Capacidades técnicas, tácticas y de respuesta para equipos red team y blue team

Jessica Alxandra Rosales Gamboa

Asesor

Eduvin Trigos Sánchez

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Especialización en seguridad informática

2026

Dedicatoria

Dedico este trabajo a Dios, por ser mi guía y fortaleza en cada etapa de este proceso académico; a mi familia, por su apoyo incondicional, comprensión y constante motivación, fundamentales para alcanzar mis metas; y a todas aquellas personas que han contribuido a mi crecimiento personal y profesional, inspirándome a continuar fortaleciendo mis conocimientos y competencias en el campo de la ciberseguridad y las tecnologías de la información.

Agradecimientos

Expreso mi más sincero agradecimiento a la Universidad Nacional Abierta y a Distancia (UNAD) por brindar los espacios académicos, las herramientas y los recursos necesarios para fortalecer mis conocimientos y competencias profesionales.

De manera especial, agradezco a los docentes y tutores del Seminario Especializado Equipos Estratégicos en Ciberseguridad: Red Team y Blue Team, por su orientación, acompañamiento y valiosos aportes académicos, los cuales fueron fundamentales para el desarrollo de las actividades y el cumplimiento de los objetivos propuestos.

Asimismo, extiendo mi gratitud a mis compañeros de estudio y a todas las personas que compartieron sus experiencias, conocimientos y apoyo durante esta etapa de formación, contribuyendo significativamente a mi crecimiento académico y profesional y a la consolidación de este trabajo.

Resumen

El presente informe técnico final consolida los resultados obtenidos durante el desarrollo del Seminario Especializado Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team, integrando los conocimientos teóricos, prácticos, éticos y normativos adquiridos a lo largo de las diferentes etapas del curso. El trabajo se desarrolló a partir del escenario propuesto por SecureNova Labs, organización ficticia utilizada para simular situaciones relacionadas con incidentes de seguridad informática, análisis de vulnerabilidades, pruebas de penetración y estrategias de defensa. Durante el seminario se abordaron aspectos fundamentales asociados con la legislación informática colombiana, la ética profesional en operaciones de ciberseguridad, la aplicación de metodologías de pentesting y la implementación de mecanismos de detección y respuesta ante incidentes. Desde la perspectiva ofensiva, se ejecutaron actividades propias de un equipo Red Team orientadas a identificar vulnerabilidades, evaluar superficies de ataque y analizar posibles vectores de compromiso en sistemas Windows. De manera complementaria, desde la perspectiva defensiva, se desarrollaron actividades Blue Team enfocadas en la detección, análisis, contención y mitigación de amenazas mediante herramientas de monitoreo y protección. Los resultados permitieron identificar debilidades relacionadas con la exposición de servicios vulnerables, configuraciones inseguras y deficiencias en los mecanismos de monitoreo, evidenciando la necesidad de implementar estrategias de hardening, gestión de vulnerabilidades, segmentación de redes y monitoreo continuo para fortalecer la postura de seguridad organizacional. Finalmente, el informe presenta un análisis integral de los hallazgos identificados, así como conclusiones y recomendaciones orientadas a mejorar los controles técnicos, administrativos y operacionales necesarios para proteger la confidencialidad, integridad y disponibilidad de la información.

Palabras clave: Ciberseguridad, hardening, pentesting, riesgo, vulnerabilidad.

Abstract

This final technical report consolidates the results obtained during the Specialized Seminar Strategic Cybersecurity Teams: Red Team & Blue Team, integrating the theoretical, practical, ethical, and regulatory knowledge acquired throughout the different stages of the course. The work was developed based on the SecureNova Labs scenario, a simulated organization designed to recreate cybersecurity incidents, vulnerability assessments, penetration testing activities, and defensive security strategies. Throughout the seminar, key topics related to Colombian cyber legislation, professional ethics, penetration testing methodologies, and incident response practices were addressed. From the offensive perspective, Red Team activities were conducted to identify vulnerabilities, assess attack surfaces, and analyze potential compromise vectors within Windows-based systems. From the defensive perspective, Blue Team operations focused on threat detection, monitoring, containment, and mitigation through the implementation of security monitoring and protection mechanisms. The results revealed weaknesses associated with vulnerable services, insecure configurations, and insufficient monitoring controls, highlighting the importance of implementing hardening measures, vulnerability management programs, network segmentation, and continuous monitoring processes to strengthen organizational security. Finally, this report provides an integrated analysis of the identified findings, together with conclusions and recommendations aimed at improving the technical, administrative, and operational controls required to ensure the confidentiality, integrity, and availability of information assets.

Keywords: Cybersecurity, hardening, pentesting, risk, vulnerability.

Tabla de contenido

Lista de Figuras

Lista de Tablas

Lista de Apéndices

Glosario

Activo de información:

Recurso físico o digital que posee valor para una organización y que requiere protección frente a amenazas que puedan afectar su confidencialidad, integridad o disponibilidad.

Blue Team:

Equipo de ciberseguridad encargado de las actividades defensivas dentro de una organización. Sus funciones incluyen la detección, análisis, contención y respuesta ante incidentes de seguridad informática.

Ciberseguridad:

Conjunto de prácticas, procesos, tecnologías y controles orientados a proteger sistemas informáticos, redes, aplicaciones y datos frente a amenazas, ataques o accesos no autorizados.

Confidencialidad:

Principio de la seguridad de la información que garantiza que los datos únicamente puedan ser consultados por personas, sistemas o procesos debidamente autorizados.

EDR:

Tecnología de seguridad conocida como Endpoint Detection and Response, diseñada para monitorear, detectar y responder a amenazas que afectan los dispositivos finales conectados a una red.

Escalamiento de privilegios:

Técnica utilizada por un atacante para obtener permisos superiores a los inicialmente concedidos dentro de un sistema comprometido.

Exploit:

Código, herramienta o procedimiento utilizado para aprovechar una vulnerabilidad existente en un sistema, aplicación o servicio con el fin de obtener acceso o ejecutar acciones no autorizadas.

Hardening:

Proceso de fortalecimiento de la seguridad de sistemas operativos, aplicaciones o dispositivos mediante la eliminación de configuraciones inseguras y la implementación de controles de protección.

Host:

Dispositivo conectado a una red que posee una dirección IP y puede ofrecer o consumir servicios dentro de un entorno informático.

IDS:

Sistema de detección de intrusiones encargado de monitorear eventos y actividades dentro de una red o sistema para identificar comportamientos sospechosos o maliciosos.

Integridad:

Principio de seguridad que garantiza que la información permanezca completa, exacta y libre de modificaciones no autorizadas.

Metasploit:

Framework utilizado en pruebas de penetración que permite validar vulnerabilidades mediante la ejecución controlada de exploits y módulos de seguridad.

Nmap:

Herramienta de análisis de redes utilizada para descubrir dispositivos conectados, identificar puertos abiertos y determinar los servicios activos en un sistema.

Pentesting:

Metodología de evaluación de seguridad que consiste en simular ataques controlados con el propósito de identificar vulnerabilidades y debilidades en sistemas informáticos.

Pivoting:

Técnica utilizada después de comprometer un sistema para acceder o desplazarse hacia otros dispositivos ubicados dentro de la misma red.

Red Team:

Equipo especializado en la simulación de ataques informáticos con el objetivo de identificar vulnerabilidades, evaluar controles de seguridad y medir la capacidad de detección de una organización.

SIEM (Security Information and Event Management):

Solución tecnológica que centraliza la recopilación y correlación de registros de seguridad provenientes de diferentes fuentes, permitiendo identificar comportamientos anómalos, investigar eventos y apoyar la respuesta ante incidentes de manera más eficiente.

SMB (Server Message Block):

Protocolo de red ampliamente empleado en entornos Windows que facilita el acceso compartido a recursos como archivos, dispositivos de impresión y otros servicios disponibles entre equipos conectados a la misma infraestructura de red.

Vulnerabilidad:

Corresponde a cualquier debilidad presente en un sistema, aplicación, procedimiento o configuración que pueda ser aprovechada por una amenaza para comprometer la confidencialidad, integridad o disponibilidad de la información.

Wazuh:

Plataforma de monitoreo y gestión de eventos de seguridad utilizada para la detección de amenazas, análisis de registros y respuesta ante incidentes.

Introducción

La ciberseguridad se ha consolidado como uno de los pilares fundamentales para la protección de la información y la continuidad de las operaciones dentro de las organizaciones modernas. El crecimiento de las tecnologías digitales, la adopción masiva de servicios en red y la constante evolución de las amenazas informáticas han generado la necesidad de implementar estrategias que permitan identificar, prevenir y responder oportunamente ante posibles incidentes de seguridad.

En este contexto, los equipos Red Team y Blue Team desempeñan un papel fundamental en la evaluación y el fortalecimiento de los controles de seguridad. Mientras el Red Team adopta una perspectiva ofensiva mediante la simulación de ataques controlados, el Blue Team desarrolla actividades orientadas a la detección, el monitoreo, el análisis y la mitigación de amenazas. La interacción entre ambos enfoques permite obtener una visión integral del estado de seguridad de una organización y contribuye al fortalecimiento continuo de sus capacidades defensivas

El presente informe técnico final consolida los resultados obtenidos durante el desarrollo del Seminario Especializado Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team, integrando los conocimientos teóricos, prácticos, éticos y normativos abordados a lo largo de las diferentes etapas del curso. Para ello, se toma como referencia el escenario SecureNova Labs, diseñado para simular situaciones relacionadas con vulnerabilidades, incidentes de seguridad y procesos de respuesta organizacional.

