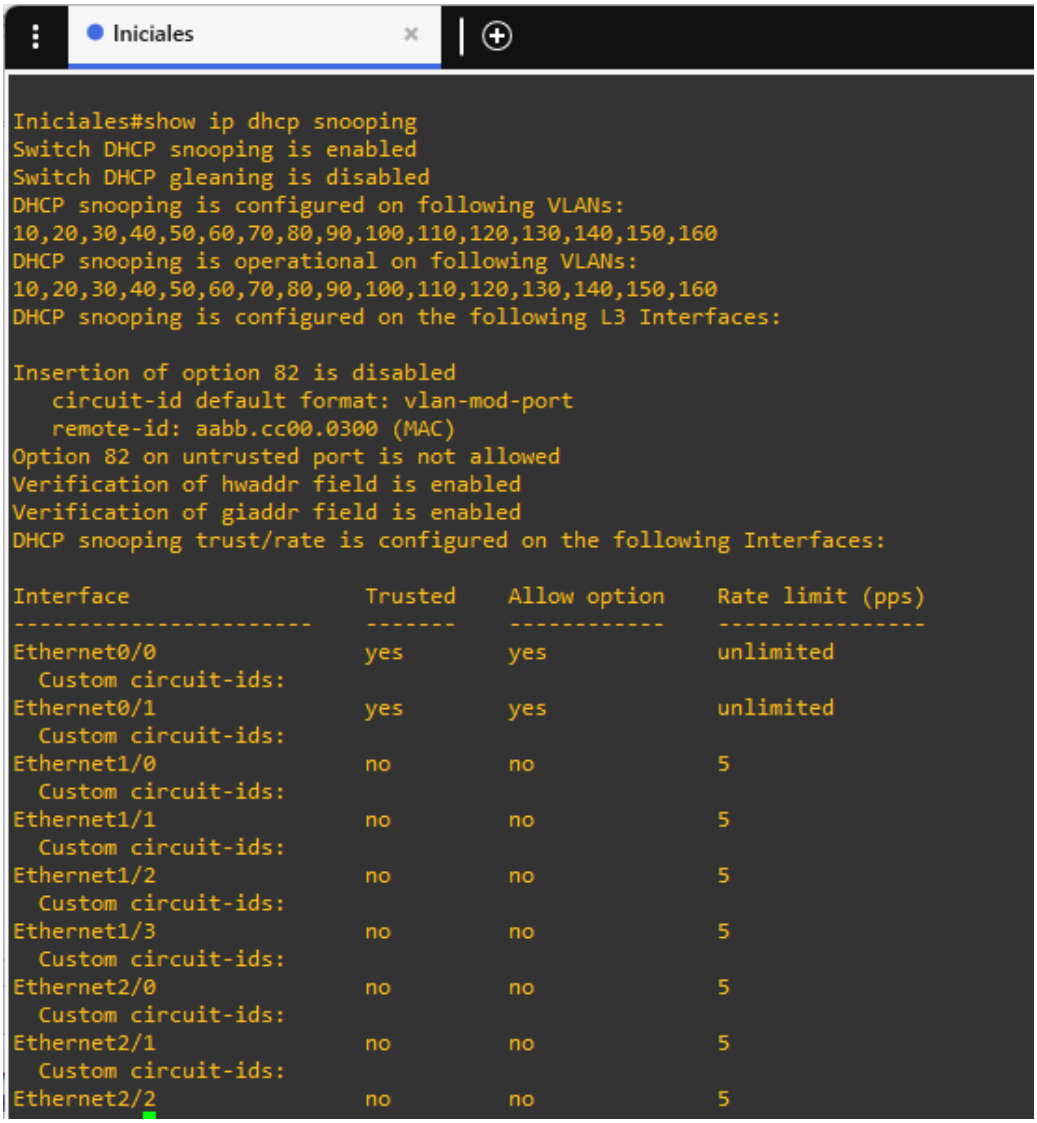

Figura 7. Seguridad DHCP Snooping

Además, se configuraron ACLs extendidas en el router que restringen el acceso al servidor contable únicamente a las subredes administrativas (VLANs 10, 50, 90 y 130), tal como se detalla en los comandos de configuración, ver Figura 8.

