UNIVERSIDAD SANTO TOMÁS DE AQUINO
SECCIONAL TUNJA

FACULTAD DE INGENIERÍA ELECTRÓNICA

DISEÑO DE GUÍAS PRÁCTICAS DE FUNDAMENTOS DE CIBERSEGURIDAD CISCO

Trabajo de grado que presenta

SANTIAGO AGUILAR CÁRDENAS

Para obtener el título profesional de

INGENIERO ELECTRÓNICO

Tunja - Colombia
Febrero - 2026

UNIVERSIDAD SANTO TOMÁS DE AQUINO
SECCIONAL TUNJA

FACULTAD DE INGENIERÍA ELECTRÓNICA

DISEÑO DE GUÍAS PRÁCTICAS DE FUNDAMENTOS DE CIBERSEGURIDAD CISCO

Trabajo de grado que presenta

SANTIAGO AGUILAR CÁRDENAS

Director del trabajo de Grado:

Ph.D. William Fabián Chaparro Becerra

Codirectores del trabajo de Grado:

M.Sc. Angélica María Salazar Madrigal

M.Sc. Cristian David Camacho Parra

Tunja - Colombia
Febrero - 2026

Exoneración de Responsabilidades

Exonero de cualquier responsabilidad directa o indirecta a la Universidad Santo Tomás o a la Facultad de Ingeniería Electrónica por el contenido de este proyecto. Garantizo que la investigación, resultados, análisis, prácticas elaboradas y conclusiones aquí presentados son de mi entera autoría y exclusiva responsabilidad.

Dedicatoria

A mi familia, y en especial a mis padres y hermanos, por su amor incondicional, su apoyo constante y su paciencia infinita. Gracias por enseñarme con su ejemplo el valor del esfuerzo, la perseverancia y la honestidad, y por estar siempre a mi lado en cada paso de este camino. Su confianza en mí me dio la fuerza para superar los momentos difíciles y la motivación para seguir adelante. Les dedico este logro con todo mi corazón, porque nada de esto habría sido posible sin ustedes.

Agradecimientos

Quiero expresar mi más sincero agradecimiento a todas las personas que, con su apoyo y orientación, han hecho posible mi aprendizaje y crecimiento a lo largo de este camino.

En primer lugar, agradezco a los ingenieros que me guiaron y enseñaron con dedicación y paciencia, formando parte fundamental de mi crecimiento profesional y personal. De manera muy especial, quiero reconocer la orientación y el apoyo de mi director de trabajo de grado, William Fabián Chaparro Becerra. Igualmente, agradezco a mis codirectores, Angélica María Salazar Madrigal y Cristian David Camacho Parra, por su acompañamiento, sus consejos y su compromiso con mi aprendizaje.

A todos los que compartieron conmigo experiencias, aprendizajes y buenos momentos, quiero agradecerles por su apoyo, su compañerismo y por hacer que cada reto fuera más llevadero y enriquecedor. A mis amigos, que siempre estuvieron presentes brindándome ánimo, motivación y comprensión, les expreso mi más sincera gratitud.

Cada uno de ustedes ha dejado una huella especial en mi, y este logro también refleja su esfuerzo, enseñanzas y amistad.

Índice general

Índice de figuras

Resumen

El presente trabajo aborda el diseño, desarrollo y validación de un conjunto de guías prácticas orientadas a la enseñanza de fundamentos de ciberseguridad y redes en el contexto de la formación universitaria en ingeniería. La propuesta surge ante la necesidad de fortalecer el aprendizaje práctico en laboratorio mediante materiales estructurados que permitan integrar conceptos teóricos con la configuración y operación de infraestructuras de red reales. Para ello, se empleó una metodología basada en el Aprendizaje Basado en Problemas (ABP), en coherencia con el modelo educativo institucional, orientada a la resolución de situaciones representativas de escenarios reales de redes y seguridad.

Las guías desarrolladas abarcan contenidos relacionados con introducción a la ciberseguridad, direccionamiento IP y subneteo, configuración de routers Cisco, listas de control de acceso (ACL), VPNs IPsec y firewalls ASA, combinando el uso de herramientas de simulación y equipos físicos disponibles en laboratorio. Como parte del proceso, se realizó una fase de validación técnica de los equipos de red, identificando y solucionando problemas de configuración y funcionamiento en dispositivos nuevos y antiguos, garantizando su operatividad para las prácticas propuestas.

La evaluación del aprendizaje se planteó mediante el uso de rúbricas evaluativas, concebidas como instrumentos de valoración integral del desempeño del estudiante, considerando criterios técnicos, funcionales y de gestión del tiempo durante la ejecución

de las actividades. Los resultados evidencian que las guías permiten estandarizar las prácticas de laboratorio, facilitan la correcta implementación de configuraciones de red y contribuyen al desarrollo de competencias técnicas y analíticas, favoreciendo la autonomía del estudiante y la aplicación de los conocimientos adquiridos en nuevos escenarios.

Palabras Clave: Ciberseguridad, Cisco, Aprendizaje Basado en Problemas, Protocolos de seguridad

Abstract

This paper addresses the design, development, and validation of a set of practical guidelines aimed at teaching the fundamentals of cybersecurity and networks in the context of university engineering education. The proposal arises from the need to strengthen practical learning in the laboratory through structured materials that allow theoretical concepts to be integrated with the configuration and operation of real network infrastructures. To this end, a methodology based on Problem-Based Learning (PBL) was used, in line with the institutional educational model, aimed at resolving situations representative of real network and security scenarios.

The guides developed cover content related to an introduction to cybersecurity, IP addressing and subnetting, Cisco router configuration, access control lists (ACLs), IPsec VPNs, and ASA firewalls, combining the use of simulation tools and physical equipment available in the laboratory. As part of the process, a technical validation phase of the network equipment was carried out, identifying and solving configuration and operational problems in new and old devices, ensuring their operability for the proposed practices.

Learning assessment was carried out using evaluation rubrics, designed as comprehensive tools for assessing student performance, taking into account technical, functional, and time management criteria during the execution of activities. The results show that the guides allow for the standardization of laboratory practices, facilitate the

correct implementation of network configurations, and contribute to the development of technical and analytical skills, promoting student autonomy and the application of acquired knowledge in new scenarios.

Keywords: Cybersecurity, Cisco, Problem-Based Learning, Security Protocols

Capítulo 1

Introducción

El presente trabajo se desarrolla como un proyecto de innovación tecnológica y educativa, orientado a la mejora de la enseñanza de ciberseguridad dentro de la Facultad de Ingeniería Electrónica de la Universidad Santo Tomás, seccional Tunja, con validación técnica interna que delimita su alcance al contexto institucional.

El aumento sostenido de incidentes, ataques y vulnerabilidades en los entornos digitales ha posicionado a la ciberseguridad como un componente fundamental en la formación de ingenieros. La protección de la información, la disponibilidad de los servicios y la integridad de las redes demandan profesionales capaces no solo de comprender los principios teóricos de la seguridad informática, sino también de aplicar dichos conocimientos en escenarios técnicos reales.

En el contexto universitario, la enseñanza de la ciberseguridad requiere integrar la comprensión de los principios de ciberseguridad con la configuración, el enrutamiento y la operación de infraestructuras de red, mediante actividades prácticas que permiten aplicar y validar los conceptos estudiados. Este enfoque permite que el aprendizaje se valide a través de la implementación y comprobación del funcionamiento de routers, switches y dispositivos de seguridad, produciendo resultados medibles y verificables en escenarios de laboratorio.

La Facultad de Ingeniería Electrónica de la Universidad Santo Tomás, seccional Tunja, cuenta con infraestructura Cisco que permite el desarrollo de prácticas de redes y ciberseguridad. No obstante, la ausencia de guías prácticas estructuradas, coherentes y estandarizadas ha dificultado la uniformidad en las experiencias de laboratorio, la progresión ordenada de los contenidos y la evaluación objetiva del desempeño de los estudiantes. Esta situación limita la posibilidad de que los estudiantes consoliden habilidades técnicas de forma sistemática y autónoma.

Ante esta necesidad, el presente trabajo propone el diseño de un conjunto de guías prácticas orientadas a los fundamentos de redes y ciberseguridad, con énfasis en la configuración y análisis de listas de control de acceso (ACL), redes privadas virtuales (VPN) IPsec y firewalls Cisco ASA. Las guías integran el uso de herramientas de simulación, específicamente Cisco Packet Tracer, con prácticas en laboratorio físico, buscando fortalecer el aprendizaje aplicado, facilitar la replicabilidad de las configuraciones y aportar un recurso didáctico alineado con las exigencias actuales de la formación en seguridad de redes.

1.1. Planteamiento del Problema

En los últimos años se ha evidenciado un crecimiento exponencial en la complejidad y frecuencia de los ciberataques a nivel mundial, lo que ha intensificado la demanda de profesionales altamente capacitados en la implementación de protocolos de ciberseguridad específicos en infraestructura de red (Bautista et al., 2023). Cisco Networking Academy ha impactado más de 20 millones de estudiantes en 190 países desde 1997, evidenciando la importancia global de la formación especializada en tecnologías Cisco para la ciberseguridad (Cisco Networking Academy, nd). Esta situación crítica plantea desafíos significativos para las instituciones de educación superior en el desarrollo de programas académicos que preparen efectivamente a los

estudiantes para configurar e implementar protocolos de seguridad Cisco en entornos reales.

Los desafíos específicos en la formación de protocolos Cisco incluyen la escasez de recursos didácticos especializados que integren teoría con configuraciones avanzadas, la limitada disponibilidad de ejercicios prácticos que simulen entornos reales, y la necesidad crítica de desarrollar competencias técnicas específicas en comandos Cisco IOS y troubleshooting de protocolos, problemática que se ha intensificado durante la educación remota (Accenture, 2024). En la Facultad de Ingeniería Electrónica de la Universidad Santo Tomás, esta situación se manifiesta específicamente en el Laboratorio de Telecomunicaciones, donde, a pesar de contar con dispositivos como routers, switches y herramientas de simulación, la ausencia de material didáctico que integre efectivamente estos recursos físicos con herramientas de simulación representa una oportunidad desaprovechada para fortalecer el perfil profesional de los egresados y posicionar la facultad como referente en formación especializada en ciberseguridad aplicada.

Ante este escenario, surge la necesidad crítica de desarrollar guías educativas estructuradas que aborden la brecha existente entre la formación teórica en ciberseguridad y las competencias prácticas específicas requeridas para la configuración e implementación de protocolos de seguridad en equipos Cisco. En este contexto, se plantea la siguiente pregunta de investigación:

1.2. Formulación de Pregunta

¿Cómo diseñar guías prácticas de laboratorio que integren el uso de Cisco Packet Tracer y dispositivos de red físicos, estructuradas bajo el enfoque de Aprendizaje Basado en Problemas, para abordar contenidos fundamentales de redes y ciberseguridad Cisco

(ACLs, VPN IPsec, firewall ASA) en el contexto de la formación universitaria?

1.3. Justificación

La presente propuesta de investigación surge de una necesidad crítica identificada en el contexto educativo actual: la brecha existente entre la formación teórica en ciberseguridad y las competencias prácticas específicas requeridas para la implementación de protocolos de seguridad en equipos Cisco. Esta problemática adquiere particular relevancia considerando que las instituciones educativas enfrentan crecientes riesgos de ciberseguridad, siendo objetivo de aproximadamente 388 incidentes cibernéticos diarios en instituciones de Latinoamérica, lo que equivale a más de 2.700 ataques por institución, según estudios recientes de ciberseguridad (Bautista et al., 2023).

Este proyecto es particularmente relevante para el programa de Ingeniería Electrónica, ya que integra conocimientos fundamentales de redes y comunicaciones, áreas centrales en la formación del ingeniero electrónico con las competencias emergentes en ciberseguridad, las cuales son cada vez más críticas en un mundo hiperconectado. La capacidad de configurar, asegurar y administrar infraestructuras de red utilizando dispositivos como el router Cisco ISR 1100 4G, Cisco 1841, no solo fortalece el perfil técnico de los estudiantes, sino que también los prepara para enfrentar los desafíos de la industria 4.0.

Además del componente técnico, el proyecto tiene un enfoque pedagógico orientado a la formación integral de los estudiantes. Las guías prácticas no solo buscan el dominio de configuraciones de red y ciberseguridad en dispositivos Cisco, sino también desarrollar competencias de aprendizaje autónomo, pensamiento crítico y trabajo colaborativo, en coherencia con el modelo pedagógico institucional de la Universidad Santo Tomas, fundamentado en el Aprendizaje Basado en Problemas (ABP). El

proyecto trasciende la dimensión técnica para convertirse en una herramienta académica que fortalece el proceso de enseñanza-aprendizaje en el área de redes y ciberseguridad (Albarracín and Camacho, 2010).