A lo largo del documento se presentan los principales hallazgos obtenidos durante las actividades desarrolladas, incluyendo aspectos relacionados con la identificación de vulnerabilidades, el análisis de riesgos, la aplicación de metodologías de pentesting, el monitoreo de eventos de seguridad y el fortalecimiento de controles técnicos. Finalmente, se exponen las

conclusiones y recomendaciones derivadas del ejercicio realizado, orientadas a mejorar la postura de seguridad y la gestión del riesgo en entornos organizacionales.

Justificación

La creciente dependencia de los sistemas de información y de las infraestructuras tecnológicas ha incrementado la exposición de las organizaciones a múltiples amenazas cibernéticas capaces de afectar la confidencialidad, integridad y disponibilidad de la información. Esta realidad exige la formación de profesionales con capacidades técnicas y analíticas que les permitan comprender el comportamiento de las amenazas, evaluar vulnerabilidades y diseñar estrategias efectivas para la protección de los activos digitales.

El desarrollo de actividades basadas en metodologías Red Team y Blue Team permite recrear escenarios similares a los que enfrentan las organizaciones en entornos reales, facilitando la comprensión de los procesos ofensivos y defensivos involucrados en la gestión de la seguridad informática. A través de estos ejercicios es posible identificar debilidades, validar controles existentes y fortalecer las capacidades de detección y respuesta frente a incidentes de seguridad.

Asimismo, el análisis del escenario SecureNova Labs proporciona un contexto práctico que permite integrar aspectos técnicos, éticos y legales relacionados con la ciberseguridad. Esto favorece el desarrollo de competencias orientadas a la toma de decisiones, la gestión del riesgo y la implementación de medidas de protección alineadas con las necesidades actuales de las organizaciones.

Finalmente, este informe se justifica por su aporte académico y profesional, ya que permite consolidar los conocimientos adquiridos durante el seminario, documentar los resultados obtenidos y formular recomendaciones orientadas al fortalecimiento de la seguridad en entornos organizacionales.

Objetivos

Objetivo General

Analizar los resultados obtenidos durante el desarrollo del Seminario Especializado Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team, mediante la aplicación de estrategias ofensivas y defensivas orientadas a la identificación de vulnerabilidades, evaluación de riesgos y fortalecimiento de la seguridad en el escenario SecureNova Labs.

Objetivos Específicos

Identificar las principales vulnerabilidades presentes en el entorno de laboratorio mediante la aplicación de técnicas de reconocimiento, escaneo y análisis de seguridad desarrolladas durante las actividades Red Team.

Analizar las implicaciones éticas, legales y normativas relacionadas con la ejecución de operaciones de ciberseguridad dentro del contexto planteado por el escenario SecureNova Labs.

Evaluar los mecanismos de detección, monitoreo, contención y respuesta implementados durante las actividades Blue Team para la gestión de incidentes de seguridad.

Determinar el impacto potencial de las vulnerabilidades identificadas sobre la confidencialidad, integridad y disponibilidad de la información

Proponer estrategias de mitigación y fortalecimiento orientadas a mejorar la postura de seguridad de la organización frente a amenazas actuales y futuras.

Desarrollo del Informe

Contexto General del Seminario

La ciberseguridad constituye uno de los componentes más importantes para la protección de la información dentro de las organizaciones modernas. El incremento constante de amenazas informáticas, vulnerabilidades tecnológicas y ataques dirigidos ha generado la necesidad de implementar mecanismos que permitan fortalecer la capacidad de prevención, detección y respuesta frente a incidentes de seguridad.

En este contexto, los equipos Red Team y Blue Team representan dos enfoques complementarios para la evaluación de la seguridad organizacional. Mientras el Red Team simula el comportamiento de un atacante con el propósito de identificar vulnerabilidades y validar controles de seguridad, el Blue Team desarrolla actividades orientadas a la protección de los activos de información mediante procesos de monitoreo, detección, análisis y respuesta ante incidentes

Durante el desarrollo del Seminario Especializado Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team se abordaron aspectos relacionados con la legislación informática, la ética profesional, las metodologías de pentesting y la gestión de incidentes de seguridad. Estas actividades permitieron integrar conocimientos teóricos y prácticos mediante el análisis de escenarios simulados diseñados para fortalecer las competencias de los participantes en materia de ciberseguridad.

El seminario se desarrolló a través de diferentes etapas que permitieron comprender el ciclo completo de una operación de seguridad, desde la identificación de vulnerabilidades hasta la implementación de controles de mitigación y fortalecimiento de la infraestructura tecnológica.

Esta aproximación facilitó la comprensión de los desafíos que enfrentan las organizaciones en la actualidad y la importancia de adoptar estrategias integrales de protección.

Descripción del Escenario SecureNova Labs

SecureNova Labs corresponde a un escenario académico diseñado para simular un incidente de seguridad informática dentro de un entorno organizacional. El caso plantea la posible existencia de actividades maliciosas relacionadas con accesos no autorizados, explotación de vulnerabilidades y compromiso de sistemas críticos

La situación inicial describe una posible fuga de información desde una estación de trabajo denominada Host-A, en la cual se detectaron indicios asociados a la creación de cuentas administrativas no autorizadas y posibles movimientos laterales hacia otros dispositivos de la red. Estos hallazgos generaron la necesidad de realizar un análisis técnico que permitiera determinar el origen del incidente, las vulnerabilidades involucradas y el impacto potencial sobre la organización.

Para el desarrollo de las actividades se implementó un entorno virtualizado compuesto por sistemas Windows vulnerables y una estación de trabajo Kali Linux utilizada para la ejecución de pruebas de seguridad. Este laboratorio permitió reproducir condiciones controladas para la identificación de vulnerabilidades, la simulación de ataques y la aplicación de mecanismos de defensa.

La utilización de escenarios simulados como SecureNova Labs facilita la aplicación práctica de metodologías de ciberseguridad sin generar riesgos sobre infraestructuras reales, permitiendo a los participantes desarrollar habilidades técnicas relacionadas con el análisis ofensivo y defensivo de sistemas de información.

Importancia de los Equipos Red Team y Blue Team

Las organizaciones actuales enfrentan amenazas cada vez más complejas que requieren enfoques de seguridad capaces de evaluar continuamente la efectividad de los controles implementados. En este sentido, los equipos Red Team y Blue Team constituyen una práctica ampliamente utilizada para medir el nivel de preparación de una organización frente a posibles ataques.

El Red Team se enfoca en la simulación de ataques reales utilizando técnicas, tácticas y procedimientos similares a los empleados por actores maliciosos. Su objetivo principal consiste en identificar vulnerabilidades, evaluar configuraciones inseguras y determinar posibles vectores de compromiso que puedan afectar la seguridad de los activos organizacionales.

Por su parte, el Blue Team desarrolla actividades orientadas a la protección de la infraestructura tecnológica mediante el monitoreo continuo, la identificación de eventos sospechosos, el análisis de registros y la respuesta ante incidentes. Este equipo desempeña un papel fundamental en la detección temprana de amenazas y en la implementación de medidas de mitigación.

La combinación de ambos enfoques permite obtener una visión integral de la seguridad organizacional, favoreciendo la mejora continua de los controles existentes y fortaleciendo la capacidad de respuesta frente a amenazas emergentes.

Alcance del Ejercicio Desarrollado

El ejercicio desarrollado durante el seminario tuvo como alcance la evaluación de vulnerabilidades presentes en un entorno de laboratorio controlado, así como la aplicación de metodologías ofensivas y defensivas orientadas al fortalecimiento de la seguridad informática.

Las actividades Red Team incluyeron procesos de reconocimiento de red, identificación de hosts activos, escaneo de puertos, enumeración de servicios y análisis de vulnerabilidades

presentes en los sistemas evaluados. Estas actividades permitieron determinar posibles superficies de ataque y validar la existencia de debilidades de seguridad asociadas a configuraciones vulnerables

Desde la perspectiva Blue Team, las actividades se enfocaron en la identificación de indicadores de compromiso, monitoreo de eventos de seguridad, análisis de registros y aplicación de medidas de contención y mitigación. Estas acciones permitieron comprender los procedimientos utilizados para gestionar incidentes y reducir el impacto potencial de las amenazas.

Todas las actividades desarrolladas se ejecutaron exclusivamente dentro de un entorno académico controlado, respetando los principios éticos, legales y profesionales asociados al ejercicio responsable de la ciberseguridad. Los resultados obtenidos tienen fines educativos y buscan fortalecer las competencias relacionadas con el análisis, reporte y comunicación de resultados técnicos en seguridad informática.

Fundamentos Teóricos de la Ciberseguridad

Ciberseguridad Organizacional

La ciberseguridad organizacional comprende el conjunto de políticas, procedimientos, tecnologías y controles implementados con el propósito de proteger los activos de información frente a amenazas internas y externas. Su objetivo principal consiste en garantizar la confidencialidad, integridad y disponibilidad de la información, principios fundamentales para el correcto funcionamiento de cualquier organización.

En la actualidad, las organizaciones dependen en gran medida de infraestructuras tecnológicas para el desarrollo de sus actividades operativas, administrativas y estratégicas. Esta dependencia ha incrementado la exposición a riesgos asociados con ataques informáticos, fuga de información, interrupción de servicios y accesos no autorizados. Como consecuencia, la

ciberseguridad ha dejado de ser un componente exclusivamente técnico para convertirse en un elemento estratégico dentro de la gestión organizacional.

La implementación de una estrategia de ciberseguridad efectiva requiere la integración de controles técnicos, administrativos y físicos orientados a reducir la superficie de ataque y fortalecer la capacidad de respuesta frente a incidentes de seguridad. Asimismo, es necesario promover una cultura organizacional basada en la gestión del riesgo y la protección de la información.