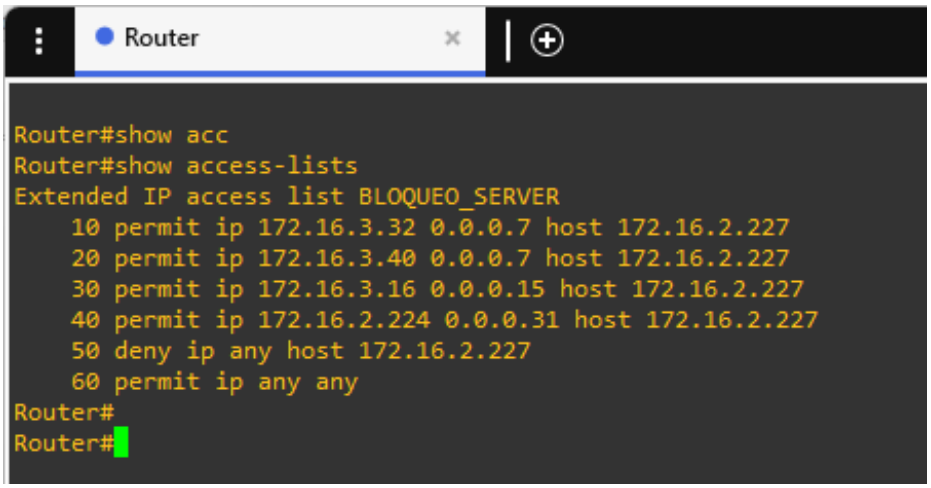

Figura 8. Seguridad DHCP Snooping

Una vez terminadas las configuraciones se realizaron pruebas de conectividad, una prueba crítica fue la comunicación InterVLAN, donde se verificó, por ejemplo, que hosts en la VLAN 20 (docentes) pudieron acceder a recursos en la VLAN 130 (administrativos) a través del acceso permitido en las ACLs.

Con las medidas de seguridad aplicadas se simularon ataques internos a la red LAN con herramientas como Yersinia para generar ataques de DHCP Spoofing, BPDU y macof para pruebas de MAC Flooding. Los resultados demostraron que las configuraciones de seguridad mitigaron efectivamente estas amenazas, aislando puertos comprometidos en modo err-disable. Además, se midió el impacto de la segmentación en el rendimiento, verificando una reducción del 60% en el tráfico de broadcast mediante capturas de paquetes en Wireshark, para los ataques externos se establecieron reglas en el firewall, y así evitar acceso no autorizados. Esta simulación permitió probar el funcionamiento del rediseño antes de su implementación física que no es parte de este reporte.

3.3. Validación técnica

El rediseño fue socializado con especialistas en el área de Redes y comunicaciones, quienes evaluaron diferentes criterios ver Tabla 4. Los especialistas destacaron la escalabilidad en el diseño para una expansión futura y la relación costo-beneficio de migrar a cableado categoría 6. Todos los criterios obtuvieron un 100% de aprobación, respaldando la viabilidad del diseño. Como paso adicional, se elaboró un plan de migración que detalla tiempos, responsables y procedimientos para minimizar interrupciones durante la implementación física.

Tabla 4. Criterios de evaluación.

Criterio	Especialista 1	Especialista 2	Resultado de la Validación
Estructura y Organización	100%	100%	100%
Satisfacción de Requerimientos	100%	100%	100%
Adaptabilidad	100%	100%	100%
Costos	100%	100%	100%
Seguridad de la red	100%	100%	100%
Claridad y Comprensión	100%	100%	100%
Escalabilidad	100%	100%	100%
PORCENTAJE DE VALIDACION TOTAL			**100%**

Los especialistas también resaltaron la claridad de la documentación técnica, que incluyó scripts de configuración y diagramas detallados. Esta validación respaldó no solo la viabilidad técnica del proyecto, sino también su alineación con las mejores prácticas de la industria.

4. CONCLUSIONES

- La conectividad y el uso de tecnologías son elementos fundamentales hoy en día en la educación, por lo que resulta imprescindible que las instituciones educativas cuenten con infraestructuras de red fiables, seguras y eficientes. En este contexto, en la Unidad Educativa Oxford se desarrolló de una propuesta de estudio de su red de comunicaciones, la misma que fue planificada mediante el método Kanban, facilitando el seguimiento y control efectivo del proyecto. Las fases que se desarrollaron en esta propuesta de estudio son: fase de Análisis, donde se evidenció una infraestructura de red fragmentada, sin planificación técnica, con dispositivos subutilizados, incumplimiento de normas de cableado estructurado y un elevado tráfico de broadcast.
- La fase de Diseño de la solución incluyó el rediseño de la infraestructura de red, un nuevo direccionamiento IP, la segmentación mediante VLANs, cumplimiento de normativas de cableado estructurado como backbone de fibra óptica, cambio a cableado UTP categoría 6, enlaces redundantes y medidas de seguridad, con una inversión estimada de 14 000 USD. Además, se establecieron sugerencias con el ISP, y consideraciones futuras para la administración de la red.
- La fase de Validación de la propuesta incluyó la simulación del rediseño en GNS3 demostrando la viabilidad técnica de la propuesta, logrando una reducción del 60 % del tráfico de broadcast y mitigando ataques internos mediante configuraciones de seguridad. La solución no solo mejoró el rendimiento y la seguridad de la red, sino que

también estableció una base escalable y sostenible, que puede servir como referencia para otras instituciones educativas que requieran una planificación de red con enfoque en eficiencia y ciberseguridad.