El proyecto se justifica como una respuesta integral a las necesidades actuales de formación en redes y ciberseguridad, al abarcar tanto los principios fundamentales de la infraestructura de red como la implementación de protocolos de seguridad Cisco. De esta manera, se proporciona un enfoque práctico y progresivo que fortalece el desarrollo de competencias técnicas y contribuye al fortalecimiento en el área de redes y ciberseguridad.

1.4. Objetivos

1.4.1. Objetivo General

Diseñar guías prácticas integrales sobre protocolos de ciberseguridad Cisco como material didáctico para estudiantes de pregrado de Ingeniería Electrónica, mediante el uso de Cisco Packet Tracer y los recursos del laboratorio de Telecomunicaciones de la Universidad Santo Tomás.

1.4.2. Objetivos Específicos

- Identificar y estructurar los contenidos fundamentales del curso Cisco Networking Academy, adaptándolos a las necesidades específicas del contexto académico y recursos disponibles en el laboratorio de telecomunicaciones.
- Desarrollar guías prácticas para la implementación de protocolos fundamentales de redes y ciberseguridad, incluyendo listas de control de acesso (ACLs), VPNs IPsec y Firewalls, en entornos controlados.
- Elaborar material práctico bajo el enfoque pedagógico de Aprendizaje Basado en Problemas (ABP), que promueve la solución de situaciones reales de redes y ciberseguridad, en coherencia con el modelo educativo de la Universidad Santo

Tomás y con fines académicos orientados al fortalecimiento del proceso de enseñanza-aprendizaje.

Capítulo 2

Fundamentos y Contexto Actual de la Investigación

Este capítulo presenta los fundamentos teóricos y conceptuales que sustentan el desarrollo de las guías prácticas de ciberseguridad. Se abordan, en primer lugar, los conceptos esenciales de redes de datos que constituyen el prerrequisito técnico para la implementación de configuraciones de seguridad y, en segundo lugar, los principios y tecnologías de ciberseguridad que conforman el núcleo temático de las prácticas de laboratorio.

2.1. Fundamentos de redes de datos

El desarrollo de competencias en ciberseguridad aplicada a infraestructuras de red requiere una base sólida de conocimientos en el área de redes de comunicaciones. Los contenidos presentados a continuación se organizan en función de su relevancia para la comprensión de los mecanismos de protección que se implementan en dispositivos Cisco y de su alineación con los temas abordados en la asignatura de Transmisión de Datos del programa de Ingeniería Electrónica.

2.1.1. Clasificación de redes

Las redes de comunicaciones se clasifican según su alcance geográfico, distinguiendo entre redes de área local (LAN), que interconectan dispositivos en espacios geográficos limitados como edificios u oficinas, y redes de área amplia (WAN), que permiten la comunicación entre ubicaciones geográficamente distantes mediante enlaces de telecomunicaciones. Esta distinción resulta fundamental para comprender la arquitectura de las redes empresariales modernas, donde diferentes segmentos LAN se interconectan a través de infraestructuras WAN, y donde las políticas de seguridad deben considerar las diferentes características y niveles de confianza de cada tipo de red. Adicionalmente, se consideran las redes de área metropolitana (MAN) y las redes de área personal (PAN), proporcionando una visión completa de la clasificación de redes según su escala.

2.1.2. Modelos de referencia: OSI y TCP/IP

La comprensión de las redes requiere el conocimiento de los modelos de referencia que organizan jerárquicamente las funciones de comunicación. El modelo OSI (Open Systems Interconnection) estructura las funciones de red en siete capas: física, enlace de datos, red,transporte, sesión, presentación y aplicación, donde cada capa proporciona servicios a la capa superior y utiliza servicios de la capa inferior (Tanenbaum and Wetherall, 2011). Este modelo proporciona un marco conceptual para comprender cómo diferentes protocolos y tecnologías operan en niveles específicos de la arquitectura de comunicaciones.

El modelo TCP/IP, utilizado en la implementación práctica de Internet y redes empresariales, condensa estas funciones en cuatro capas: acceso a red, Internet, transporte y aplicación (Kurose and Ross, 2017). La comprensión de ambos modelos resulta esencial para entender cómo las tecnologías de seguridad como ACLs, que operan en la capa de red, y firewalls, que pueden operar en múltiples capas, se integran

en la arquitectura de comunicaciones.

2.1.3. Sistemas de numeración: binario y hexadecimal

El sistema de numeración binario constituye el fundamento matemático para la comprensión del direccionamiento de red y el funcionamiento de máscaras de subred. El sistema binario, que utiliza únicamente los dígitos 0 y 1, constituye la forma nativa en que los computadores y dispositivos de red representan información. La capacidad de convertir valores entre representación decimal y binaria resulta fundamental para comprender cómo las direcciones IP de 32 bits se representan en notación decimal punteada, y cómo las operaciones lógicas AND entre direcciones IP y máscaras de subred permiten determinar la red a la cual pertenece un host.

Adicionalmente, el sistema hexadecimal, que utiliza 16 símbolos (0-9 y A-F), proporciona una forma más compacta de representar valores binarios y se utiliza extensamente en direcciones MAC de Ethernet y en direcciones IPv6. La comprensión de conversiones entre sistemas decimal, binario y hexadecimal constituye una competencia fundamental para el trabajo con redes (Odom, 2020).

2.1.4. Direccionamiento IPv4

El direccionamiento IP constituye uno de los pilares fundamentales del conocimiento de redes. El protocolo IPv4 utiliza direcciones de 32 bits que se representan en notación decimal punteada mediante cuatro octetos separados por puntos, permitiendo teóricamente más de 4 mil millones de direcciones únicas. La estructura de las direcciones IPv4 incluye una porción de red que identifica el segmento de red al cual pertenece el dispositivo, y una porción de host que identifica el dispositivo específico dentro de esa red (Odom, 2020). La clasificación histórica de direcciones por clases (A, B, C, D y E) definía rangos específicos de direcciones con diferentes divisiones entre porción de red y porción de host, aunque la adopción posterior de CIDR (Classless Inter-Domain Routing) permitió una utilización más flexible del espacio de

direccionamiento.

2.1.5. Direccionamiento IPv6

El protocolo IPv6 fue desarrollado para resolver el agotamiento del espacio de direcciones IPv4 mediante el uso de direcciones de 128 bits, permitiendo un número prácticamente ilimitado de direcciones únicas. Las direcciones IPv6 se representan en notación hexadecimal mediante ocho grupos de cuatro dígitos hexadecimales separados por dos puntos (Deering and Hinden, 2017). Aunque la adopción de IPv6 ha sido gradual, su comprensión resulta cada vez más relevante dado que muchas organizaciones están implementando esquemas de direccionamiento dual-stack que soportan simultáneamente IPv4 e IPv6. Los conceptos de direcciones unicast, multicast y anycast en IPv6, así como mecanismos de autoconfiguración sin estado, representan diferencias significativas respecto a IPv4 que deben ser comprendidas.

2.1.6. Protocolo Ethernet

El protocolo Ethernet constituye la tecnología dominante en la capa de enlace de datos para redes LAN. Ethernet define el formato de las tramas que encapsulan los paquetes IP para su transmisión sobre medios físicos, incluyendo direcciones MAC de origen y destino de 48 bits que identifican únicamente cada interfaz de red (Tanenbaum and Wetherall, 2011). La comprensión del funcionamiento de Ethernet incluye conceptos como el método de acceso al medio CSMA/CD (Carrier Sense Multiple Access with Collision Detection) en implementaciones de medio compartido, aunque las redes Ethernet modernas utilizan predominantemente conexiones full-duplex punto a punto que eliminan colisiones. El conocimiento de las diferentes velocidades de Ethernet (Fast Ethernet a 100 Mbps, Gigabit Ethernet a 1 Gbps, 10 Gigabit Ethernet) y tipos de medios físicos (cables de cobre de par trenzado, fibra óptica) proporciona el contexto para comprender las capacidades y limitaciones de la infraestructura física de red.

2.1.7. Subnetting y VLSM

El subnetting o división de redes en subredes constituye una técnica fundamental que permite la segmentación lógica del espacio de direccionamiento IP mediante la modificación de la máscara de subred. La máscara de subred, valor de 32 bits que se representa en notación decimal punteada o mediante longitud de prefijo en notación CIDR, determina qué porción de una dirección IP corresponde a la red y qué porción al host (Odom, 2020). La capacidad de calcular la máscara de subred apropiada para satisfacer requerimientos específicos de cantidad de subredes o cantidad de hosts, determinar los rangos de direcciones válidas para cada subred, y diseñar esquemas de direccionamiento jerárquicos constituye una competencia crítica para el diseño y administración de redes.

La técnica de máscaras de subred de longitud variable (VLSM) permite optimizar el uso del espacio de direccionamiento al asignar bloques de diferentes tamaños según las necesidades específicas de cada segmento, procedimiento que requiere una planificación cuidadosa para evitar solapamiento de rangos de direcciones.

2.2. Fundamentos de ciberseguridad

Los contenidos de ciberseguridad se fundamentan en el currículo Cisco Networking Academy y en los estándares internacionales de seguridad de la información. El dominio de defensa de redes resulta particularmente relevante para el presente proyecto, dado que aborda la protección de la infraestructura de comunicaciones mediante la implementación de tecnologías y protocolos de seguridad en dispositivos Cisco.

2.2.1. Principios de seguridad de la información

La tríada CIA (Confidencialidad, Integridad y Disponibilidad) representa los tres objetivos principales que busca garantizar cualquier sistema de seguridad (National Institute of Standards and Technology, 2024). La confidencialidad se refiere a la

protección de la información contra acceso no autorizado mediante controles de acceso y técnicas de cifrado. La integridad se refiere a la protección contra modificación no autorizada mediante funciones hash criptográficas y firmas digitales. La disponibilidad se refiere a garantizar que la información y los servicios estén accesibles cuando se requieran mediante la implementación de redundancia y diseño de arquitecturas tolerantes a fallas.

Los sistemas de control de acceso han evolucionado hacia arquitecturas multicapa que integran autenticación y autorización como componentes esenciales. Los modelos contemporáneos de seguridad y control requieren comprensión profunda de protocolos específicos y su implementación en dispositivos especializados (Anderson, 2020). Los enfoques actuales en seguridad enfatizan la importancia de implementar defensas en profundidad que combinen múltiples tecnologías y estrategias.

2.2.2. Access Control Lists (ACLs)

Las Access Control Lists (ACLs) representan una tecnología fundamental en la implementación de políticas de seguridad en redes Cisco. Estas herramientas permiten filtrar tráfico de red basándose en criterios específicos como direcciones IP, protocolos y puertos, proporcionando control sobre el flujo de información. La correcta implementación de ACLs constituye una medida efectiva para mitigar intentos de acceso no autorizado en redes empresariales (Calle García et al., 2024).

La configuración avanzada de ACLs requiere comprensión profunda de sintaxis especifica de Ciscos IOS y principios de seguridad de redes. Los profesionales con competencias sólidas en configuración de ACLs demuestran mayor efectividad en la detección y mitigación de amenazas de red en tiempo real, evidenciando la importancia crítica de esta competencia técnica. (Ahsan and Pathan, 2025).

2.2.3. Virtual Private Network (VPN) Ipsec

Las redes privadas virtuales que implementan el protocolo IPSec representan una tecnología esencial para garantizar comunicaciones seguras sobre infraestructuras públicas. La implementación de VPNs IPSec en dispositivos Cisco requiere configuración específica de políticas de seguridad, algoritmos de cifrado y protocolos de autenticación. Las VPNs IPSec correctamente configuradas proporcionan niveles de seguridad robustos equivalentes a redes privadas físicas, con ventajas operativas significativas (Herrera, 2023).

Los túneles VPNs IPSec implementan múltiples capas de seguridad que incluyen autenticación de dispositivos, cifrado de datos y verificación de integridad. Las organizaciones que utilizan VPNs IPSec experimentan una reducción considerable de incidentes de interceptación de comunicaciones comparado con conexiones no cifradas, validando la efectividad de esta tecnología en la protección de información sensible (Hauser et al., 2020).

2.2.4. Firewall Cisco Adactive Security Appliance (ASA)

Los Firewalls Cisco ASA (Adaptive Security Appliance) representan dispositivos especializados en seguridad perimetral que integran múltiples funcionalidades de protección. Estas plataformas combinan capacidades de statefu firewall, VPN, prevención de intrusiones y filtrado de contenido en una solución unificada. La implementación correcta de firewalls ASA puede prevenir hasta 95 % de los intentos de intrusión externa en redes corporativas (Cisco Systems, Inc., 2013). La configuración avanzada de ASA requiere comprensión específica de sintaxis de comandos, políticas de seguridad y arquitecturas de red. Los profesionales especializados en configuración ASA reducen el tiempo promedio de respuesta a incidentes de seguridad, debido a su capacidad para implementar contramedidas técnicas específicas y efectivas (Teja et al., 2023).