Ethical Hacking

El Ethical Hacking o hacking ético consiste en la aplicación autorizada de técnicas y metodologías utilizadas por atacantes con el fin de identificar vulnerabilidades y debilidades de seguridad antes de que puedan ser explotadas por actores maliciosos. Estas actividades son ejecutadas por profesionales especializados que actúan dentro de un marco legal y ético previamente definido.

El propósito principal del hacking ético es evaluar la efectividad de los controles de seguridad implementados dentro de una organización, permitiendo detectar vulnerabilidades que podrían comprometer la información o los servicios tecnológicos. Los resultados obtenidos durante estas evaluaciones sirven como base para la implementación de medidas correctivas y el fortalecimiento de la postura de seguridad.

Durante el desarrollo del seminario, los principios del Ethical Hacking fueron aplicados mediante ejercicios controlados orientados a la identificación de vulnerabilidades y al análisis de posibles vectores de ataque dentro del entorno SecureNova Labs

El hacking ético constituye una práctica fundamental para la identificación controlada de vulnerabilidades dentro de una organización y permite evaluar el nivel real de exposición frente a amenazas externas (Weidman, 2014)

Pentesting

Las pruebas de penetración, conocidas como pentesting, constituyen una metodología utilizada para evaluar la seguridad de sistemas, aplicaciones y redes mediante la simulación controlada de ataques informáticos. Su finalidad consiste en identificar vulnerabilidades, validar riesgos y determinar el nivel de exposición de una infraestructura tecnológica frente a posibles amenazas.

El proceso de pentesting generalmente se desarrolla en varias fases, incluyendo reconocimiento, descubrimiento de activos, escaneo, enumeración, explotación, post explotación y elaboración de informes. Cada una de estas etapas proporciona información relevante sobre las debilidades presentes en el entorno evaluado.

Durante las actividades desarrolladas en el laboratorio se aplicaron diferentes técnicas de pentesting para identificar vulnerabilidades asociadas al protocolo SMB y evaluar el riesgo que representaban para los sistemas analizados.

Las actividades de reconocimiento, enumeración, explotación y documentación de hallazgos forman parte de metodologías ampliamente utilizadas en pruebas de penetración profesionales (Weidman, 2014).

Gestión de Vulnerabilidades

La gestión de vulnerabilidades corresponde al proceso continuo de identificación, evaluación, tratamiento y monitoreo de debilidades presentes en sistemas de información. Su objetivo es reducir la probabilidad de explotación mediante la implementación de medidas correctivas oportunas.

Las vulnerabilidades pueden originarse por errores de configuración, software desactualizado, fallos de programación o deficiencias en los controles de seguridad. Si no son

gestionadas adecuadamente, estas debilidades pueden convertirse en puntos de entrada para atacantes y generar incidentes con impactos significativos para la organización

Una adecuada gestión de vulnerabilidades requiere la realización periódica de análisis de seguridad, aplicación de actualizaciones, implementación de controles compensatorios y seguimiento continuo de los riesgos identificados

La identificación temprana y corrección oportuna de vulnerabilidades reduce significativamente la probabilidad de explotación por parte de atacantes y constituye una práctica esencial dentro de los programas de seguridad organizacional (Easttom, 2018)

Gestión de Incidentes de Seguridad

La gestión de incidentes de seguridad comprende el conjunto de actividades orientadas a detectar, analizar, contener, erradicar y recuperar sistemas afectados por eventos que comprometen la seguridad de la información. Este proceso busca minimizar el impacto de los incidentes y restablecer las operaciones normales en el menor tiempo posible.

La efectividad de la gestión de incidentes depende de la existencia de procedimientos claramente definidos, herramientas de monitoreo adecuadas y personal capacitado para responder oportunamente ante situaciones de riesgo.

Durante las actividades Blue Team desarrolladas en el seminario se analizaron diferentes mecanismos de detección y respuesta que permitieron comprender la importancia de una adecuada gestión de incidentes dentro de las organizaciones.

Hardening

El hardening o fortalecimiento de sistemas consiste en la aplicación de configuraciones seguras destinadas a reducir las vulnerabilidades presentes en sistemas operativos, aplicaciones y dispositivos de red. Este proceso busca disminuir la superficie de ataque y limitar las posibilidades de explotación por parte de actores maliciosos.

Entre las actividades de hardening más comunes se encuentran la deshabilitación de servicios innecesarios, la aplicación de actualizaciones de seguridad, la implementación de políticas de control de acceso y el fortalecimiento de mecanismos de autenticación.

La aplicación de estas medidas constituye una de las estrategias más efectivas para reducir riesgos y mejorar la postura de seguridad de una organización.

Inteligencia de Amenazas

La inteligencia de amenazas es el proceso de recopilación, análisis e interpretación de información relacionada con amenazas actuales o potenciales que puedan afectar a una organización. Su propósito es proporcionar conocimiento útil para anticipar ataques, fortalecer controles de seguridad y mejorar la toma de decisiones.

La información obtenida mediante procesos de inteligencia puede incluir indicadores de compromiso, tácticas utilizadas por atacantes, vulnerabilidades emergentes y tendencias observadas en el panorama global de amenazas.

La integración de inteligencia de amenazas dentro de las estrategias de ciberseguridad permite adoptar un enfoque proactivo frente a los riesgos y mejorar la capacidad de detección y respuesta ante incidentes.

Este enfoque resulta fundamental para anticipar las tácticas, técnicas y procedimientos utilizados por actores maliciosos, fortaleciendo la capacidad de las organizaciones para prevenir y responder de manera efectiva a las amenazas cibernéticas (Andress & Winterfeld, 2014).

Defensa en Profundidad

La defensa en profundidad es una estrategia de seguridad basada en la implementación de múltiples capas de protección destinadas a dificultar el avance de un atacante dentro de una infraestructura tecnológica. Este enfoque reconoce que ningún control es completamente efectivo por sí solo y, por tanto, combina diferentes mecanismos de seguridad para reducir el riesgo.

Las capas de defensa pueden incluir controles físicos, administrativos y técnicos, tales como firewalls, sistemas IDS/IPS, soluciones EDR, segmentación de redes, autenticación multifactor y monitoreo continuo.

La aplicación de una estrategia de defensa en profundidad contribuye significativamente a mejorar la resiliencia organizacional frente a amenazas cibernéticas y constituye una práctica recomendada dentro de los marcos modernos de ciberseguridad.

Marco Legal y Ético Aplicado

El desarrollo de actividades relacionadas con la ciberseguridad requiere el cumplimiento de principios éticos, legales y profesionales que garanticen el uso responsable de los conocimientos y herramientas empleadas durante los procesos de evaluación de seguridad. La ejecución de pruebas de penetración, análisis de vulnerabilidades y simulación de ataques debe realizarse dentro de marcos normativos claramente definidos que permitan proteger los derechos de las organizaciones y de las personas involucradas.

En el contexto del Seminario Especializado Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team, el análisis del escenario SecureNova Labs permitió comprender la importancia de la legislación informática, la protección de datos personales y la ética profesional como elementos fundamentales para el ejercicio responsable de la ciberseguridad. Estos aspectos constituyen la base para garantizar que las actividades técnicas se desarrollen respetando los límites legales y los principios de integridad profesional.

Ley 1273 de 2009

La Ley 1273 de 2009 constituye uno de los principales referentes normativos en materia de delitos informáticos en Colombia. Esta ley incorporó al Código Penal Colombiano una serie de conductas relacionadas con la protección de la información y de los datos, estableciendo sanciones para quienes realicen accesos abusivos a sistemas informáticos, interceptación de

datos, daño informático, uso de software malicioso, hurto por medios informáticos y otras actividades que afecten la seguridad de la información (Congreso de la República de Colombia, 2009).

La importancia de esta norma radica en que proporciona el marco jurídico necesario para perseguir conductas que comprometan la seguridad de los sistemas de información. Dentro del escenario SecureNova Labs, las acciones asociadas a accesos no autorizados, elevación indebida de privilegios y posible extracción de información podrían constituir conductas sancionables si se ejecutaran en un entorno real sin autorización previa.

Asimismo, esta ley establece la necesidad de que los profesionales de ciberseguridad desarrollen sus actividades dentro de entornos autorizados y con fines legítimos, evitando cualquier acción que pueda ser interpretada como una conducta ilícita.

Ley 1581 de 2012 y Protección de Datos Personales

La Ley 1581 de 2012 establece las disposiciones generales para la protección de datos personales en Colombia. Su finalidad consiste en garantizar que toda persona tenga control sobre la información que la identifica y que esta sea tratada de manera adecuada por parte de organizaciones públicas y privadas.

Dentro de las operaciones de ciberseguridad, la protección de datos personales adquiere una relevancia especial debido a que los procesos de monitoreo, análisis de registros y gestión de incidentes pueden involucrar información sensible o confidencial. Por esta razón, resulta indispensable implementar medidas que garanticen la privacidad y el adecuado tratamiento de los datos recolectados durante las actividades de seguridad.

En el escenario analizado, cualquier información obtenida durante las actividades de evaluación debería ser utilizada exclusivamente para los fines autorizados dentro del ejercicio académico, evitando su divulgación o uso indebido.

Código de Ética Profesional del COPNIA

El Consejo Profesional Nacional de Ingeniería (COPNIA) establece principios éticos que orientan el ejercicio responsable de las profesiones relacionadas con la ingeniería y la tecnología. Estos principios promueven valores como la integridad, la honestidad, la responsabilidad, la competencia profesional y el respeto por la normatividad vigente

Los profesionales que desarrollan actividades relacionadas con la ciberseguridad deben actuar bajo criterios éticos que garanticen el uso adecuado de sus conocimientos técnicos. La capacidad para identificar vulnerabilidades o comprometer sistemas implica una alta responsabilidad profesional, ya que estas habilidades podrían ser utilizadas de manera inapropiada si no existen principios éticos sólidos.