5. BIBLIOGRAFÍA

[1] G. Millán Naveas, M. Vargas Guzmán, G. Millán Naveas, y M. Vargas Guzmán, «A flow control algorithm for high-speed computer networks», *Ingeniare Rev. Chil. Ing.*, vol. 28, n.º 1, pp. 24-30, mar. 2020, doi: 10.4067/S0718-33052020000100024.

[2] R. Hajıyeva, N. Rustamov, I. B. Sapaev, y A. Akhmedov, «Computer Network Design Problem», en *Applications of Mathematics in Science and Technology*, CRC Press, 2025. [En línea]. Disponible en: https://doi.org/10.1201/9781003606659-4

[3] S. A. Guapi Acán, R. C. Oñate López, y S. B. Anilema Mejía, «Estudio de la infraestructura de redes LAN de las instituciones educativas de la ciudad de Riobamba en el año 2021», vol. 9, pp. 508-527, doi: https://doi.org/10.23857/dc.v9i1.3148.

[4] W. Yang, «Design and Implementation of Real-time Computer Network Security Monitoring System», en *Proceedings of the 2024 2nd International Conference on Artificial Intelligence, Systems and Network Security*, en AISNS '24. New York, NY, USA: Association for Computing Machinery, mar. 2025, pp. 292-296. doi: 10.1145/3714334.3714383.

[5] A. P. Guimarães, P. R. Martins Maciel, y R. Matias, «Optimization of computer networks design integrating dependability and business aspects», en *2020 IEEE Latin-American Conference on Communications (LATINCOM)*, nov. 2020, pp. 1-6. doi: 10.1109/LATINCOM50620.2020.9282310.

[6] O. A. Dowins y O. M. Cornelio, «Computer Network Design of the office area of the telecommunications company SERTOD», *Fusion Pract. Appl.*, n.º Issue 1, pp. 26-31, ene. 2021, doi: 10.54216/FPA.060101.

[7] V. Bhuse, «Detecting Rogue Switch and Device Behaviour Using Network Anomalies in LAN», *Eur. Conf. Cyber Warf. Secur.*, vol. 24, pp. 42-51, jun. 2025, doi: 10.34190/eccws.24.1.3705.

[8] «Unidad Educativa Oxford». Accedido: 16 de septiembre de 2025. [En línea]. Disponible en: https://www.oxford.edu.ec/

[9] F. Vega-Tapia y V. Pailiacho-Mena, «Rediseño de la red de comunicaciones de la Unidad Educativa Oxford», 2024, Accedido: 16 de septiembre de 2025. [En línea]. Disponible en: https://repositorio.puce.edu.ec/handle/123456789/44096

[10] N. L. Sowjanya, «An Efficient VLAN Implementation to decrease Traffic Load in a Network», *Int. J. Adv. Trends Comput. Sci. Eng.*, vol. 9, n.º 2, pp. 2147-2153, abr. 2020, doi: 10.30534/ijatcse/2020/189922020.

[11] E. Ariganello, *Redes CISCO. Guía de estudio para la certificación CCNA Security*.

[12] A. H. Abdi, L. Audah, A. M. Omar, y M. J. Abdiaziz, «Design and Simulation of a Secured Enterprise Network Architecture for All Departments at East Africa University (EAU), Somalia», en *2024 4th International Conference of Science and Information Technology in Smart Administration (ICSINTESA)*, jul. 2024, pp. 552-557. doi: 10.1109/ICSINTESA62455.2024.10747898.

[13] K. Gallegos y V. Pailiacho-Mena, «Plan de transición de IPV4 a IPV6 en una red LAN», PUCESA. [En línea]. Disponible en: https://repositorio.puce.edu.ec/items/1d8189dd-9f4b-4501-96c9-ab52448a2b71

[14] E. Garcés Freire y V. Pailiacho Mena, *Kanban como herramienta de gestión para actividades en grupos de investigación informáticos*. 2023. [En línea]. Disponible en: https://www.pucesi.edu.ec/webs2/libros-docentes/2023/libro-ciencia-innovacion-tecnologia.pdf

[15] S. Shafiq y I. Inayat, «Towards Studying the Communication Patterns of Kanban Teams: A Research Design», en *2017 IEEE 25th International Requirements Engineering Conference Workshops (REW)*, sep. 2017, pp. 303-306. doi: 10.1109/REW.2017.34.

[16] M. A. Calle *et al.*, «Comparación de Parámetros para una Selección Apropiada de Herramientas de Simulación de Redes», *Inf. Tecnológica*, vol. 29, n.º 6, pp. 253-266, dic. 2018, doi: 10.4067/S0718-07642018000600253.