2.3. Panorama global de la ciberseguridad y educación

La evolución de las metodologías educativas en ciberseguridad ha experimentado transformaciones significativas en los últimos años. La proyección pedagógica en ciberseguridad requiere enfoques innovadores que integren teoría y práctica de manera efectiva, respondiendo a la necesidad creciente de profesionales especializados en seguridad digital (Rivera Alturo and Hernández García, 2023).

El enfoque educativo actual en ciberseguridad se caracteriza por metodologías activas que enfatizan el aprendizaje experimental y la simulación de escenarios reales. Las instituciones educativas han desarrollado estrategias pedagógicas que priorizan el "aprender haciendo" a través de laboratorios especializados y entornos controlados de práctica (Ebrahimi et al., 2025). Esta tendencia responde a la demanda del sector productivo de profesionales con competencias técnicas inmediatamente aplicables.

La formación en ciberseguridad ha evolucionado hacia modelos híbridos que combinan fundamentos teóricos con experiencias prácticas intensivas. Las metodologías educativas contemporáneas incorporan elementos como simulaciones de ataques, análisis forense digital y configuraciones de sistemas de defensa, proporcionando a los estudiantes experiencias auténticas en entornos seguros y controlados (Herrero-Martín et al., 2022).

2.4. Metodologías de enseñanza en ciberseguridad

Las metodologías educativas contemporáneas en ciberseguridad han evolucionado hacia enfoques integrados que combinan múltiples estrategias pedagógicas para maximizar el desarrollo de competencias técnicas específicas. La investigación en educación especializada ha identificado que las metodologías más efectivas son aquellas

que integran experiencias prácticas inmediatas con marcos teóricos sólidos, proporcionando a los estudiantes competencias directamente aplicables en entornos profesionales (Ismail et al., 2024).

- **Metodología de aprendizaje basada en casos de estudio reales**

La metodología de enseñanza basada en casos de estudio representa una de las tendencias más efectivas en la educación en ciberseguridad. Permite utilizar análisis detallados de incidentes de seguridad reales proporcionando a los estudiantes una comprensión integral de las amenazas cibernéticas y sus implicaciones (Sánchez et al., 2025). Este modelo comienza con un examen minucioso de brechas de seguridad del mundo real, donde los estudiantes investigan los detalles específicos de estos ataques y comprenden cómo se desarrollaron desde el inicio hasta su conclusión.

La implementación de esta metodología ha demostrado efectividad en el desarrollo de pensamiento crítico y habilidades de solventar problemas. Los estudiantes que participan en programas basados en casos de estudio muestran una mejora en la identificación de vulnerabilidades de seguridad e incremento en la capacidad de proponer soluciones técnicas apropiadas (Suárez et al., 2024). Esta metodología permite que los estudiantes desarrollen una mejor visión de la seguridad, integrando aspectos técnicos y organizacionales en los aspectos de ciberseguridad.

- **Metodología de investigación aplicada**

La metodología de investigación aplicada basada en el desarrollo de recursos didácticos tecnológicos representa un enfoque innovador que integra la investigación científica con la creación de herramientas educativas concretas y verificables. Esta metodología se fundamenta en la premisa de que el conocimiento teórico debe traducirse en aplicaciones prácticas que resuelvan problemáticas específicas del contexto educativo

en ciberseguridad (Aguilar Ojeda et al., 2024).

El proceso metodológico se estructura en ciclos repetitivos que incluyen revisión bibliográfica especializada, análisis de necesidades formativas, diseño de prototipos educativos, implementación controlada y evaluación efectiva. Esta metodología ha demostrado particular efectividad en el desarrollo de guías prácticas y material didáctico para tecnologías específicas como protocolos Cisco, debido a su capacidad para combinar rigor científico con aplicabilidad directa en entornos académicos controlados (López, 2018).

- **Aprendizaje Basado en Problemas (ABP)**

El Aprendizaje Basado en Problemas representa una metodología pedagógica innovadora que sitúa al estudiante en el centro del proceso educativo mediante la confrontación con situaciones problemáticas auténticas y contextualmente relevantes. Esta aproximación metodológica se fundamenta en los principios del constructivismo social, donde el conocimiento emerge a través de la interacción activa con problemas del mundo real, promoviendo el desarrollo de competencias cognitivas superiores como el análisis crítico, la síntesis de información compleja y la toma de decisiones fundamentadas (Albarrán Torres and Díaz Larenas, 2021). El ABP trasciende la mera transmisión de contenidos para convertirse en un proceso dinámico donde los estudiantes desarrollan autonomía intelectual, capacidad investigativa y habilidades que les permiten autorregular su aprendizaje y transferir conocimientos a contextos diversos.

- **Justificación Institucional de la Metodología**

La selección del Aprendizaje Basado en Problemas como enfoque metodológico para el desarrollo del presente proyecto se sustenta en el modelo pedagógico adoptado por la Universidad Santo Tomás, institución que promueve un enfoque formativo centrado en el aprendizaje activo, la construcción autónoma del conocimiento y la solución de

problemáticas reales del contexto profesional y social (Tomás, 2023). En coherencia con su Proyecto Educativo Institucional, la Universidad Santo Tomás fomenta metodologías que fortalecen la formación integral, el pensamiento crítico y la articulación entre teoría y práctica.

En este sentido, la adopción del ABP no solo responde a criterios pedagógicos contemporáneos, sino también a la alineación con los lineamientos académicos institucionales, garantizando coherencia entre el diseño metodológico del proyecto y el modelo formativo de la universidad. De esta manera, el proyecto se integra de manera consistente dentro del marco académico institucional, fortaleciendo su pertinencia y validez formativa.

- **Principales Beneficios y Capacidades del ABP**

La implementación del Aprendizaje Basado en Problemas permite el desarrollo de múltiples competencias académicas y profesionales de alto nivel, entre las que destacan:

Desarrollo de habilidades superiores: Fomenta el pensamiento crítico, la resolución de problemas complejos, la formulación de hipótesis y la capacidad investigativa, fortaleciendo procesos de análisis, argumentación y toma de decisiones fundamentadas.

Aprendizaje activo y autónomo: El estudiante asume un rol protagónico en la construcción de su conocimiento, gestiona su propio proceso de aprendizaje y desarrolla estrategias de autorregulación, lo que contribuye a disminuir la ansiedad académica y aumentar la motivación intrínseca.

Fortalecimiento de competencias transversales: Potencia el trabajo colaborativo, la comunicación efectiva, la capacidad de liderazgo, la gestión del tiempo y la toma de decisiones en escenarios reales o simulados, habilidades esenciales para el desempeño profesional.

- **Estructura Metodológica del ABP**

La implementación del ABP en entornos educativos sigue una secuencia estructurada que maximiza su efectividad pedagógica. El proceso inicia con la presentación de un problema estructurado, caracterizado por su complejidad, ambigüedad y múltiples soluciones posibles, diseñado para activar conocimientos previos y generar conflicto cognitivo (Peralta Lara and Guamán Gómez, 2020). Los estudiantes, organizados en equipos de trabajo, participan en un proceso de análisis colaborativo donde identifican los elementos conocidos, formulan hipótesis preliminares y determinan los vacíos de conocimiento que deben abordar.

La fase de investigación autodirigida permite a los participantes explorar diversas fuentes de información, desarrollar criterios para la evaluación de evidencias y construir marcos conceptuales sólidos. Finalmente, la síntesis y presentación de soluciones, seguida de procesos de evaluación formativa y sumativa, consolida los aprendizajes y promueve la reflexión metacognitiva sobre las estrategias empleadas.

2.5. Tecnologías y fabricantes líderes en ciberseguridad

El ecosistema de la ciberseguridad está compuesto por diversas tecnologías y fabricantes que ofrecen soluciones avanzadas para la protección de infraestructuras críticas. Empresas como Palo Alto Networks, Fortinet, Check Point, Huawei, Juniper Networks e IBM Security. Han desarrollado plataformas de firewall, sistemas de prevención de intrusos (IPS), soluciones de autentificación y servicios de gestión de amenazas que aportan significativamente al fortalecimiento de la seguridad digital en entornos empresariales.

A pesar de la diversidad de alternativas disponibles, Cisco Systems se ha consolidado como la empresa líder mundial en infraestructura de redes y seguridad, con una participación superior en las redes empresariales a nivel mundial (Saito, 2021). La

compañía ha integrado soluciones de hardware y software en un mismo ecosistema, incluyendo routers, switches, firewalls, VPNs y plataformas de administración centralizada, lo que permite ofrecer una visión integral de la seguridad de las redes.

Un factor diferenciador de Cisco frente a otros fabricantes es la creación de Cisco Networking Academy (NetAcad), programa educativo presente en más de 190 países que ha formado a más de 20 millones de estudiantes desde 1997 (Rodríguez-Rivas et al., 2020). Esto posiciona a Cisco no solo como proveedor tecnológico, sino también como referente en formación académica y certificación profesional en ciberseguridad.

Capítulo 3

Metodología

El proyecto se desarrolló bajo una metodología de investigación aplicada, orientada al diseño y consolidación de un recurso didáctico para el fortalecimiento de competencias en redes y ciberseguridad mediante tecnologías Cisco. La metodología se centró en la planificación y desarrollo de guías prácticas de laboratorio, apoyadas en el uso de herramientas de simulación y equipos físicos disponibles, con el fin de asegurar su correcta implementación en un entorno académico.

La metodología se estructuró en cuatro fases, definidas en coherencia con los objetivos del proyecto. Estas fases permitieron:

(I) Asegurar la disponibilidad y operatividad del laboratorio.

(II) Identificar y adaptar contenidos del currículo Cisco al contexto institucional.

(III) Diseñar e implementar guías prácticas bajo el enfoque de Aprendizaje Basado en Problemas (ABP) como estrategia didáctica.

(IV) Realizar la revisión y ajuste del material elaborado, con el propósito de garantizar su claridad, coherencia y adecuación a las condiciones del laboratorio y al nivel de formación de los estudiantes.

FASE	¿POR QUÉ?	¿QUÉ LLEVA?	RECURSOS	ENTREGABLES
1 **Validación**	Garantizar que la infraestructura de red funcione correctamente para soportar las prácticas de laboratorio.	— Inventario técnico — Inspección física — Pruebas de conectividad — Diagnóstico de problemas — Documentación técnica	— Routers Cisco — Switches — Cables de consola — Software IOS XE — Herramientas diagnóstico	— Manual ISR 1100X-4G — Manual Cisco 1841 — Equipos validados — Reporte técnico
2 **Identificación**	Alinear contenidos teóricos con capacidades prácticas y recursos disponibles en el laboratorio.	— Análisis documental — Identificación de dominios — Selección temática — Mapeo de competencias — Alineación con ABP	— Currículo Cisco — Asignatura Transmisión — Recursos laboratorio — Modelo USTA	— GA-1: Fund. Redes — GA-2: Fund. Cibersec. — Matriz de contenidos — Secuencia aprendizaje
3 **Diseño**	Materializar el proceso educativo en recursos didácticos prácticos que faciliten la aplicación del aprendizaje.	— Diseño estructura ABP — Redacción paso a paso — Ejercicios independientes — Herramienta web — Topologías diseñadas	— Infra. validada (F1) — Contenidos (F2) — Cisco Packet Tracer — Equipos físicos — Software diseño	— 7 Guías laboratorio — Herramienta web — Ejercicios prácticos — Topologías completas
4 **Validación**	Asegurar que el material sea técnicamente correcto, pedagógicamente coherente y evaluable según ABP.	— Ejecución de guías — Verificación replicabilidad — Diseño de rúbricas — Identificación mejoras — Ajustes finales	— Todas las guías — Criterios técnicos — Equipos funcionando — Software simulación	— 4 Rúbricas evaluación — Guías finales — Validación documentada — Producto final

Figura 3.0.1: Matriz metodológica

Fuente: Autor

La construcción y presentación de una matriz metodológica responde a la necesidad de estructurar de manera ordenada la relación entre los objetivos del proyecto, las fases de desarrollo, las actividades ejecutadas y los productos obtenidos. La matriz cumple una función organizativa y analítica, ya que permite visualizar de forma integrada cómo cada objetivo específico se desarrolla a través de acciones concretas y verificables dentro del proceso investigativo.

En proyectos de carácter aplicado, especialmente aquellos orientados al diseño de recursos didácticos y tecnológicos, la matriz metodológica facilita la trazabilidad del proceso, asegurando coherencia entre la formulación del problema, los objetivos planteados y los resultados alcanzados. De esta manera, se evita la dispersión metodológica y se garantiza que cada actividad desarrollada contribuya directamente al cumplimiento del objetivo general.