Durante el desarrollo del seminario se evidenció la importancia de actuar dentro de límites claramente definidos, respetando las autorizaciones otorgadas y evitando cualquier acción que exceda el alcance permitido del ejercicio.

Acuerdo de Confidencialidad y Responsabilidad Profesional

La confidencialidad constituye uno de los principios fundamentales dentro de las operaciones de ciberseguridad. Los profesionales encargados de realizar evaluaciones de seguridad suelen tener acceso a información sensible relacionada con sistemas, procesos y activos organizacionales, por lo que deben garantizar la protección de dicha información.

En el análisis desarrollado durante las etapas anteriores se identificaron aspectos relevantes relacionados con acuerdos de confidencialidad y responsabilidades profesionales. Estos acuerdos tienen como finalidad establecer límites claros respecto al uso de la información obtenida durante las actividades de evaluación, evitando su divulgación no autorizada o utilización con fines distintos a los previamente establecidos.

El incumplimiento de estos compromisos puede generar consecuencias legales, disciplinarias y reputacionales tanto para el profesional como para la organización involucrada.

Reglas de Enfrentamiento (Rules of Engagement – RoE)

Las Reglas de Enfrentamiento, conocidas como Rules of Engagement (RoE), constituyen un conjunto de directrices que establecen los límites, restricciones y procedimientos aplicables durante la ejecución de pruebas de seguridad. Estas reglas permiten definir claramente qué actividades están autorizadas, cuáles son los activos que pueden ser evaluados y qué acciones deben evitarse para no afectar la operación de los sistemas.

La existencia de unas Reglas de Enfrentamiento adecuadamente definidas contribuye a minimizar riesgos y garantiza que las actividades de evaluación se desarrollen de forma controlada y segura. Además, proporcionan un marco de referencia para resolver posibles situaciones de conflicto que puedan surgir durante la ejecución de las pruebas.

En el caso de SecureNova Labs, las actividades desarrolladas estuvieron limitadas al entorno académico establecido por el seminario, garantizando que todas las acciones realizadas se mantuvieran dentro de los objetivos definidos para el ejercicio

Importancia de la Ética en las Operaciones de Ciberseguridad

La ética constituye un elemento esencial dentro de cualquier actividad relacionada con la seguridad informática. Los profesionales de ciberseguridad tienen acceso a herramientas y conocimientos que podrían utilizarse tanto para proteger como para comprometer sistemas de información. Por esta razón, resulta indispensable actuar bajo principios de responsabilidad, transparencia y respeto por la legalidad.

La formación ética permite comprender que el objetivo de las actividades de seguridad no consiste únicamente en identificar vulnerabilidades, sino también en contribuir al fortalecimiento de los controles y a la protección de los activos organizacionales. Asimismo, promueve una

cultura profesional orientada a la prevención de riesgos y al uso responsable de las capacidades técnicas adquiridas.

El desarrollo del seminario permitió reforzar la importancia de integrar consideraciones éticas y legales dentro de todas las fases de una operación de ciberseguridad. En el entorno SecureNova Labs, las actividades de reconocimiento, análisis y validación de vulnerabilidades fueron ejecutadas exclusivamente sobre sistemas previamente autorizados y dentro de un entorno controlado, garantizando el cumplimiento de los principios de legalidad, confidencialidad y uso responsable de las herramientas empleadas. Asimismo, la obtención y documentación de evidencias técnicas se realizó únicamente con fines académicos, respetando los límites establecidos para las pruebas de seguridad y evitando cualquier afectación sobre sistemas reales o información de terceros. Análisis del Riesgo Residual.

Estos principios garantizan que las actividades de seguridad se desarrollen dentro de marcos legales y profesionales claramente establecidos (Casey, 2011).

Desarrollo de las Actividades Red Team

Las actividades desarrolladas desde la perspectiva Red Team tuvieron como propósito evaluar la seguridad del entorno propuesto por SecureNova Labs mediante la aplicación de técnicas de reconocimiento, análisis y validación de vulnerabilidades. Estas acciones permitieron identificar posibles debilidades presentes en los sistemas evaluados y determinar el nivel de exposición frente a amenazas potenciales.

El ejercicio práctico fue ejecutado siguiendo una metodología estructurada que permitió recopilar información sobre los sistemas analizados, identificar servicios expuestos, detectar vulnerabilidades y evaluar los riesgos asociados a dichas debilidades. Todas las actividades fueron realizadas dentro de un entorno controlado y con fines exclusivamente académicos.

Metodología Aplicada Durante el Ejercicio Red Team

Con el propósito de representar de manera gráfica las actividades realizadas durante el laboratorio, la Figura 1 presenta la secuencia metodológica utilizada durante la evaluación de seguridad.

Figura 1

Metodología aplicada durante las actividades Red Team

Nota. Se presenta el flujo metodológico desarrollado durante las actividades Red Team ejecutadas en el entorno SecureNova Labs. El proceso incluye las fases de reconocimiento,

descubrimiento de hosts, escaneo de puertos, enumeración de servicios, identificación y validación de vulnerabilidades, análisis de resultados y elaboración del informe técnico. Elaboración propia (2026).

La metodología aplicada permitió desarrollar de forma organizada cada una de las etapas del proceso de evaluación de seguridad, facilitando la obtención de evidencias técnicas y la identificación de hallazgos relevantes para el análisis posterior.

Reconocimiento y Descubrimiento de Activos

La fase inicial estuvo orientada a identificar los dispositivos presentes dentro del entorno de laboratorio. Para ello se realizaron actividades de reconocimiento y descubrimiento de hosts con el fin de determinar qué sistemas se encontraban activos y disponibles para la evaluación.

Durante esta etapa se verificó la conectividad entre las máquinas virtuales configuradas para el ejercicio y se identificaron los activos que conformaban el escenario de análisis. La información obtenida permitió establecer el alcance técnico de las pruebas posteriores.

Escaneo y Enumeración de Servicios

Una vez identificados los sistemas activos, se procedió a realizar actividades de escaneo de puertos y enumeración de servicios con el propósito de conocer los servicios expuestos y las características técnicas de los sistemas evaluados.

Los resultados obtenidos permitieron identificar protocolos activos, puertos abiertos y versiones asociadas a determinados servicios. Esta información fue fundamental para correlacionar los hallazgos con bases de datos de vulnerabilidades conocidas y determinar posibles vectores de ataque.

Identificación y Validación de Vulnerabilidades

A partir de la información recopilada durante las fases anteriores se efectuó el análisis de vulnerabilidades presentes en el sistema objetivo. Como resultado se identificó una

vulnerabilidad crítica asociada al protocolo SMB, correspondiente al boletín de seguridad MS17-010.

La validación de esta vulnerabilidad se realizó dentro del entorno académico controlado, permitiendo confirmar la existencia de la debilidad y evaluar el riesgo potencial que representa para los sistemas afectados. Este análisis evidenció la importancia de implementar procesos adecuados de gestión de vulnerabilidades y actualización de sistemas.

La identificación y priorización de vulnerabilidades puede apoyarse en marcos de referencia reconocidos internacionalmente, como OWASP Top 10, los cuales proporcionan lineamientos para la gestión de riesgos asociados a debilidades de seguridad comúnmente explotadas por atacantes (OWASP, 2021).

Resultados Obtenidos Durante la Evaluación

Con el propósito de consolidar los hallazgos identificados durante las actividades Red Team, la Tabla 1 presenta los principales resultados obtenidos durante las diferentes fases de la evaluación.

Tabla 1

Resultados obtenidos durante las actividades Red Team

Actividad	**Herramienta utilizada**	**Resultado obtenido**
Descubrimiento de hosts	Netdiscover	Identificación de equipos activos dentro de la red de laboratorio
Escaneo de puertos	Nmap	Identificación de puertos abiertos y servicios expuestos

Enumeración de servicios	Nmap NSE	Obtención de información detallada sobre versiones y protocolos activos
Análisis de vulnerabilidades	Nmap Scripts y CVE	Identificación de vulnerabilidades asociadas al servicio SMB
Validación de vulnerabilidades	Metasploit Framework	Confirmación de la exposición del sistema frente a MS17-010

Nota. Resultados obtenidos durante las actividades de reconocimiento, enumeración y validación realizadas en el entorno SecureNova Labs. Elaboración propia (2026)

La información recopilada permitió identificar debilidades relevantes en la configuración de los sistemas evaluados y proporcionó evidencia suficiente para realizar el análisis de riesgos correspondiente.

Vulnerabilidades Identificadas

Los hallazgos identificados durante la evaluación permitieron establecer las vulnerabilidades con mayor impacto potencial sobre la seguridad de la infraestructura analizada.

Tabla 2

Vulnerabilidades identificadas durante la evaluación técnica

Vulnerabilidad	**Servicio afectado**	**Nivel de riesgo**	**Método de identificación**
MS17-010	SMB	Crítico	Escaneo y validación mediante herramientas de análisis
SMBv1 habilitado	Compartición de archivos	Alto	Enumeración de servicios

Configuración insegura de servicios	Servicios de red expuestos	Medio	Escaneo de puertos y análisis de configuración

Nota. Vulnerabilidades identificadas durante las actividades de análisis de seguridad desarrolladas en el laboratorio. Elaboración propia (2026).

La vulnerabilidad MS17-010 fue considerada el hallazgo más relevante debido a su criticidad y al impacto que históricamente ha tenido en múltiples incidentes de seguridad a nivel mundial.

Análisis del Impacto sobre la Tríada CIA

Con el fin de evaluar el impacto potencial de los hallazgos identificados, se realizó un análisis basado en los principios de confidencialidad, integridad y disponibilidad de la información.