La matriz metodológica actúa como un mecanismo de control y seguimiento del proyecto, permitiendo verificar que las etapas propuestas fueron ejecutadas de manera ordenada y que los entregables —manuales, guías académicas, guías de laboratorio y rúbricas— corresponden directamente con las acciones definidas en cada fase. Esto refuerza la validez interna del proceso metodológico y demuestra la coherencia entre planificación, ejecución y resultados obtenidos.

3.1. Fase 1: Validación y verificación de funcionamiento de equipos

El propósito de esta fase fue confirmar el estado de operación de los dispositivos de red disponibles en el laboratorio de telecomunicaciones y garantizar condiciones mínimas para la ejecución de prácticas. Se realizó un inventario técnico del equipamiento existente y de los equipos incorporados al laboratorio, incluyendo routers Cisco serie 1841, Cisco ISR 1100X-4G y Cisco 2800 series, así como switches Catalyst 2960, 3560 v2, 3750 y Catalyst 1300 series. A partir del inventario, se llevaron a cabo actividades de revisión y verificación de funcionamiento, que incluyeron inspección física, encendido de los equipos, acceso por consola o mediante administración remota, verificación de la versión de IOS, comprobación del estado de las interfaces y revisión de los parámetros básicos de arranque y configuración.

La verificación funcional se ejecutó mediante pruebas controladas de conectividad y operación de capa 2 y capa 3, según el rol del equipo en el laboratorio. En switches se comprobaron, entre otros, el estado de puertos, la creación de VLAN, el enlace troncal y la conmutación básica. En routers se validaron aspectos como direccionamiento, enrutamiento en escenarios de referencia y acceso administrativo.

3.2. Fase 2: Identificación y adaptación de contenidos

En esta fase se realizó un análisis documental del currículo de Cisco Networking Academy asociado a fundamentos de ciberseguridad y de los contenidos de redes requeridos para la implementación de configuraciones en plataformas Cisco. El análisis permitió definir una secuencia de aprendizaje y un conjunto de resultados esperados, integrando conceptos como amenazas y vulnerabilidades, control de acceso, segmentación y protección de redes, fundamentos de cifrado y manejo básico de incidentes. De manera complementaria se incorporaron prerrequisitos de redes (direccionamiento IP, subneteo, enrutamiento y servicios esenciales) para asegurar comprensión técnica de las configuraciones de seguridad.

La adaptación de los contenidos al contexto institucional se realizó a partir del análisis de la relación entre las competencias a desarrollar y los recursos disponibles en el laboratorio. Para cada tema se estableció el tipo de práctica a implementar (simulación o trabajo con equipos físicos), así como los requerimientos de topología y los criterios básicos de verificación, tales como comandos de comprobación y pruebas de conectividad o de control de tráfico. De esta manera, se aseguró que los escenarios propuestos fueran viables desde el punto de vista académico y acordes con el nivel de formación, evitando el uso de funcionalidades no disponibles en el equipamiento existente o no pertinentes para el propósito formativo.

3.3. Fase 3: Diseño e implementación de guías prácticas bajo el enfoque ABP

La fase de diseño se orientó a la elaboración de guías prácticas bajo el enfoque de Aprendizaje Basado en Problemas (ABP), con énfasis en la aplicación de conceptos de ciberseguridad sobre infraestructuras de red basadas en tecnologías Cisco. Las guías se formularon como recursos de apoyo al aprendizaje práctico, integrando componentes

teóricos y actividades de configuración que permitieran al estudiante comprender la relación entre redes y seguridad.

Cada guía incorporó contenidos teóricos de redes y ciberseguridad, junto con actividades de aprendizaje dirigidas a la configuración paso a paso de dispositivos Cisco. Estas actividades se apoyaron en escenarios de simulación y en equipos físicos disponibles, facilitando la comprensión del funcionamiento y comportamiento de los dispositivos en contextos controlados.

Estructura de las guías de laboratorio

Se definió una estructura base común a todas las guías de laboratorio, garantizando coherencia pedagógica y uniformidad en la experiencia del estudiante. Esta estructura responde al ABP al ubicar al estudiante frente a un escenario problemático real desde el inicio, guiando progresivamente la construcción del conocimiento a través de la acción técnica verificable. Los componentes de cada guía son:

1. **Encabezado institucional.** Asignatura, número de guía y duración estimada.
2. **Objetivos de aprendizaje.** Competencias técnicas medibles formuladas en términos de desempeño observable.
3. **Marco teórico de referencia.** Síntesis de los fundamentos necesarios para comprender el escenario y los comandos.
4. **Escenario problemático (ABP).** Situación técnica realista con restricciones de diseño, requerimientos de seguridad y criterios de verificación explícitos.
5. **Desarrollo por partes.** Configuración guiada paso a paso con explicación de cada comando y verificación intermedia.
6. **Ejercicios independientes.** Ejercicio sin guía paso a paso para aplicar los conocimientos en un escenario distinto.

3.4. Fase 4: Revisión de la calidad del material didáctico y construcción de rúbricas

La cuarta fase se orientó a la revisión de la calidad del material didáctico desarrollado, con el propósito de garantizar que las guías fueran técnicamente correctas, pedagógicamente coherentes y funcionales dentro de los recursos disponibles. Este proceso se llevó a cabo mediante una revisión interna exhaustiva, en la que el autor ejecutó paso a paso cada una de las guías, tanto en el entorno de simulación (Cisco Packet Tracer) como en los equipos físicos del laboratorio. El objetivo fue detectar y corregir posibles errores, ambigüedades o inconsistencias en los procedimientos descritos, asegurando que las instrucciones fueran claras, completas y replicables.

Como parte de esta fase, se construyeron rúbricas de evaluación que cumplen una doble finalidad: por un lado, sirvieron como instrumento para contrastar la calidad de las guías durante el proceso de revisión, permitiendo verificar que cada una contenía los elementos necesarios para una valoración objetiva; por otro lado, están concebidas para su aplicación futura en el laboratorio, proporcionando criterios claros y uniformes para que el docente pueda evaluar el desempeño de los estudiantes en coherencia con los objetivos de aprendizaje y el enfoque de Aprendizaje Basado en Problemas (ABP).

Capítulo 4

Resultados

4.1. Resultados Fase 1

La Fase inicial del proyecto se orientó a la verificación del estado operativo de los equipos de red disponibles en el laboratorio de telecomunicaciones. Esta etapa permitió identificar las condiciones de funcionamiento de los dispositivos, detectar configuraciones incorrectas y resolver problemas técnicos que impedían su correcta operación, garantizando así la disponibilidad de la infraestructura necesaria para el desarrollo de las prácticas de laboratorio.

Durante el proceso de revisión se encontró que los switches de las series Catalyst 2960, 3560 v2, 3750 y 1300 se encontraban en condiciones operativas adecuadas, sin presentar inconvenientes que afectaran su funcionamiento básico. Por el contrario, los routers requirieron intervención técnica especializada para resolver problemas de configuración y de software que limitaban su uso en el contexto académico propuesto.

Routers Cisco ISR 1100X-4G

Los routers de la serie ISR 1100X-4G, equipos de reciente adquisición, presentaron dificultades de acceso y operación al momento de iniciar sesión en la interfaz de línea de comandos (CLI). Al conectarse mediante consola, el sistema solicitaba el ingreso de

credenciales de usuario y contraseña, y posteriormente requería el cambio obligatorio de la contraseña administrativa. Sin embargo, una vez completado este procedimiento, el equipo generaba errores recurrentes que impedían el acceso al modo de configuración mediante el comando ***configure terminal***, lo cual imposibilitaba la ejecución de prácticas de laboratorio.

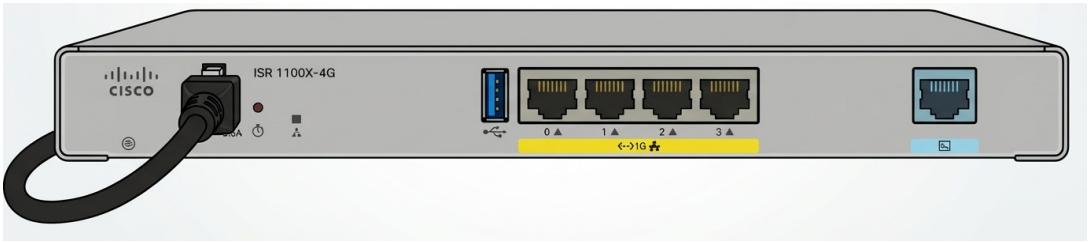

Figura 4.1.1: Router Cisco Serie ISR 1100X-4G

Fuente: Autor

El análisis técnico del problema, realizado en coordinación con el equipo de soporte técnico de la empresa proveedora de los equipos, permitió identificar que la causa raíz del inconveniente se debía a que los routers estaban configurados de fábrica en modo Controller-Managed, diseñado para operar bajo la arquitectura Cisco SD-WAN. Este modo de operación restringe el acceso directo a ciertos comandos de configuración en IOS XE, dado que el dispositivo espera ser gestionado de forma centralizada por un controlador de red, limitando así la configuración manual desde la CLI.

Para resolver esta situación, se procedió a cambiar el modo de operación del equipo de Controller-Managed a modo autónomo (IOS XE tradicional), proceso que requirió intervención a nivel de ROMMON (ROM Monitor), el entorno de recuperación de bajo nivel del sistema operativo Cisco IOS. El procedimiento técnico consistió en reiniciar el router y acceder al prompt de ROMMON mediante la combinación de teclas adecuada durante el arranque del dispositivo. Una vez en el entorno ROMMON, se ejecutaron los siguientes comandos para modificar la variable de configuración que define el modo de operación del equipo:

```
set DEVICE_MANAGED_MODE=autonomous
sync
reset
```

Routers Cisco Serie 1841

Los routers de la serie 1841, equipos con mayor antigüedad en el inventario del laboratorio, presentaron problemas relacionados con la memoria de almacenamiento no volátil (Compact Flash). El diagnóstico técnico reveló que las tarjetas Compact Flash contenían imágenes de IOS incorrectas o dañadas, lo cual afectaba la estabilidad del sistema operativo. Adicionalmente, se detectó que los dispositivos no permitían guardar las configuraciones realizadas en la sesión activa (running-config) hacia la configuración de inicio (startup-config) mediante los comandos ***copy running-config startup-config*** o ***write memory***, lo que impedía la persistencia de las configuraciones tras el reinicio del equipo.

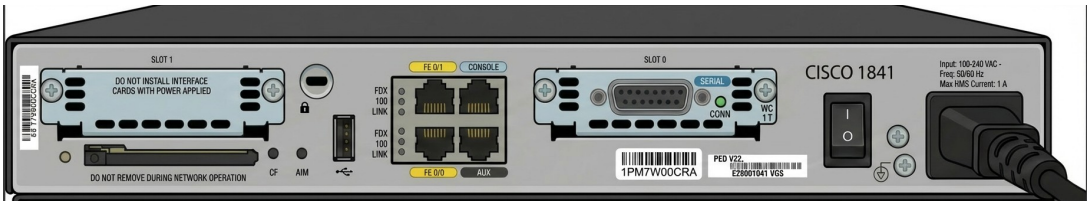

Figura 4.1.2: Ilustración Router Cisco Serie 1841

Fuente: Autor

El análisis del registro de configuración reveló que los routers estaban configurados con el valor 0x2142 en el Configuration Register, el cual indica al sistema que debe ignorar el archivo de configuración de inicio (startup-config) almacenado en la NVRAM durante el proceso de arranque. Esta configuración es comúnmente utilizada para procedimientos de recuperación de contraseñas, pero resulta inadecuada para operación normal del equipo, ya que cada vez que el router se reinicia, carga únicamente la configuración básica de fábrica, perdiendo todas las modificaciones realizadas

previamente.

Para corregir esta situación, se procedió a modificar el valor del Configuration Register de 0x2142 a 0x2102, que corresponde al modo de arranque estándar del dispositivo. Este cambio se realizó accediendo al modo de configuración global mediante el comando configure terminal y ejecutando la instrucción config-register 0x2102, seguida de la confirmación mediante write memory y reload para reiniciar el equipo con la nueva configuración del registro.

El cambio al valor 0x2102 en el Configuration Register garantiza que el router opere de forma correcta bajo las siguientes condiciones: carga del sistema operativo IOS desde la memoria Flash, lectura y aplicación del archivo startup-config almacenado en la NVRAM al momento del arranque, aplicación completa de todas las configuraciones guardadas (direccionamiento IP, enrutamiento, contraseñas, listas de control de acceso, entre otras), y utilización de la velocidad estándar de la consola (9600 bps). Tras implementar esta corrección, los routers de la serie 1841 quedaron completamente funcionales, permitiendo la persistencia de las configuraciones y su utilización efectiva en las prácticas de laboratorio.

Documentación del proceso

Como parte de los entregables de esta fase, se desarrolló documentación técnica detallada en forma de manuales de funcionamiento, dirigidos tanto a docentes como a estudiantes, con el propósito de facilitar futuras intervenciones técnicas sobre los equipos y servir como referencia para la comprensión de los procedimientos de solución de problemas comunes en los dispositivos. Estos manuales se incluyen en el **Anexo A** del presente documento y abarcan aspectos como el acceso inicial a los equipos, la identificación de modos de operación, la modificación de parámetros de arranque y la verificación del estado operativo de los dispositivos.

La resolución exitosa de los problemas técnicos identificados en esta fase garantizó la disponibilidad de la infraestructura de red necesaria para el desarrollo de las guías prácticas de ciberseguridad, asegurando que tanto los equipos nuevos como los antiguos pudieran utilizarse de manera confiable en el contexto académico del laboratorio de telecomunicaciones.

4.2. Resultados Fase 2

La segunda fase del proyecto se orientó a la identificación, análisis y adaptación de los contenidos necesarios para la implementación de prácticas de ciberseguridad en el laboratorio de telecomunicaciones. Este proceso requirió un estudio detallado tanto de los fundamentos de transmisión de datos como de los contenidos específicos del programa Cisco Networking Academy en ciberseguridad.

Análisis curricular y selección de contenidos

Se realizó un análisis documental del currículo Cisco Networking Academy, específicamente del curso Cisco Cybersecurity Essentials, identificando los dominios críticos de conocimiento: seguridad de endpoints, defensa de redes y gestión de amenazas cibernéticas. El dominio de defensa de redes resultó particularmente relevante, dado que aborda la protección de la infraestructura de comunicaciones mediante tecnologías y protocolos de seguridad implementables en los dispositivos Cisco disponibles en el laboratorio.

El análisis permitió identificar dos conjuntos de contenidos fundamentales. Por un lado, los contenidos de redes de datos que constituyen prerrequisitos técnicos indispensables, incluyendo clasificación de redes, modelos de referencia OSI y TCP/IP, protocolos de comunicación, sistemas de numeración, direccionamiento IPv4 e IPv6, protocolo Ethernet, subnetting, VLSM y enrutamiento IP. Por otro lado, los contenidos específicos de ciberseguridad, abarcando los principios de seguridad de la información

(tríada CIA), listas de control de acceso (ACL), redes privadas virtuales (VPN) IPsec y firewalls Cisco ASA. Estos contenidos se describen en detalle en el Capítulo 3 del presente documento.

Adaptación al contexto institucional

La adaptación de los contenidos se realizó evaluando la correspondencia entre las competencias a desarrollar y los recursos disponibles en el laboratorio. Para cada tema se definió el tipo de práctica a implementar (simulación mediante Cisco Packet Tracer o trabajo con equipos físicos), los requerimientos de topología y los criterios de verificación, asegurando que los escenarios propuestos fueran viables y acordes con el nivel de formación de los estudiantes. Se estableció una secuencia de aprendizaje progresiva que parte de los fundamentos de redes hacia la implementación de configuraciones de seguridad de complejidad creciente.

Guías de aprendizaje desarrolladas

Como resultado tangible de esta fase, se desarrollaron dos guías de aprendizaje que constituyen el material didáctico fundamental para proporcionar el marco teórico y conceptual necesario antes de la ejecución de las prácticas de laboratorio.

La primera guía, denominada "Fundamentos de Redes de Datos", consolida los contenidos de redes identificados y analizados, integrándolos en un documento estructurado que sirve como base conceptual y técnica para las prácticas de seguridad posteriores. La guía organiza de manera coherente los conocimientos fundamentales requeridos para la comprensión de infraestructuras de red y su relación con los mecanismos de protección implementados en dispositivos Cisco.

La segunda guía, "Principios de Ciberseguridad en Infraestructuras de Red", presenta los conceptos fundamentales de ciberseguridad aplicados al contexto de las redes de datos. Introduce los protocolos y tecnologías de seguridad que constituyen el

núcleo de las prácticas de laboratorio, proporcionando una descripción conceptual de su funcionamiento antes de abordar su configuración técnica.

Las guías de aprendizaje desarrolladas en esta fase se incluyen en el Anexo B del presente documento y constituyen material de referencia fundamental que los estudiantes deben estudiar previamente a la ejecución de las prácticas de laboratorio.

4.3. Resultados Fase 3

La tercera fase tuvo como propósito la construcción del material didáctico que constituye el núcleo del presente trabajo. A partir de los contenidos identificados en la Fase 2 y de la infraestructura verificada en la Fase 1, se elaboraron once documentos estructurados bajo el enfoque del Aprendizaje Basado en Problemas (ABP): dos manuales de uso y solución de problemas de los equipos del laboratorio, dos guías de aprendizaje teórico y siete guías de laboratorio que articulan la formación en redes y ciberseguridad con el uso de Cisco Packet Tracer y equipos físicos del Laboratorio de Telecomunicaciones.

Organización general del material didáctico

El conjunto de materiales se organiza en tres categorías de función pedagógica complementaria:

Manuales de equipo

Documentos técnicos de referencia que describen el uso correcto de los equipos físicos del laboratorio (Cisco ISR 1100X-4G y Cisco 1841/2800), incluyendo procedimientos de acceso inicial, configuración básica y resolución de problemas frecuentes. Constituyen material de consulta permanente tanto para docentes como para estudiantes durante las sesiones de laboratorio.

Guías de aprendizaje

Documentos teóricos para el estudio autónomo previo a cada sesión de laboratorio. Presentan fundamentos conceptuales, modelos de referencia y principios de operación de los protocolos trabajados, garantizando que el estudiante llegue a la práctica con el marco teórico necesario para comprender el propósito de cada configuración.

Guías de laboratorio

Documentos prácticos que guían la ejecución de actividades de configuración. Para los temas de enrutamiento, ACL y VPN se diseñaron dos guías por temática: una para Cisco Packet Tracer y otra para los equipos físicos del laboratorio. Para el tema de firewall, la guía se limitó al entorno de simulación por razones de infraestructura que se detallan más adelante.

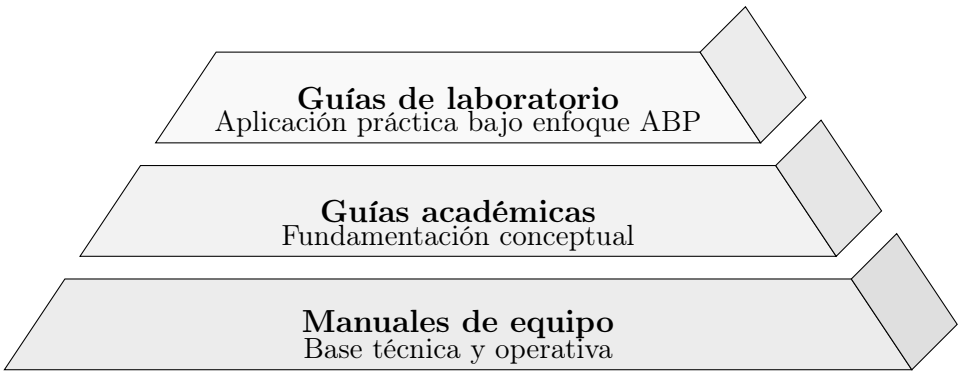

Figura 4.3.1: Estructura piramidal progresiva del material didáctico

La organización del material didáctico responde a una estructura piramidal que refleja la progresión formativa planteada en el proyecto. En la base se sitúan los manuales de equipo, que garantizan la operatividad técnica del laboratorio; en el nivel intermedio, las guías de aprendizaje consolidan los fundamentos conceptuales necesarios; y en la cúspide, las guías de laboratorio materializan la aplicación práctica bajo el enfoque de Aprendizaje Basado en Problemas (ABP). Esta disposición evidencia que los entregables fueron diseñados de manera articulada y secuencial.

Tabla 4.3.1: Relación completa de materiales didácticos diseñados (Fase 3)

Código	Título del documento	Modalidad	Alcance
	Manuales de equipo (Anexo A)		
MA-1	Manual de uso — Router Cisco ISR 1100X-4G	Referencia técnica	Docentes y estudiantes
MA-2	Manual de uso — Routers Cisco 1841	Referencia técnica	Docentes y estudiantes
	Guías Académicas (Anexo B)		
GA-1	Fundamentos de redes de datos	Estudio autónomo	Estudiantes
GA-2	Fundamentos de ciberseguridad	Estudio autónomo	Estudiantes
	Guías de laboratorio (Anexo C)		
GL-1	Configuración de routers Cisco — Cisco Packet Tracer	Simulación	Estudiantes
GL-2	Configuración de routers Cisco — laboratorio físico	Equipo físico	Estudiantes
GL-3	Configuración de protocolo ACL estándar y extendido en Cisco Packet Tracer	Simulación	Estudiantes
GL-4	Configuración de protocolo ACL estándar y extendido en laboratorio físico	Equipo físico	Estudiantes
GL-5	Configuración de protocolo VPN IPsec en Cisco Packet Tracer	Simulación	Estudiantes
GL-6	Configuración de protocolo VPN IPsec en laboratorio físico	Equipo físico	Estudiantes
GL-7	Configuración de firewall Cisco ASA en Cisco Packet Tracer	Simulación	Estudiantes
	Total: 11 documentos	**2 manuales + 9 guías**	

4.3.1. Manuales de uso y solución de problemas

Como primer resultado tangible de la Fase 3, y en estrecha articulación con la documentación del proceso de validación de equipos realizada en la Fase 1, se elaboraron dos manuales técnicos dirigidos a docentes y estudiantes del Laboratorio de Telecomunicaciones. Estos manuales responden a la necesidad identificada durante la verificación de equipos: la ausencia de documentación en español, específica para el contexto académico y adaptada al nivel de los estudiantes de pregrado, que orientara el acceso inicial, la configuración básica y la resolución de los problemas técnicos más frecuentes en cada equipo. Ambos manuales se incluyen como Anexo A del presente documento.

MA-1: Manual de uso del router Cisco ISR 1100X-4G

El primer manual aborda el uso del router Cisco ISR 1100X-4G, equipo de reciente adquisición en el laboratorio. Su diseño partió de los problemas técnicos identificados y resueltos durante la Fase 1, documentando los procedimientos que permiten utilizar estos equipos en el contexto académico, dada su configuración de fábrica orientada a entornos SD-WAN y no a laboratorio.

El manual está organizado en las siguientes secciones:

1. **Descripción del equipo.** Identificación de las interfaces físicas, puertos de consola, LED de estado y módulos disponibles en el Cisco ISR 1100X-4G.

2. **Acceso inicial por consola.** Procedimiento de conexión mediante cable de consola RJ-45 a USB, y secuencia de inicio de sesión.

3. **Cambio de modo de operación a autónomo.** Procedimiento completo para modificar el modo de operación de *controller-managed* (SD-WAN) a IOS XE autónomo mediante el entorno ROMMON, incluyendo los comandos: `set DEVICE_MANAGED_MODE=autonomous`, `sync` y `reset`. Este procedimiento es indispensable para el uso del equipo en prácticas de laboratorio.

4. **Configuración básica del equipo.** Secuencia de comandos para asignar nombre de host, configurar contraseñas de acceso, definir el mensaje de inicio y guardar la configuración inicial.

5. **Verificación del estado del equipo.** Conjunto de comandos *show* para verificar la versión de IOS XE, el estado de las interfaces, la configuración en ejecución y los parámetros de arranque del sistema.

MA-2: Manual de uso de los routers Cisco 1841

El segundo manual cubre los routers Cisco 1841, equipos de mayor antigüedad en el inventario del laboratorio. Su contenido se construyó a partir de los problemas técnicos detectados y resueltos en la Fase 1, especialmente los relacionados con la memoria de almacenamiento CompactFlash y el valor del *configuration register*, documentando los procedimientos para dejar estos equipos en condiciones operativas correctas y para su uso cotidiano en prácticas de laboratorio.

El manual está organizado en las siguientes secciones:

1. **Descripción del equipo.** Identificación de las interfaces físicas (FastEthernet y Serial), ranura CompactFlash, puertos de consola y auxiliar, LED indicadores y módulos WIC disponibles (incluyendo el WIC-1T necesario para las prácticas de enrutamiento).

2. **Instalación del módulo WIC-1T.** Procedimiento de apagado previo, inserción física del módulo en la ranura WIC del router y verificación de reconocimiento mediante *show version*, incluyendo la advertencia de que la inserción en caliente puede dañar el equipo.

3. **Acceso inicial por consola.** Conexión mediante cable de consola RJ-45 a DB-9 (o adaptador USB), parámetros del terminal y secuencia de inicio.

4. **Verificación y corrección del *configuration register*.** Procedimiento para verificar el valor del registro mediante *show version* (última línea de la salida),

corrección del valor a `0x2102` mediante `config-register 0x2102` en modo de configuración global y verificación posterior al reinicio. Se explica por qué un valor `0x2142` provoca pérdida de configuración en cada reinicio y cuándo se utiliza este valor (recuperación de contraseñas).