Tabla 3

Evaluación del impacto sobre la seguridad de la información.

Componente	**Impacto identificado**	**Nivel de impacto**
Confidencialidad	Posible acceso no autorizado a información sensible	Alto
Integridad	Riesgo de modificación no autorizada de datos	Alto
Disponibilidad	Posible interrupción de servicios mediante explotación de vulnerabilidades	Medio

Nota. Evaluación del impacto potencial de las vulnerabilidades identificadas sobre los principios fundamentales de la seguridad de la información. Elaboración propia (2026).

Los resultados evidencian que la explotación exitosa de las vulnerabilidades identificadas podría afectar significativamente la protección de los activos de información de una organización.

Limitaciones Encontradas Durante el Laboratorio

Como parte del análisis técnico, también se identificaron algunas limitaciones asociadas al entorno de laboratorio y a las condiciones propias del ejercicio académico.

Tabla 4

Limitaciones identificadas durante la ejecución de las actividades Red Team.

Limitación	**Descripción**	**Impacto sobre la evaluación**
Restricciones propias del laboratorio	El entorno fue diseñado con fines académicos y alcance controlado	Bajo
Alcance limitado de validación	Algunas actividades avanzadas de post explotación no fueron ejecutadas	Medio
Condiciones del entorno virtualizado	La infraestructura utilizada difiere de escenarios empresariales reales	Bajo

Nota. Limitaciones identificadas durante la ejecución de las pruebas de seguridad desarrolladas en el entorno SecureNova Labs. Elaboración propia (2026).

A pesar de las limitaciones identificadas, los resultados obtenidos permitieron cumplir los objetivos planteados para la evaluación, facilitando la comprensión de las diferentes fases de una

operación Red Team y fortaleciendo las competencias técnicas relacionadas con el análisis ofensivo de sistemas informáticos.

Desarrollo de las Actividades Blue Team

Las actividades desarrolladas desde la perspectiva Blue Team estuvieron orientadas a la identificación, análisis y respuesta frente a los eventos de seguridad detectados durante el escenario SecureNova Labs. El objetivo principal consistió en comprender cómo una organización puede detectar actividades sospechosas, analizar evidencias digitales y aplicar medidas de mitigación para reducir el impacto de un posible incidente de seguridad.

El enfoque Blue Team permitió complementar las actividades ofensivas desarrolladas por el Red Team, proporcionando una visión integral sobre la gestión de incidentes y el fortalecimiento de la postura de seguridad organizacional.

Metodología Aplicada Durante el Ejercicio Blue Team

Con el propósito de representar gráficamente las actividades desarrolladas durante el ejercicio, la Figura 2 presenta el flujo general seguido durante el análisis y respuesta ante el incidente de seguridad.

Figura 2

Metodología aplicada durante las actividades Blue Team.

Nota. Se presenta el flujo metodológico utilizado para la detección, análisis y respuesta ante incidentes de seguridad dentro del escenario SecureNova Labs. El proceso incluye las fases de detección del evento, recolección de evidencias, análisis de registros, identificación de indicadores de compromiso, contención, recuperación y fortalecimiento de controles de seguridad. Elaboración propia (2026).

La metodología permitió comprender las diferentes fases involucradas en la gestión de incidentes y la importancia de contar con procedimientos estructurados para responder de manera efectiva ante eventos de seguridad.

Identificación del Incidente

El análisis desarrollado permitió identificar indicios asociados a posibles actividades no autorizadas dentro del entorno evaluado. Estos eventos incluían la presencia de vulnerabilidades explotables y posibles accesos indebidos a recursos del sistema.

La detección temprana de estos eventos constituye uno de los principales objetivos de los equipos Blue Team, ya que permite reducir el tiempo de exposición frente a amenazas potenciales y facilita la implementación oportuna de medidas correctivas.

Análisis de Evidencias Digitales

Una vez identificado el posible incidente, se procedió a realizar el análisis de las evidencias disponibles. Este proceso incluyó la revisión de información obtenida durante las actividades de monitoreo, registros del sistema y resultados generados por las herramientas utilizadas durante la evaluación.

El análisis de evidencias permitió comprender mejor el comportamiento observado dentro del entorno y establecer relaciones entre los diferentes eventos detectados.

Indicadores de Compromiso (IoC)

Los Indicadores de Compromiso constituyen evidencias que permiten determinar la posible ocurrencia de actividades maliciosas dentro de un sistema o red. Durante el ejercicio se identificaron diversos elementos que podrían ser utilizados para apoyar futuras actividades de monitoreo y detección.

Tabla 5

Indicadores de compromiso identificados durante el análisis.

Indicador de compromiso	**Descripción**	**Fuente de identificación**
Servicio SMB vulnerable	Presencia de configuraciones asociadas a la vulnerabilidad MS17-010	Escaneo de vulnerabilidades
Puertos expuestos	Servicios accesibles desde la red sin restricciones adecuadas	Escaneo de puertos
Configuraciones inseguras	Servicios habilitados con configuraciones vulnerables	Enumeración de servicios
Sistemas desactualizados	Ausencia de parches y actualizaciones de seguridad	Análisis de vulnerabilidades
Protocolos heredados	Uso de SMBv1 dentro del entorno evaluado	Enumeración de servicios

Nota. Indicadores de compromiso identificados durante el análisis técnico realizado en el entorno SecureNova Labs. Elaboración propia (2026).

Proceso de Contención

Una vez identificadas las vulnerabilidades presentes en el sistema, se plantearon acciones de contención orientadas a reducir la exposición frente a posibles amenazas. Estas acciones incluyeron la restricción de servicios vulnerables, fortalecimiento de configuraciones y aplicación de controles de seguridad adicionales.

La contención constituye una de las fases más importantes dentro de la gestión de incidentes, ya que busca evitar que una amenaza continúe afectando los activos organizacionales.

Recuperación y Restablecimiento

Posteriormente se definieron actividades de recuperación orientadas a restablecer las condiciones seguras de operación de los sistemas evaluados. Estas acciones contemplaron la

aplicación de actualizaciones de seguridad, verificación de configuraciones y validación del correcto funcionamiento de los servicios.

La recuperación adecuada de un sistema comprometido permite reducir la probabilidad de reincidencia y fortalecer la resiliencia de la infraestructura tecnológica.

Resultados del Análisis Blue Team

Los resultados obtenidos permitieron identificar oportunidades de mejora relacionadas con la gestión de vulnerabilidades, monitoreo de eventos y fortalecimiento de controles de seguridad.

Tabla 6

Resultados obtenidos durante las actividades Blue Team

Actividad	**Resultado obtenido**	**Beneficio para la organización**
Identificación de vulnerabilidades	Detección de debilidades críticas en servicios expuestos	Reducción del riesgo de explotación
Análisis de evidencias	Correlación de eventos e identificación de riesgos	Mayor capacidad de investigación
Identificación de IoC	Definición de indicadores de monitoreo	Detección temprana de amenazas
Contención	Propuesta de acciones para reducir la exposición	Minimización del impacto potencial
Recuperación	Definición de medidas para restablecer condiciones seguras	Continuidad operativa

Fortalecimiento de controles	Identificación de mejoras de seguridad	Incremento de la madurez de seguridad

Nota. Resultados obtenidos durante las actividades Blue Team desarrolladas en el entorno de laboratorio. Elaboración propia (2026).

La detección, análisis y respuesta a incidentes forman parte de los procesos fundamentales de las operaciones defensivas de ciberseguridad (Scarfone & Mell, 2007).

Fortalecimiento de los Controles de Seguridad

El proceso de evaluación permitió evidenciar oportunidades de mejora en áreas críticas de la seguridad, especialmente en la administración de vulnerabilidades, la actualización tecnológica, la supervisión permanente de eventos y la segmentación adecuada de la infraestructura de red.

La implementación de estos controles contribuiría a reducir significativamente la superficie de ataque y mejorar la capacidad de detección y respuesta frente a futuras amenazas. Asimismo, permitiría incrementar el nivel de madurez de seguridad de la organización y fortalecer la protección de sus activos de información.

Medidas de Contención Aplicadas

Una vez identificadas las vulnerabilidades presentes en el entorno de laboratorio, se definieron diversas medidas de contención orientadas a reducir la superficie de ataque y minimizar la probabilidad de explotación por parte de actores maliciosos. Estas acciones se fundamentan en buenas prácticas de ciberseguridad y en los principios de defensa en profundidad, los cuales buscan implementar múltiples capas de protección para salvaguardar los activos de información.

Las medidas propuestas están enfocadas principalmente en la restricción de servicios vulnerables, la reducción de accesos innecesarios y el fortalecimiento de los mecanismos de control de red. La Tabla 7 presenta las principales acciones de contención identificadas durante el análisis realizado.

Tabla 7

Medidas de contención propuestas para el entorno analizado

Medida de contención	**Objetivo**	**Beneficio esperado**
Restricción de servicios vulnerables	Reducir vectores de ataque	Menor exposición a amenazas
Deshabilitación de SMBv1	Eliminar protocolos inseguros	Reducción del riesgo de explotación
Aplicación de reglas de firewall	Limitar accesos no autorizados	Mayor control del tráfico de red
Segmentación de red	Restringir movimientos laterales	Contención de incidentes
Monitoreo continuo	Detectar actividades sospechosas	Respuesta más rápida ante eventos

Nota. Medidas de contención definidas a partir de los hallazgos obtenidos durante el análisis del entorno SecureNova Labs. Elaboración propia (2026).

Posteriormente, se evaluó el impacto esperado de cada medida, determinando que su implementación contribuiría significativamente a disminuir la exposición frente a amenazas conocidas y a fortalecer la capacidad de respuesta ante incidentes de seguridad dentro de la organización.

Acciones de Recuperación y Fortalecimiento

Después de aplicar las medidas de contención, resulta fundamental establecer actividades orientadas a la recuperación de los sistemas y al fortalecimiento permanente de la infraestructura tecnológica. Estas acciones tienen como objetivo restaurar las condiciones seguras de operación, corregir las debilidades identificadas y prevenir la ocurrencia de incidentes similares en el futuro.

El proceso de recuperación no solo contempla la aplicación de actualizaciones y correcciones técnicas, sino también la implementación de controles de monitoreo, programas de capacitación y mecanismos de mejora continua que permitan incrementar el nivel de madurez de seguridad organizacional. En la Tabla 8 se presentan las principales acciones recomendadas para la recuperación y fortalecimiento de los sistemas evaluados.

Tabla 8

Acciones de recuperación y fortalecimiento de la seguridad

Acción recomendada	**Descripción**	**Impacto esperado**
Aplicación de parches de seguridad	Actualización de sistemas vulnerables	Eliminación de vulnerabilidades conocidas
Actualización de protocolos	Sustitución de protocolos obsoletos	Incremento de la seguridad
Implementación de monitoreo centralizado	Consolidación de eventos de seguridad	Mejor visibilidad de amenazas
Capacitación del personal	Fortalecimiento de la cultura de seguridad	Reducción de errores humanos
Revisión periódica de vulnerabilidades	Evaluaciones continuas de seguridad	Mejora continua de los controles

Nota. Acciones recomendadas para la recuperación y fortalecimiento de la infraestructura tecnológica analizada. Elaboración propia (2026).

La implementación de estas acciones permitiría mejorar la resiliencia de la infraestructura tecnológica frente a amenazas emergentes, fortalecer los procesos de gestión de vulnerabilidades y optimizar la capacidad de detección y respuesta ante futuros incidentes de seguridad.

Herramientas Utilizadas Durante el Seminario

El desarrollo de las prácticas académicas demandó el uso de diferentes soluciones tecnológicas especializadas en reconocimiento de redes, análisis de vulnerabilidades, validación de configuraciones inseguras y ejecución controlada de pruebas de seguridad. Estas herramientas permitieron desarrollar las actividades prácticas planteadas en cada una de las etapas del curso y facilitaron la obtención de evidencias técnicas para el análisis de resultados.

La selección de las herramientas respondió a criterios de funcionalidad, reconocimiento dentro de la comunidad de ciberseguridad y aplicabilidad en entornos de laboratorio controlados. Su utilización permitió comprender tanto las capacidades ofensivas asociadas a las operaciones Red Team como las actividades defensivas relacionadas con los equipos Blue Team

Herramientas Empleadas Durante las Actividades Prácticas

La Tabla 9 presenta las principales herramientas utilizadas durante el desarrollo del seminario, así como su propósito y contribución dentro de las actividades realizadas.

Tabla 9

Herramientas utilizadas durante el Seminario Especializado en Ciberseguridad.

Herramienta	**Tipo**	**Función principal**	**Aplicación dentro del seminario**

Kali Linux	Sistema operativo	Plataforma especializada para pruebas de seguridad	Entorno principal para las actividades Red Team
Nmap	Escáner de red	Descubrimiento de hosts y análisis de puertos	Reconocimiento y enumeración de servicios
Netdiscover	Descubrimiento de red	Identificación de dispositivos activos	Identificación de hosts dentro del laboratorio
Metasploit Framework	Framework de explotación	Validación de vulnerabilidades	Análisis de la vulnerabilidad MS17-010
VirtualBox	Virtualización	Creación y administración de máquinas virtuales	Implementación del entorno de laboratorio
Windows 7 Host-A	Sistema objetivo	Equipo vulnerable del escenario	Evaluación de vulnerabilidades
Host-B	Sistema complementario	Simulación de infraestructura organizacional	Validación de conectividad y análisis de red

Nota. Herramientas utilizadas durante las actividades prácticas desarrolladas en el Seminario Especializado en Ciberseguridad. Elaboración propia (2026).

Las herramientas empleadas permitieron ejecutar cada una de las fases contempladas en el ejercicio práctico, desde la identificación de activos hasta la validación de vulnerabilidades y el análisis de los resultados obtenidos.

Relación de Herramientas con las Fases del Ejercicio

Con el fin de representar la relación entre las herramientas empleadas y las actividades ejecutadas en el laboratorio, la Tabla 10 presenta la relación existente entre cada herramienta y las fases metodológicas ejecutadas durante las actividades Red Team y Blue Team.

Tabla 10

Relación entre herramientas y fases del ejercicio práctico

Fase	**Herramienta principal**	**Objetivo**
Reconocimiento	Netdiscover	Descubrir dispositivos activos
Escaneo	Nmap	Identificar puertos y servicios
Enumeración	Nmap NSE	Obtener información detallada de servicios
Análisis de vulnerabilidades	Nmap Scripts	Detectar vulnerabilidades conocidas
Validación	Metasploit Framework	Verificar vulnerabilidades identificadas
Monitoreo y análisis	Herramientas de sistema	Revisar eventos y evidencias
Documentación	Microsoft Word	Elaboración de informes técnicos

Nota. Relación entre las herramientas utilizadas y las fases desarrolladas durante el laboratorio práctico. Elaboración propia (2026).

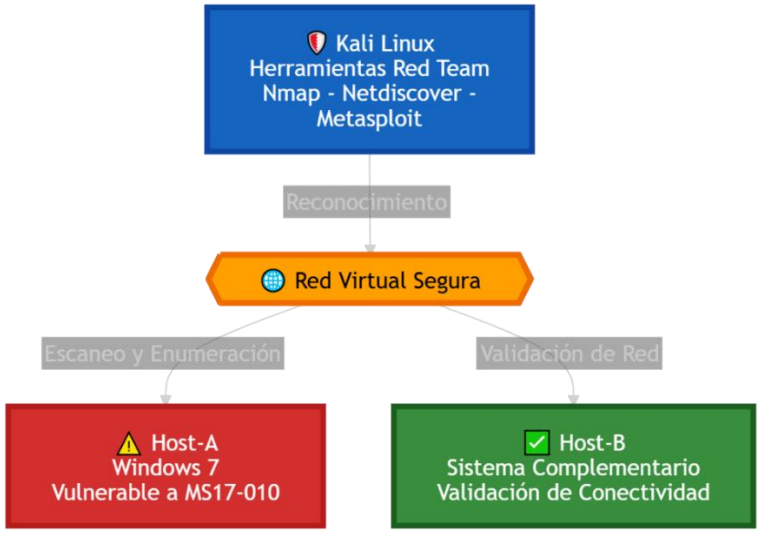
El uso combinado de las herramientas seleccionadas facilitó la ejecución ordenada de cada fase del proceso de evaluación de seguridad, facilitando la obtención de evidencias técnicas y el análisis integral del entorno evaluado.

Representación del Entorno Tecnológico Utilizado

Para comprender la interacción entre los diferentes componentes empleados durante el laboratorio, la Figura 3 presenta la arquitectura general del entorno utilizado durante las actividades prácticas.

Figura 3

Arquitectura general del entorno de laboratorio



Nota. Se presenta la arquitectura lógica implementada en el entorno virtualizado de SecureNova Labs. El escenario estuvo compuesto por una estación Kali Linux utilizada para las actividades Red Team, una red virtual controlada y dos equipos objetivo-empleados para la validación de vulnerabilidades, análisis de conectividad y ejecución de pruebas de seguridad. Elaboración propia (2026).

La arquitectura implementada permitió simular un entorno de red controlado en el que fue posible desarrollar actividades de reconocimiento, análisis y validación de vulnerabilidades sin afectar sistemas reales.

Valor de las Herramientas en el Aprendizaje del Seminario

La utilización de soluciones tecnológicas especializadas favoreció el desarrollo de habilidades prácticas relacionadas con la identificación y gestión de riesgos de seguridad. Asimismo, facilitó la comprensión de metodologías utilizadas en entornos profesionales de ciberseguridad y permitió integrar conocimientos teóricos con actividades prácticas desarrolladas dentro del laboratorio académico. Este tipo de formación práctica fortalece las capacidades necesarias para implementar controles de seguridad y desarrollar una visión integral de la protección de los sistemas de información, tal como lo plantean Manson et al. (2014). De igual manera, el uso de entornos basados en Linux, como Kali Linux, proporciona una plataforma adecuada para el aprendizaje y la ejecución de herramientas orientadas al análisis de seguridad y pruebas controladas de vulnerabilidades (OccupyTheWeb, 2021).

Análisis Técnico de Resultados

Consolidación de los Hallazgos Técnicos

El análisis realizado sobre el entorno SecureNova Labs permitió consolidar un conjunto de hallazgos que evidencian debilidades significativas en la postura de seguridad del sistema evaluado. La identificación de servicios expuestos, configuraciones inseguras, protocolos obsoletos y ausencia de actualizaciones demuestra que las vulnerabilidades detectadas no corresponden a eventos aislados, sino a deficiencias en los procesos de gestión de vulnerabilidades y administración de la infraestructura tecnológica.

La correlación de la información obtenida mediante las actividades de reconocimiento, enumeración y validación permitió construir una visión integral del estado de seguridad del entorno, facilitando la identificación de relaciones entre los activos expuestos, los servicios ejecutados y las posibles rutas de explotación. Este enfoque evidencia la importancia de analizar

los hallazgos de manera conjunta, ya que la combinación de varias debilidades incrementa considerablemente el nivel de riesgo al que se encuentra expuesta una organización.