5. **Configuración básica del equipo.** Comandos para nombre de host, contraseñas, guardado de configuración (`copy running-config startup-config` y `write memory`) y verificación.

6. **Solución de problemas frecuentes.** Procedimientos para los inconvenientes más comunes, incluyendo: pérdida de configuración al reiniciar (*configuration register* incorrecto), imagen de IOS dañada o incorrecta en CompactFlash, interfaces que no encienden (*down/down*), fallo al guardar la configuración y errores en puertos seriales por ausencia o mal asentamiento del módulo WIC-1T.

Tabla 4.3.2: Solución de problemas frecuentes: routers Cisco 1841

Falla	**Causa probable**	**Procedimiento**
La configuración se pierde al reiniciar	*Configuration register* en `0x2142`	Ejecutar `config-register 0x2102` y luego `write memory`.
No acepta `copy run start`	IOS dañado o CompactFlash defectuosa	Reemplazar la imagen de IOS desde TFTP o usar una nueva CompactFlash.
Las interfaces seriales no aparecen	Módulo WIC-1T no instalado o mal asentado	Apagar el equipo, retirar y reinsertar el WIC-1T, y verificar con *show version*.
Interfaz en estado *down/down*	Falta `no shutdown` o cable desconectado	Verificar cableado y ejecutar `no shutdown`.
No permite acceso por contraseña olvidada	Contraseña olvidada	Aplicar el procedimiento de recuperación desde ROMMON.

4.3.2. Guías Academicas

Con el fin de garantizar coherencia curricular y pertinencia académica, la estructura de las guías académicas se diseñó tomando como referencia directa el syllabus oficial del espacio académico Transmisión de Datos. La organización temática respeta la secuencia, los prerrequisitos conceptuales y las competencias definidas en dicho programa, realizando únicamente una separación estratégica de contenidos para facilitar el aprendizaje progresivo y el estudio autónomo previo a las prácticas de laboratorio.

Esta alineación asegura que el material desarrollado no constituye un contenido paralelo, sino una herramienta de profundización y estructuración pedagógica del plan de estudios institucional.

Tabla 4.3.3: Estructura interna de la Guía Académica 1 en alineación con el syllabus

Unidad	**Unidad del syllabus**	**Propósito**
1	Unidad Temática 1	Marco conceptual general de redes y modelos de referencia.
2	Unidad Temática 1	Profundización en capa de enlace y segmentación básica.
3–5	Unidad Temática 2	Direccionamiento IP, CIDR y subdivisión de redes (Subnetting y VLSM).
6	Unidad Temática 3	Introducción al enrutamiento como base para laboratorio.

La versión completa de la estructura y el desarrollo detallado de cada unidad se encuentra en el Anexo B – Fundamentos de Redes, donde se presenta el contenido organizado conforme a esta alineación curricular.

GA-1: Fundamentos de redes de datos

La primera guía de aprendizaje consolida los contenidos teóricos de redes identificados en la Fase 2, organizados en un documento estructurado que sirve como base conceptual para todas las prácticas de laboratorio. Cubre clasificación de redes (LAN, WAN, MAN

y PAN), modelos OSI y TCP/IP, sistema binario y hexadecimal, direccionamiento IPv4 e IPv6, protocolo Ethernet, subneteo y VLSM, y enrutamiento IP estático. El documento permite al estudiante consultar conceptos concretos de forma rápida durante la práctica, sin necesidad de recurrir a fuentes externas.

GA-2: Fundamentos de ciberseguridad

La segunda guía presenta los fundamentos de ciberseguridad aplicados al contexto de redes de datos: la tríada CIA, tipos de amenazas y vulnerabilidades, y el modelo de defensa en profundidad. Dedica secciones específicas a los principios de funcionamiento de las tecnologías trabajadas en las guías GL-3 a GL-7: listas de control de acceso (ACL), redes privadas virtuales (VPN) con IPsec y firewalls como dispositivos de seguridad perimetral. Esta guía es el material de estudio previo obligatorio antes de cualquier práctica de ciberseguridad.

4.3.3. Guías de laboratorio

Enrutamiento estático (GL-1 y GL-2)

El bloque de enrutamiento estático constituye el punto de entrada a la configuración de equipos Cisco. Su diseño partió del reconocimiento de que los estudiantes requieren consolidar competencias en el manejo de la CLI de Cisco IOS y, de forma previa e indispensable, en el diseño de esquemas de direccionamiento IP mediante técnicas de subnetting y VLSM. Como prerrequisito esencial para las prácticas de seguridad posteriores, estas guías enfatizan la construcción metódica de topologías de red y la aplicación sistemática de cálculos de subneteo.

Herramienta web interactiva para diseño de topologías y subnetting

Como recurso didáctico complementario a las guías GL-1 y GL-2, se desarrolló una herramienta web interactiva (implementada en HTML) denominada *Editor de Topologías y Subnetting*. Esta permite a los estudiantes diseñar visualmente la topología de red, calcular esquemas de direccionamiento VLSM y documentar la asignación de direcciones

IP antes de proceder con la configuración en Cisco Packet Tracer o en los equipos físicos del laboratorio.

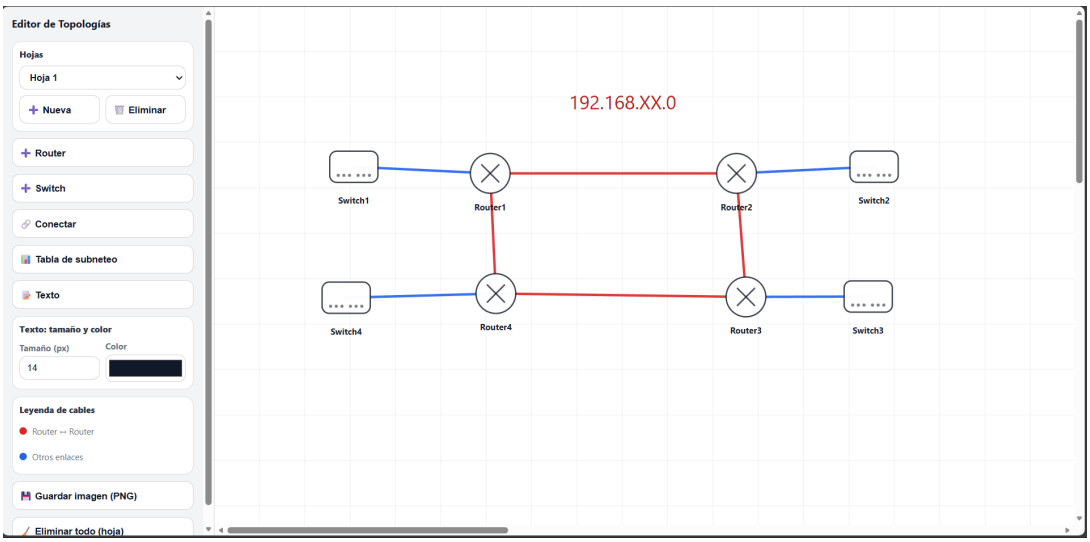

Figura 4.3.2: Interfaz web del *Editor de Topologías y Subnetting*
Fuente: Autor

La herramienta opera enteramente en el navegador, sin requerir instalación de software adicional, y proporciona las siguientes funcionalidades:

1. **Construcción visual de topologías.** Permite arrastrar y ubicar dispositivos (routers y switches) sobre un lienzo de trabajo, y conectarlos mediante enlaces tipo Ethernet o Serial, replicando visualmente el proceso que posteriormente se realizará en Cisco Packet Tracer.

2. **Documentación de direccionamiento IP.** Cada nodo puede ser etiquetado con su nombre, dirección IP y máscara de subred mediante texto editable directamente sobre el diagrama, facilitando la organización visual del esquema de direccionamiento.

3. **Widgets de cálculo de subnetting.** La herramienta incluye elementos gráficos específicos para documentar el diseño VLSM: el estudiante puede crear *widgets de subred* que muestran la red base, la máscara, el rango de direcciones utilizable y el propósito de cada subred, consolidando toda la información del esquema de direccionamiento en un solo diagrama interactivo.

4. **Notas y anotaciones de texto libre.** Permite incluir cuadros de texto en cualquier posición del lienzo para documentar criterios de diseño, restricciones del escenario o secuencia de pasos de configuración, apoyando la organización metódica del trabajo previo a la práctica.

5. **Exportación de diseños.** El diseño completo puede ser guardado localmente (formato PNG) para su posterior recuperación, permitiendo al estudiante trabajar de forma iterativa sobre el esquema de direccionamiento hasta consolidarlo antes de proceder con la configuración efectiva en el laboratorio.

Sugerencia de uso (propósito pedagógico). El uso de esta herramienta no es obligatorio; sin embargo, se recomienda para estudiantes que presentan dificultades con el cálculo de subredes o con la organización visual de topologías complejas. Al realizar el proceso de diseño y cálculo del esquema de direccionamiento fuera del entorno de Packet Tracer o del equipo físico, el estudiante puede concentrarse en comprender la lógica del subnetting VLSM sin las distracciones de la interfaz de simulación, validar su diseño con el docente antes de iniciar la configuración y reducir significativamente los errores de direccionamiento, que constituyen una de las causas más frecuentes de fallo en las prácticas de enrutamiento estático. La herramienta facilita la evaluación formativa del proceso de diseño por parte del docente, quien puede revisar el esquema propuesto por el estudiante antes de que este invierta tiempo en su implementación.

GL-1: Enrutamiento estático en Cisco Packet Tracer

Esta guía introduce al estudiante en el entorno de simulación y en el proceso completo de configuración de una topología multi-router. El simulador permite cometer errores e identificarlos sin riesgo sobre los equipos físicos, construyendo familiaridad con la CLI de Cisco IOS antes del trabajo con hardware real. Incluye dos ejercicios independientes.

La guía se estructuró en tres partes:

1. **Construcción y cableado en Packet Tracer,** incluyendo la instalación del módulo WIC-1T.

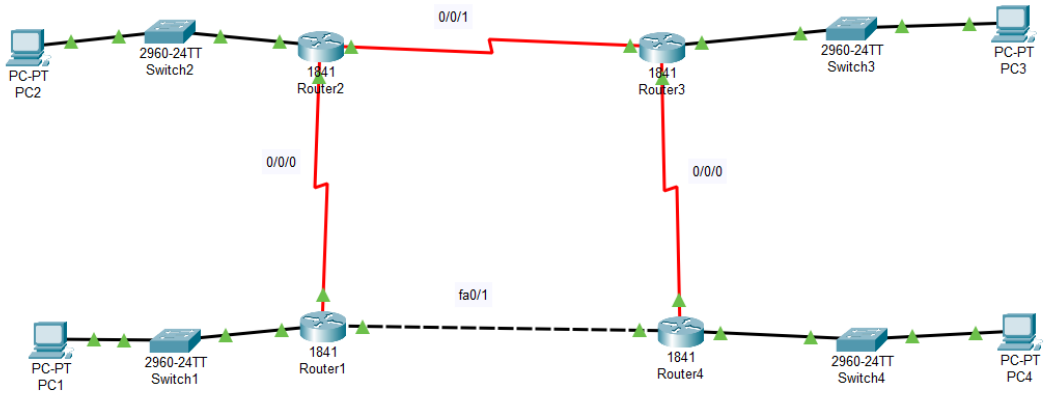

Figura 4.3.3: Topología Cisco Packet Tracer
Fuente: Autor

2. **Configuración de interfaces FastEthernet y Serial,** con direcciones IP, activación y establecimiento de *clock rate*.

3. **Implementación y verificación de rutas estáticas,** validación mediante los comandos *show ip route* y *ping*.

GL-2: Enrutamiento estático en laboratorio físico

Esta guía adaptó el escenario de GL-1 al trabajo con routers del laboratorio (Cisco 1841, 2800 y ISR 1100X), pero los procedimientos incorporan las particularidades del hardware real: conexión por cable de consola, identificación física de los puertos seriales, interpretación de mensajes del sistema ausentes en la simulación y verificación del registro de configuración (*config-register* `0x2102`) como condición para que la configuración persista tras el reinicio. La guía demostró las diferencias entre simulación y equipo físico, preparando al estudiante para un entorno profesional.

Figura 4.3.4: Routers físicos y cableado de laboratorio para la práctica de enrutamiento estático

Fuente: Autor

Guías de laboratorio: listas de control de acceso (GL-3 y GL-4)

El segundo bloque de prácticas introdujo a los estudiantes en la implementación de políticas de seguridad sobre la red ya configurada en las prácticas anteriores. El objetivo central fue que los estudiantes aprendieran a controlar qué dispositivos pueden comunicarse con otros y qué servicios pueden utilizar, mediante la configuración de listas de controlde acceso (ACL) en los routers Cisco.

GL-3: ACLs estándar y extendidas en Cisco Packet Tracer

La guía de simulación permitió a los estudiantes experimentar con las Listas de Control de Acceso (ACL) sin riesgo de afectar equipos reales. Partiendo de la topología de cuatro routers utilizada en prácticas anteriores, se añadió un servidor en una de las redes y se configuró paso a paso cómo:

- Crear una ACL estándar con reglas de tipo permitir (`permit`) y denegar (`deny`).
- Aplicar la ACL sobre la interfaz adecuada del router.
- Verificar que el tráfico se bloquea o permite conforme a la configuración establecida.
- Crear una ACL extendida para controlar servicios específicos.
- Comprobar cuántos paquetes han sido bloqueados por cada regla.

El modo de simulación de Packet Tracer permite observar cómo cada paquete es evaluado por la ACL, lo que facilita la comprensión del funcionamiento interno del filtrado de tráfico.

GL-4: ACLs estándar y extendidas en laboratorio físico

Esta guía trasladó la configuración de ACL a los routers Cisco 1841, 2800 y ISR 1100 del laboratorio. Los estudiantes aplicaron las mismas configuraciones sobre equipos reales, observando cómo las ACL afectan el tráfico generado desde los computadores del laboratorio. La práctica en equipo físico permitió trabajar con situaciones más cercanas a la realidad profesional, como la necesidad de modificar o eliminar ACL sin interrumpir el servicio de red.

Guías de laboratorio: VPN IPsec (GL-5 y GL-6)

El tercer bloque de prácticas abordó la creación de túneles seguros de comunicación entre dos redes. El objetivo fue que los estudiantes aprendieran a proteger la información que viaja por Internet entre dos redes, de manera que nadie pueda interceptarla ni modificarla durante su transmisión.

GL-5: VPN IPsec en Cisco Packet Tracer

La guía de simulación permitió configurar el túnel VPN completo entre dos routers sin riesgo de afectar equipos reales. Los estudiantes aprendieron a:

- Definir las políticas de seguridad (algoritmos de cifrado y métodos de autenticación).

- Especificar qué tráfico debe protegerse dentro del túnel.
- Aplicar la configuración en ambos extremos del túnel.
- Verificar que el túnel se establezca correctamente.
- Comprobar que el tráfico realmente viaje cifrado.

El modo de simulación de Packet Tracer permite observar el proceso de negociación del túnel paso a paso, lo que facilita la comprensión de cómo los routers intercambian información para establecer una conexión segura.

GL-6: VPN IPsec en laboratorio físico

Esta guía trasladó la configuración de VPN IPsec a dos routers Cisco 1841, 2800 o ISR 1100 del laboratorio. El trabajo con equipos físicos permitió a los estudiantes observar el proceso real de negociación del túnel y enfrentarse a situaciones prácticas, como la resolución de problemas cuando el túnel no se establece correctamente. La guía incluyó una sección de diagnóstico de problemas (*troubleshooting*), en la cual se emplearon comandos especializados que permiten visualizar en detalle lo que ocurre durante la negociación del túnel. Esto facilitó que el estudiante pudiera identificar y corregir errores de configuración de manera autónoma.

Guía de laboratorio: firewall Cisco ASA (GL-7)

GL-7: Configuración de Firewall Cisco ASA en Cisco Packet Tracer

Limitación de infraestructura

El Laboratorio de Telecomunicaciones de la Facultad de Ingeniería Electrónica no cuenta actualmente con dispositivos de firewall dedicados tipo Cisco ASA (Adaptive Security Appliance) u otros *appliances* de seguridad perimetral. Por esta razón, la guía GL-7 se diseñó únicamente en modalidad de simulación mediante Cisco Packet Tracer, que incluye el dispositivo ASA 5505 en su librería de equipos, reproduciendo con fidelidad suficiente el comportamiento del *appliance* para los escenarios propuestos. Se recomienda que, como

etapa posterior del proyecto, y una vez adquirido al menos un equipo Cisco ASA físico, se diseñe y compruebe la guía de laboratorio físico correspondiente.

Dualidad

El diseño en pares (simulación + laboratorio físico) para enrutamiento, ACL y VPN responde a una decisión pedagógica fundamentada en la literatura sobre formación en redes. La simulación permite experimentar libremente, repetir configuraciones y observar comportamientos de protocolos en modo paso a paso. El laboratorio físico expone al estudiante a la realidad del trabajo con hardware Cisco: gestión de la consola, mensajes de sistema, limitaciones de hardware y persistencia de configuración.

Esta estructura en dos etapas garantiza que el estudiante llegue al laboratorio físico con el procedimiento ya validado en simulación, reduciendo el tiempo en errores básicos y maximizando el tiempo con equipos reales. En coherencia con el ABP, ambas guías de cada par comparten el mismo escenario problemático central, de modo que la solución construida en simulación se valida y refuerza sobre la infraestructura real.

Las guías de laboratorio completas, que incluyen el desarrollo detallado de cada práctica, los comandos paso a paso y los ejercicios de aplicación independiente, se presentan en el Anexo C de este documento.

4.4. Resultados Fase 4

La cuarta fase tuvo como objetivo revisar la calidad del material didáctico mediante un proceso de análisis interno y la elaboración de los instrumentos de evaluación correspondientes. Este proceso se organizó en dos dimensiones: una revisión técnica de los procedimientos a través de la ejecución directa de las guías, y la construcción de rúbricas evaluativas como herramienta de control de calidad y para su posterior uso en el laboratorio.

4.4.1. Revisión interna del material mediante ejecución controlada

El proceso de revisión consistió en la ejecución completa de cada guía por parte del autor, siguiendo estrictamente cada paso descrito, con el fin de comprobar que los procedimientos produjeran los resultados esperados tanto en Packet Tracer como en los equipos físicos. Esta revisión controlada permitió someter el material a un análisis sistemático basado en los siguientes criterios:

1. **Replicabilidad.** Se verificó que la secuencia de comandos y procedimientos produce resultados idénticos en cualquier equipo del laboratorio que cumpla las especificaciones, sin requerir ajustes adicionales.

2. **Verificabilidad.** Se comprobó que los resultados obtenidos son contrastables mediante los comandos *show* y las pruebas de conectividad especificadas en cada guía.

3. **Conectividad funcional.** Se confirmó que las configuraciones propuestas permiten establecer comunicación extremo a extremo, validada mediante pruebas *ping* y *traceroute* según el protocolo trabajado.

4. **Claridad de las instrucciones.** Se evaluó que cada paso está redactado de forma comprensible y pueda ser ejecutado de manera autónoma por un estudiante con los conocimientos previos definidos.

5. **Coherencia entre modalidades.** En los pares de guías diseñados para simulación y laboratorio físico (GL-1/GL-2, GL-3/GL-4 y GL-5/GL-6), se constató que el escenario planteado en Packet Tracer es funcionalmente equivalente al implementado en equipos reales.

4.4.2. Diseño de rúbricas de evaluación

Como parte del proceso de revisión de la calidad del material didáctico, se diseñaron rúbricas de evaluación concebidas como herramientas de valoración integral del desempeño del estudiante. Su doble función es formativa, al comunicar los criterios al estudiante antes de la práctica, y sumativa, al proporcionar criterios uniformes para asignar calificación. Esta doble función es coherente con el ABP: la evaluación no se limita a verificar si se siguió un procedimiento, sino que valora la capacidad de razonamiento técnico, la autonomía y la calidad de la verificación.

Estructura de la rúbrica

La rúbrica adopta una estructura matricial que cruza criterios con niveles de desempeño, organizados según las secciones de cada guía. Para cada criterio se definen tres niveles con descriptores cualitativos:

Tabla 4.4.1: Niveles de desempeño y descriptores generales de la rúbrica

Nivel	Porcentaje	Descripción
Logrado	100	Ejecuta el criterio de forma completa y autónoma, sin orientación del docente, con resultados verificables acordes al comportamiento esperado del dispositivo.
En proceso	50	Ejecuta el criterio parcialmente o con errores menores que puede corregir con mínima orientación; el resultado refleja comprensión funcional del principio técnico.
No logrado	0	No completa el criterio de forma funcional o requiere orientación directa y extensa del docente para avanzar.

Rúbricas de evaluación

Se diseñaron rúbricas específicas para cada bloque de prácticas, con el propósito de garantizar coherencia entre los objetivos de aprendizaje, las actividades desarrolladas y los criterios de evaluación. En total, se elaboraron cuatro rúbricas, una por cada bloque

temático de las guías de laboratorio:

1. **Rúbrica para Enrutamiento Estático (GL-1 y GL-2):** Evalúa el armado de la topología, la configuración de direcciones IP en los routers, la implementación de rutas estáticas, la configuración de hosts y la realización de pruebas de conectividad. Consta de 9 criterios que suman un total de 100 puntos.

2. **Rúbrica para ACL (GL-3 y GL-4):** Evalúa la configuración de listas de control de acceso estándar y extendidas, su aplicación correcta en las interfaces, la verificación de las reglas y la realización de pruebas de tráfico bloqueado y permitido. Consta de 9 criterios que suman un total de 100 puntos.

3. **Rúbrica para VPN IPsec (GL-5 y GL-6):** Evalúa la configuración de las políticas ISAKMP, la definición de los parámetros de cifrado, la aplicación del *crypto map*, el establecimiento exitoso del túnel y la verificación del tráfico cifrado. Consta de 8 criterios que suman un total de 100 puntos.

4. **Rúbrica para Firewall Cisco ASA (GL-7):** Evalúa el diseño de la topología de tres zonas, la asignación de niveles de seguridad, la configuración de las listas de acceso entre zonas, la implementación de NAT y la realización de pruebas de tráfico controlado. Consta de 8 criterios que suman un total de 100 puntos.

Es importante señalar que todas las rúbricas se rigen por el sistema de evaluación institucional, cuya calificación es sobre 5.0. Aunque cada rúbrica se estructura sobre una base de 100 puntos para distribuir de manera equilibrada los criterios técnicos evaluados, la nota final se convierte proporcionalmente a la escala oficial de la Universidad.

El diseño general de la Rúbrica 1 puede observarse en la Figura 4.4.1, la cual presenta la organización de los criterios y niveles de desempeño. Las rúbricas completas, con la descripción detallada de cada criterio, los niveles de desempeño y la ponderación correspondiente, se presentan en el Anexo D de este documento.