Desde una perspectiva organizacional, los resultados obtenidos ponen de manifiesto la necesidad de establecer procesos permanentes de gestión del riesgo, orientados a la identificación temprana, priorización y tratamiento de vulnerabilidades antes de que puedan ser aprovechadas por un atacante. La ausencia de estos procesos incrementa la probabilidad de incidentes de seguridad que afecten la confidencialidad, integridad y disponibilidad de la información, además de comprometer la continuidad operativa y generar impactos económicos, legales y reputacionales. Este enfoque coincide con los principios de la seguridad de la información, que promueven la gestión continua de riesgos y la implementación de controles como elementos esenciales para la protección de los activos de información (Kim & Solomon, 2018).

En consecuencia, los hallazgos identificados no solo representan evidencia técnica de las debilidades presentes en el entorno evaluado, sino que también constituyen un insumo para la toma de decisiones relacionadas con el fortalecimiento de los controles de seguridad, la planificación de acciones correctivas y la mejora continua de la postura de ciberseguridad de la organización.

Evidencias Técnicas de Validación de Vulnerabilidades

Durante la fase de reconocimiento se identificó que el host objetivo tenía expuesto el servicio SMB sobre el puerto TCP 445. Mediante el uso de Nmap y scripts NSE orientados a la detección de vulnerabilidades, se obtuvo evidencia de la presencia de la vulnerabilidad MS17-010 (EternalBlue), asociada a sistemas Windows que no cuentan con las actualizaciones de seguridad correspondientes.

Los resultados obtenidos durante el escaneo permitieron identificar la presencia de los puertos 135/TCP (MSRPC), 139/TCP (NetBIOS-SSN) y 445/TCP (Microsoft-DS), servicios comúnmente utilizados en entornos Windows para la comunicación y compartición de recursos. Asimismo, Nmap identificó el sistema objetivo como Windows 7 Professional SP1, versión que históricamente ha sido afectada por la vulnerabilidad EternalBlue cuando no dispone de los parches de seguridad publicados por Microsoft. La evidencia técnica correspondiente al proceso de reconocimiento y enumeración puede consultarse en el Apéndice C.

La identificación de estos servicios y protocolos de red permitió comprender la importancia de su adecuada configuración y administración dentro de la infraestructura tecnológica, ya que constituyen elementos fundamentales para la comunicación entre sistemas y, cuando presentan vulnerabilidades o configuraciones inseguras, pueden convertirse en puntos de entrada para ataques informáticos (Tanenbaum & Wetherall, 2013).

La validación realizada permitió confirmar que el servicio SMBv1 se encontraba habilitado, condición que incrementa significativamente la superficie de ataque del sistema. La vulnerabilidad MS17-010 afecta precisamente este protocolo y permite la ejecución remota de código mediante el envío de paquetes especialmente diseñados hacia el servicio expuesto. Esta vulnerabilidad adquirió relevancia mundial al ser utilizada por amenazas como WannaCry para comprometer miles de sistemas a nivel global.

Desde una perspectiva técnica, la explotación exitosa de esta vulnerabilidad podría permitir a un atacante obtener acceso no autorizado al sistema afectado, ejecutar código arbitrario, instalar software malicioso, comprometer la confidencialidad de la información almacenada y utilizar el equipo comprometido como punto de partida para movimientos laterales dentro de la red.

La validación controlada mediante Metasploit permitió verificar la presencia de condiciones compatibles con la vulnerabilidad MS17-010 sin generar afectaciones sobre el entorno de laboratorio. Los resultados obtenidos evidenciaron el nivel de exposición existente y permitieron confirmar el riesgo asociado al servicio vulnerable identificado durante las fases previas de reconocimiento y análisis. La evidencia técnica correspondiente al proceso de validación puede consultarse en el Apéndice D.

La correlación de la información obtenida mediante Nmap y Metasploit permitió confirmar la existencia de una vulnerabilidad crítica asociada a sistemas desactualizados y protocolos obsoletos. Estos resultados evidencian la importancia de mantener procesos permanentes de gestión de vulnerabilidades, aplicación de parches de seguridad y revisión continua de configuraciones con el fin de reducir la probabilidad de compromiso de la infraestructura tecnológica.

Más allá de la validación técnica de la vulnerabilidad, los resultados obtenidos permiten evidenciar la necesidad de que las organizaciones adopten un enfoque preventivo para la administración de sus activos tecnológicos. La permanencia de vulnerabilidades críticas como MS17-010 refleja deficiencias en los procesos de gestión de parches, inventario de activos y seguimiento del ciclo de vida de los sistemas operativos. En un entorno corporativo, este tipo de debilidades podría facilitar ataques de ejecución remota de código, comprometer información crítica y favorecer movimientos laterales dentro de la red, incrementando el impacto operativo del incidente. Por ello, la identificación temprana de estas vulnerabilidades debe traducirse en decisiones orientadas al fortalecimiento de los controles de seguridad y a la reducción del riesgo organizacional.

Herramientas como Nmap y Metasploit son ampliamente utilizadas para la identificación, validación y documentación de vulnerabilidades en ejercicios controlados de seguridad ofensiva (Weidman, 2014).

Reconocimiento y Enumeración de Servicios

Durante la fase de reconocimiento se identificó el host objetivo con dirección IP 192.168.10.20 mediante las herramientas Netdiscover y Nmap. El proceso permitió confirmar la disponibilidad del sistema dentro de la red virtual y establecer la base para las actividades posteriores de enumeración y análisis de vulnerabilidades.

Posteriormente, mediante el escaneo de servicios realizado con Nmap, se identificaron múltiples puertos abiertos asociados a servicios de Microsoft Windows, entre ellos 135/TCP (MSRPC), 139/TCP (NetBIOS-SSN) y 445/TCP (Microsoft-DS). La exposición del puerto 445 resultó especialmente relevante debido a que corresponde al protocolo SMB, servicio directamente relacionado con la vulnerabilidad MS17-010 identificada durante el ejercicio práctico.

La información obtenida durante la fase de reconocimiento demuestra que el proceso de enumeración de servicios constituye una actividad estratégica dentro de cualquier evaluación de seguridad, ya que permite identificar activos expuestos y priorizar aquellos que representan un mayor nivel de riesgo. Desde la perspectiva de la gestión del riesgo, conocer los servicios disponibles y su estado de actualización facilita la toma de decisiones para implementar controles preventivos antes de que las vulnerabilidades sean explotadas. Asimismo, evidencia la importancia de mantener inventarios actualizados de activos y realizar revisiones periódicas de la superficie de ataque de la organización.

Clasificación de los Hallazgos Identificados

Con el propósito de priorizar las vulnerabilidades detectadas, se realizó una clasificación basada en el nivel de riesgo asociado a cada hallazgo.

Tabla 11

Clasificación de hallazgos identificados durante la evaluación

Hallazgo	**Descripción**	**Criticidad**
Vulnerabilidad MS17-010	Posibilidad de ejecución remota de código mediante SMB	Crítica
Uso de SMBv1	Protocolo heredado con múltiples vulnerabilidades conocidas	Alta
Servicios expuestos	Puertos accesibles desde la red sin restricciones suficientes	Media
Configuraciones inseguras	Servicios habilitados sin endurecimiento adecuado	Media
Ausencia de actualizaciones	Sistemas sin aplicación de parches recientes	Alta

Nota. Clasificación realizada con base en el impacto potencial de los hallazgos identificados durante las actividades prácticas. Elaboración propia (2026).

El análisis técnico realizado permitió determinar que la vulnerabilidad MS17-010 constituye el hallazgo con mayor nivel de criticidad.

El análisis técnico permitió determinar que la vulnerabilidad MS17-010 constituye el hallazgo de mayor criticidad debido a su alta probabilidad de explotación y al impacto que podría generar sobre la infraestructura tecnológica. Sin embargo, la evaluación también

evidenció que el riesgo organizacional no depende exclusivamente de una vulnerabilidad crítica, sino de la acumulación de múltiples debilidades, como la permanencia de protocolos obsoletos, configuraciones inseguras y la ausencia de actualizaciones. La coexistencia de estos factores incrementa la superficie de ataque y favorece escenarios en los que un atacante puede combinar diferentes técnicas para comprometer los activos de información, lo que hace indispensable establecer un proceso continuo de priorización y tratamiento de riesgos.

Análisis de Riesgo Asociado a las Vulnerabilidades

La valoración del riesgo facilita la estimación de la posibilidad de explotación y de las consecuencias asociadas a cada vulnerabilidad identificada y el impacto potencial que podría generar sobre los activos de información de una organización. Para este ejercicio se consideraron factores como facilidad de explotación, nivel de exposición y consecuencias potenciales sobre los sistemas evaluados.

Tabla 12

Evaluación de riesgo de las vulnerabilidades identificadas

Vulnerabilidad	**Probabilidad**	**Impacto**	**Nivel de riesgo**
MS17-010	Alta	Muy alto	Crítico
SMBv1 habilitado	Alta	Alto	Alto
Servicios expuestos	Media	Medio	Medio
Configuraciones inseguras	Media	Medio	Medio
Falta de actualizaciones	Alta	Alto	Alto

Nota. Evaluación de riesgo realizada a partir de los hallazgos obtenidos durante las actividades de análisis de vulnerabilidades. Elaboración propia (2026).

Los resultados de la evaluación evidencian que las vulnerabilidades con mayor nivel de riesgo requieren una atención prioritaria dentro de cualquier estrategia de gestión de la seguridad. En particular, la presencia de MS17-010 y de protocolos heredados como SMBv1 demuestra que la falta de actualización tecnológica incrementa significativamente la probabilidad de explotación por parte de actores maliciosos. Desde la perspectiva de la gestión del riesgo, estos hallazgos justifican la implementación inmediata de acciones de mitigación, como la aplicación de parches de seguridad, el endurecimiento de configuraciones y la eliminación de servicios obsoletos. Asimismo, ponen de manifiesto la necesidad de mantener procesos permanentes de monitoreo, evaluación y mejora continua que permitan reducir la exposición de la organización frente a amenazas emergentes.