UNIVERSIDAD SANTO TOMÁS · FACULTAD DE INGENIERÍA ELECTRÓNICA

Rúbrica de Evaluación

Laboratorio N.º 1 · Configuración de Routers Cisco con Enrutamiento Estático

Criterio	Logrado (100%)	En proceso (50%)	No logrado (0%)	Peso (sobre 5.0)
(Marcar el nivel alcanzado en cada criterio)	100%	50%	0%	5.0
PARTE 1 — CONSTRUCCIÓN DE LA TOPOLOGÍA				
Armado y cableado de la topología *Verificación: Topología completa y funcional*	Arma la topología completa (4 routers, 4 switches, 4 PCs) sin errores. Selecciona correctamente el tipo de cable para cada conexión e instala los módulos WIC-2T sin orientación.	Arma la topología con uno o dos errores menores en el tipo de cable o en la instalación de módulos, que logra corregir con mínima orientación del docente.	No completa el armado de la topología, o comete errores fundamentales en el cableado que impiden avanzar sin orientación directa del docente.	**0.5**
PARTE 2 — CONFIGURACIÓN DE INTERFACES				
Direcciones IP y máscaras en los 4 routers *Verificación: show ip interface brief*	Configura correctamente las 12 interfaces (3 por router) con las direcciones IP y máscaras exactas. Todas aparecen como *up/up* en `show ip interface brief`.	Configura con 1–3 errores de dirección IP o máscara, pero demuestra comprensión del proceso. La mayoría de las interfaces están activas y operativas.	Más de 3 interfaces con errores o sin configurar. Omite `no shutdown` en varias, resultando en interfaces *down/down*.	**1.0**
Clock rate y enlaces seriales *Verificación: show controllers serial*	Identifica de forma autónoma el extremo DCE de cada enlace serial usando `show controllers`, configura el clock rate correcto y todos los enlaces están en estado *up/up*.	Configura el clock rate con ayuda o comete un error en la identificación del extremo DCE, pero logra al menos 2 de los 3 enlaces seriales activos.	No identifica el extremo DCE o no configura el clock rate, dejando los enlaces seriales en estado *down/down* sin corregirlo.	**0.25**
PARTE 3 — ENRUTAMIENTO ESTÁTICO				
Rutas estáticas en los 4 routers *Verificación: show ip route*	Implementa correctamente las 20 rutas estáticas (5 por router) con red destino, máscara e interfaz de salida exactas. `show ip route` muestra la tabla completa marcada con "S".	Implementa entre 14 y 19 rutas correctas. La tabla de enrutamiento refleja rutas faltantes en 1–2 routers, pero la conectividad parcial es funcional.	Menos de 14 rutas correctas, o errores críticos en red/máscara que impiden el enrutamiento. `show ip route` no refleja la topología esperada.	**1.25**
Verificación con comandos *show* *Verificación: Uso autónomo de comandos*	Usa de forma autónoma `show ip interface brief` y `show ip route` para verificar su configuración, interpreta correctamente la salida e identifica y corrige errores sin intervención.	Ejecuta los comandos de verificación cuando se le indica; interpreta la mayor parte de la salida pero requiere ayuda para relacionar los resultados con los errores de configuración.	No ejecuta los comandos de verificación de forma espontánea o no interpreta su salida; depende del docente para detectar y corregir cualquier error.	**0.25**
PARTE 4 — HOSTS Y PRUEBAS DE CONECTIVIDAD				
Configuración de los 4 PCs *Verificación: ping al gateway*	Configura los 4 PCs con dirección IP, máscara de subred y gateway predeterminado correctos. Cada PC hace ping exitoso a su propio gateway.	Configura correctamente 3 de los 4 PCs; el cuarto tiene un error en IP o gateway que el estudiante detecta pero no corrige por completo.	Configura 1–2 PCs o comete errores en la mayoría de los campos, impidiendo la conectividad básica desde los hosts.	**0.5**
Pruebas de conectividad con `ping` *Verificación: 100% conectividad entre LANs*	Todos los pings entre redes diferentes son exitosos (100% de conectividad entre las 4 LANs). El estudiante prueba sistemáticamente desde cada PC hacia hosts en las demás redes.	Al menos el 75% de los pings entre redes distintas son exitosos. Hay fallo en 1–2 rutas específicas que el estudiante puede identificar pero no resolver por completo.	Menos del 50% de los pings son exitosos. La conectividad entre redes no está establecida y el estudiante no logra identificar la causa del problema.	**0.5**
EJERCICIO INDEPENDIENTE 1 — SIN GUÍA PASO A PASO				
Diseño VLSM y tabla de direccionamiento *Evaluación: Trabajo autónomo*	Diseña correctamente el esquema VLSM: calcula subredes, determina máscaras, asigna IPs y construye la tabla de direccionamiento sin errores ni orientación.	El diseño VLSM presenta 1–2 errores menores (máscara incorrecta o dirección fuera de rango) que el estudiante corrige al señalársele.	El diseño VLSM presenta errores en más del 50% de las subredes o el estudiante no completa la tabla sin orientación extensa del docente.	**0.4**
Configuración y conectividad autónoma *Evaluación: Resultado funcional sin apoyo*	Configura todas las interfaces y rutas estáticas a partir de su propia tabla, verifica con `show` y logra conectividad total entre todas las redes, sin consultar la guía.	Completa la configuración con una consulta puntual. El resultado final es funcional con errores mínimos que no afectan la conectividad global.	No logra completar la configuración de forma autónoma o la conectividad final es inferior al 50%, requiriendo orientación en cada etapa.	**0.2**
EJERCICIO INDEPENDIENTE 2 — SIN GUÍA PASO A PASO				
Armado y exactitud de la configuración *Evaluación: Precisión técnica*	Construye, cablea y configura la segunda topología propuesta de forma completamente autónoma. Todos los comandos de Cisco IOS son correctos, sin errores tipográficos ni de lógica de red.	Configura la topología con 1–3 errores de IOS (comandos mal escritos o parámetros incorrectos) que detecta y corrige con mínima ayuda.	Comete errores recurrentes en IOS o en la lógica de configuración que le impiden avanzar sin apoyo del docente en cada paso.	**0.1**
Conectividad total y demostración *Evaluación: Pruebas finales y sustentación*	Demuestra conectividad total entre todas las redes mediante pings exitosos y exhibe las tablas de enrutamiento completas, respondiendo con seguridad a las preguntas.	Conectividad del 75%, con tablas de enrutamiento parcialmente correctas. El estudiante responde preguntas básicas pero tiene dificultad con las más técnicas.	Conectividad inferior al 50% o el estudiante no puede explicar la lógica de su configuración ni interpretar los resultados de los comandos de verificación.	**0.05**
			CALIFICACIÓN FINAL (suma de pesos ponderados)	5.0

Figura 4.4.1: Rúbrica de Evaluación - Laboratorio N.°1

Fuente: Autor

Conclusiones

El desarrollo del presente trabajo permitió diseñar un conjunto integral de once documentos didácticos orientados a la enseñanza de redes y ciberseguridad Cisco, dirigidos al programa de Ingeniería Electrónica de la Universidad Santo Tomás. Estos materiales —dos manuales de equipo, dos guías de aprendizaje teórico y siete guías de laboratorio— responden a la necesidad de estandarizar las prácticas de laboratorio y ofrecer recursos estructurados que faciliten el desarrollo de competencias en tecnologías Cisco.

La combinación de guías teóricas y prácticas para los temas de enrutamiento, listas de control de acceso (ACL) y VPN permitió conectar los conceptos fundamentales con su aplicación en entornos de laboratorio. Esta metodología favorece la comprensión de las configuraciones de red y la resolución de problemas, asegurando que los estudiantes puedan aplicar los protocolos y procedimientos de manera consistente y segura.

Por último, las rúbricas de evaluación construidas como parte del proceso de revisión de la calidad proporcionan criterios claros, objetivos y medibles para valorar el desempeño estudiantil. Estas rúbricas aseguran coherencia entre los objetivos de aprendizaje, las actividades prácticas y los resultados esperados, fortaleciendo la transparencia del proceso evaluativo. Asimismo, su estructura facilita la retroalimentación formativa, orientando a los estudiantes en la mejora de aspectos técnicos y procedimentales.

Referencias

Accenture, W. E. F. (2024). Global cybersecurity outlook 2024. Technical report, World Economic Forum.

Aguilar Ojeda, C. E., Hernández Omaña, T. H., and Soto Ortíz, S. I. (2024). Buenas prácticas de ciberseguridad en educación superior = good cybersecurity practices in higher education. *South Florida Journal of Development*, 5(12):1–10.

Ahsan, M. S. and Pathan, A.-S. K. (2025). A comprehensive survey on the requirements, applications, and future challenges for access control models in iot: The state of the art. *IEEE Access*, 9:1317–1345.

Albarracín, E. R. and Camacho, P. J. D. (2010). Modelo educativo pedagógico universidad santo tomás. Technical report, Universidad Santo Tomás.

Albarrán Torres, F. A. and Díaz Larenas, C. H. (2021). Metodologías de aprendizaje basado en problemas, proyectos y estudio de casos en el pensamiento crítico de estudiantes universitarios = teaching-learning methodologies based on problems, projects and case-study for the development of critical thinking in university students. *Revista de Ciencias Médicas de Pinar del Río*, 25(3):e5116. Publicado 17 de junio de 2021.

Anderson, R. (2020). *Security Engineering: A Guide to Building Dependable Distributed Systems*. Wiley, 3 edition.

Bautista, F. G., Guzmán, L. M., and Blanco, L. F. (2023). Estudio anual de ciberseguridad. *Cámara Colombiana de Informática y Telecomunicaciones (CCIT)*.

Calle García, A. J., Conforme Merchan, Y. M., Magallanes Bueno, E. L., and Guaranda Bravo, J. Y. (2024). Importancia de la ciberseguridad en la investigación de mercados digital. *Ciencia y Desarrollo*.

Cisco Networking Academy (n.d.). About cisco networking academy. urlhttps://www.netacad.com/es/about. Recuperado el 11 de febrero de 2026.

Cisco Systems, Inc. (2013). *Cisco ASA 5500-X Series Firewalls: Next-Generation Security Appliances*. Consultado en línea.

Deering, S. and Hinden, R. (2017). Internet protocol, version 6 (ipv6) specification. RFC 8200.

Ebrahimi, E., Pare, M., Stoker, G., and White, S. (2025). Cybersecurity early education: A review of current cybersecurity education for young children. In *Proceedings of the 17th International Conference on Computer Supported Education - Volume 1: ERSeGEL*, pages 822–833. INSTICC, SciTePress.

Hauser, F., Häberle, M., Schmidt, M., and Menth, M. (2020). P4-ipsec: Site-to-site and host-to-site vpn with ipsec in p4-based sdn. *IEEE Access*, 8:139567–139580.

Herrera, C. (2023). AnÁlisis de la seguridad en el cifrado de tÚneles ipv6 con el manejo de los protocolos ipsec. *UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD*.

Herrero-Martín, J., Rodríguez-Merino, C., Alba, R. V., and Amo-Filva, D. (2022). Ciberseguridad y educación: Variables de sensibilidad y cambio en la formación del profesorado. In *Actas del VIII Congreso de Innovación Educativa y Docencia en Red (IN-RED 2022)*, pages 956–964, Valencia, España. Universitat Politècnica de València.

Ismail, M., Madathil, N. T., Alalawi, M., Alrabaee, S., Bataineh, M. A., Melhem, S., and Mouheb, D. (2024). Cybersecurity activities for education and curriculum design: A survey. *Computers in Human Behavior Reports*, 16:100501.

Kurose, J. F. and Ross, K. W. (2017). *Redes de computadoras: Un enfoque descendente.* Pearson Educación, 7 edition.

López, Z. (2018). El diseño de materiales didácticos sobre tic para una enseñanza universitaria inclusiva y online = the design of instructional materials about ict to an inclusive and online university teaching. *Revista Internacional de Comunicación y Desarrollo (RICD)*, 2(9):30–41.

National Institute of Standards and Technology (2024). The nist cybersecurity framework (csf) 2.0. U.S. Department of Commerce.

Odom, W. (2020). *CCNA 200-301 Official Cert Guide, Volume 1.* Cisco Press.

Peralta Lara, D. C. and Guamán Gómez, V. J. (2020). Metodologías activas para la enseñanza y aprendizaje de los estudios sociales = active methodologies for the teaching and learning of social studies. *Revista Sociedad & Tecnología*, 3(2):2–10.

Rivera Alturo, L. M. and Hernández García, S. A. (2023). La ciberseguridad un enfoque de aprendizaje, desde el rol del suboficial del ejército nacional de colombia. *Miradas*, 18(2):190–209.

Rodríguez-Rivas, J. G., Zúñiga, M. A. R., and Rosales, A. R. S. (2020). Capítulo 7. cisco networking academy: entornos virtuales de aprendizaje en educación superior.

Saito, H. (2021). Automatización de las redes para los servicios de tecnología financiera: La automatización de los entornos de cisco con red hat ansible automation platform. Estudio de caso, Mizuho Information & Research Institute, Inc. Incluye datos de IDC Market Forecast 2022–2026 y casos de automatización de TI en servicios financieros.

Suárez, G. Y., Bolino, P. E., Venosa, P., and Queiruga, C. A. (2024). Acercando la ciberseguridad a la escuela secundaria desde una perspectiva lúdica. *SADIO Electronic Journal of Informatics and Operations Research*, 23(2):e056.

Sánchez, V. G. J., Masabanda, R. I. T., and Espinoza, C. J. L. (2025). Ciberseguridad en

la educación superior: evaluación y estrategias de formación. *Technology Rain Journal*, 4(2).

Tanenbaum, A. S. and Wetherall, D. J. (2011). *Computer Networks*. Prentice Hall, Upper Saddle River, NJ, USA, 5th edition.

Teja, K., Hanish, T. S., Abhijith, K., Chaitanya, G. K., Deepak, O. N., and Subramanyam, M. M. (2023). Prevention of attacks and flow control of firewalls. In *Proceedings of the 2023 9th International Conference on Advanced Computing and Communication Systems (ICACCS)*, pages 2144–2150, Coimbatore, India. IEEE. Presented on 17–18 March 2023.

Tomás, U. S. (2023). Proyecto educativo institucional (pei). acuerdo no. 20 del 13 de junio de 2023.

Anexos

Anexo A: MANUALES

- Manual de Uso - Router Cisco ISR 1100X-4G
- Manual de Uso - Routers Cisco 1841

Anexo B: GUÍAS ACADEMICAS

- Fundamentos de Redes de Datos
- Fundamentos de Ciberseguridad

Anexo C: GUÍAS DE LABORATORIO

- Configuración de Routers Cisco - Cisco Packet Tracer
- Configuración de Routers Cisco - Laboratorio Físico
- Configuración de Protocolo ACLs Estándar y Extendido en Cisco Packet Tracer
- Configuración de Protocolo ACLs Estándar y Extendido en Laboratorio Físico
- Configuración de Protocolo VPN IPsec en Cisco Packet Tracer
- Configuración de Protocolo VPN IPsec en Laboratorio Físico
- Configuración de Firewall

Anexo D: RUBRICAS DE EVALUACIÓN

- Rúbrica para Enrutamiento Estático
- Rúbrica para ACL
- Rúbrica para VPN IPsec
- Rúbrica para Firewall Cisco ASA