Impacto de los Hallazgos sobre la Seguridad Organizacional

Cuando una organización mantiene vulnerabilidades sin remediar, incrementa significativamente la probabilidad de materialización de amenazas que pueden afectar la continuidad operativa, la protección de la información y el cumplimiento de sus objetivos estratégicos. Los hallazgos identificados durante la evaluación evidencian que la exposición de servicios críticos, el uso de protocolos obsoletos y la ausencia de una adecuada gestión de actualizaciones representan condiciones que pueden ser aprovechadas por actores maliciosos para obtener accesos no autorizados, comprometer la integridad de los datos e interrumpir la disponibilidad de los servicios tecnológicos.

Desde la perspectiva de la gestión del riesgo, estos resultados ponen de manifiesto la necesidad de fortalecer los procesos de identificación, evaluación y tratamiento de vulnerabilidades como parte de una estrategia integral de ciberseguridad. La presencia de debilidades críticas no solo refleja fallas técnicas, sino también oportunidades de mejora en la

gestión de activos, la administración de parches, el monitoreo continuo y la implementación de controles preventivos orientados a reducir la superficie de ataque.

Asimismo, el impacto de estas vulnerabilidades trasciende el ámbito tecnológico, ya que un incidente derivado de su explotación podría generar pérdidas económicas, afectaciones reputacionales, incumplimiento de obligaciones legales y regulatorias, interrupción de procesos críticos y disminución de la confianza de usuarios y demás partes interesadas. En este sentido, la evaluación realizada demuestra que la gestión de vulnerabilidades debe entenderse como un proceso estratégico que contribuye a fortalecer la resiliencia organizacional y a respaldar la toma de decisiones para la protección de los activos de información.

Análisis Integrado Red Team y Blue Team

Entre los aspectos más relevantes identificados durante el seminario se encuentra la interacción permanente entre las capacidades ofensivas y defensivas de la ciberseguridad. Mientras las actividades Red Team permitieron identificar y validar vulnerabilidades presentes en los sistemas evaluados, las actividades Blue Team facilitaron la detección, análisis y propuesta de medidas orientadas a la mitigación de los riesgos identificados.

La experiencia práctica demostró que la protección efectiva de los sistemas requiere tanto la identificación de vulnerabilidades como la capacidad de respuesta frente a incidentes, sino también de la capacidad organizacional para responder oportunamente a los incidentes y fortalecer continuamente sus controles de seguridad.

Tabla 13

Comparación de actividades Red Team y Blue Team

Hallazgo Red Team	**Riesgo identificado**	**Medida Blue Team**	**Resultado esperado**

MS17-010	Ejecución remota de código	Aplicación de parches	Eliminación de la vulnerabilidad
SMBv1 habilitado	Explotación remota	Deshabilitación de SMBv1	Reducción de superficie de ataque
Servicios expuestos	Acceso no autorizado	Firewall y segmentación	Restricción de accesos
Sistemas desactualizados	Compromiso del sistema	Gestión de parches	Disminución del riesgo
Falta de monitoreo	Detección tardía	SIEM y EDR	Mayor capacidad de detección

Nota. Relación entre los hallazgos identificados durante las actividades Red Team y las medidas de mitigación propuestas desde la perspectiva Blue Team. Elaboración propia (2026).

La integración de las actividades Red Team y Blue Team permitió transformar los hallazgos técnicos identificados durante el análisis en acciones concretas de mitigación y fortalecimiento de la seguridad. Los resultados obtenidos evidenciaron que la identificación temprana de vulnerabilidades, combinada con la implementación de controles defensivos adecuados, contribuye significativamente a la reducción del riesgo y al fortalecimiento de la postura de seguridad de la infraestructura tecnológica evaluada.

Lecciones Técnicas Derivadas del Análisis

La información recopilada durante las actividades prácticas permitió reconocer elementos clave para fortalecer la gestión de la ciberseguridad organizacional. Entre ellos se destacan la importancia de mantener actualizados los sistemas operativos, realizar evaluaciones periódicas

de vulnerabilidades, implementar mecanismos de monitoreo continuo y fortalecer los procesos de gestión de incidentes.

Asimismo, el ejercicio evidenció que muchas de las amenazas más críticas pueden originarse a partir de vulnerabilidades conocidas que no han sido corregidas oportunamente. Esto resalta la necesidad de adoptar enfoques preventivos orientados a la mejora continua de la seguridad.

Evaluación del Riesgo y Análisis de Impacto

La identificación de vulnerabilidades constituye únicamente una parte del proceso de gestión de la seguridad. Para determinar la prioridad de las acciones correctivas es necesario evaluar el nivel de riesgo asociado a cada hallazgo, considerando tanto la probabilidad de ocurrencia como el impacto potencial sobre los activos de información de la organización.

La evaluación efectuada sobre el entorno de laboratorio facilitó la clasificación y priorización de los riesgos detectados dentro del entorno SecureNova Labs, facilitando la priorización de medidas de mitigación y fortalecimiento de controles de seguridad.

Metodología de Evaluación del Riesgo

Para valorar los riesgos identificados se utilizaron criterios relacionados con la probabilidad de ocurrencia y el impacto potencial de cada vulnerabilidad. La probabilidad representa la posibilidad de que una vulnerabilidad sea explotada, mientras que el impacto corresponde a las consecuencias que dicha explotación podría generar sobre la organización.

La combinación de estos dos factores permitió determinar el nivel de riesgo asociado a cada vulnerabilidad identificada durante las actividades prácticas del seminario.

Matriz de Probabilidad e Impacto

La Tabla 14 presenta la escala utilizada para la valoración de los riesgos identificados durante el análisis técnico.

Tabla 14

Escala de evaluación de riesgos

Nivel	**Probabilidad**	**Impacto**
Muy Bajo	Poco probable	Consecuencias mínimas
Bajo	Baja posibilidad de ocurrencia	Impacto limitado
Medio	Ocurrencia moderada	Afectación parcial
Alto	Alta posibilidad de ocurrencia	Impacto significativo
Crítico	Muy probable	Impacto severo

Nota. Escala utilizada para la valoración de riesgos dentro del entorno de laboratorio.

Elaboración propia (2026).

La aplicación de esta escala permitió clasificar los hallazgos de acuerdo con su criticidad y establecer prioridades para la implementación de controles de seguridad.

Valoración de Riesgos Identificados

Con base en los resultados obtenidos durante el análisis de vulnerabilidades, se realizó la valoración de los principales riesgos identificados en el entorno evaluado.

Tabla 15

Valoración de riesgos identificados.

Vulnerabilidad	**Probabilidad**	**Impacto**	**Nivel de riesgo**
MS17-010	Alta	Crítico	Crítico
SMBv1 habilitado	Alta	Alto	Alto
Servicios expuestos	Media	Medio	Medio
Configuración insegura de servicios	Media	Medio	Medio

Sistemas desactualizados	Alta	Alto	Alto

Nota. Valoración de riesgos realizada a partir de los resultados obtenidos durante el ejercicio práctico. Elaboración propia (2026).

Los resultados muestran que la vulnerabilidad MS17-010 representa el riesgo más significativo dentro del entorno analizado debido a su facilidad de explotación y a las graves consecuencias que podría generar sobre la infraestructura tecnológica.

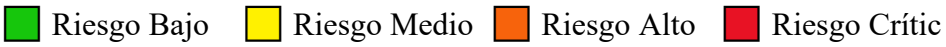
Mapa de Calor de Riesgos

Con el propósito de representar gráficamente los niveles de riesgo identificados durante la evaluación, la Figura presenta un mapa de calor basado en los criterios de probabilidad e impacto.

Figura 4

Mapa de calor de riesgos identificados.

Probabilidad / Impacto	**Muy Bajo**	**Bajo**	**Medio**	**Alto**	**Crítico**
Muy Alta					
Alta				SMBv1 Sistemas Desactualizados	MS17-010
Media			Servicios Expuestos Configuración Insegura		
Baja					
Muy Baja					



Nota. Mapa de calor construido a partir de la valoración de probabilidad e impacto de los hallazgos identificados durante la evaluación técnica del entorno SecureNova Labs. Elaboración propia (2026).

La representación gráfica evidencia que las vulnerabilidades vinculadas a MS17-010 y SMBv1 demandan una intervención inmediata debido a su nivel de criticidad.

Análisis del Riesgo Residual

Después de implementar las medidas de mitigación propuestas, el nivel de riesgo asociado a las vulnerabilidades identificadas puede reducirse significativamente. Sin embargo, es importante reconocer que ningún entorno tecnológico puede eliminar completamente todos los riesgos existentes.

El riesgo residual corresponde al nivel de riesgo que permanece después de aplicar controles de seguridad y medidas correctivas. Su gestión requiere monitoreo continuo, actualización permanente de sistemas y revisiones periódicas de seguridad.

Tabla 16

Evaluación del riesgo residual

Vulnerabilidad	**Riesgo inicial**	**Control aplicado**	**Riesgo residual**
MS17-010	Crítico	Aplicación de parches de seguridad	Bajo
SMBv1 habilitado	Alto	Deshabilitación de SMBv1	Bajo
Servicios expuestos	Medio	Firewall y segmentación de red	Bajo

Configuraciones inseguras	Medio	Endurecimiento de servicios	Bajo
Sistemas desactualizados	Alto	Gestión de actualizaciones	Medio

Nota. Evaluación del riesgo residual estimada después de la aplicación de las medidas de mitigación propuestas para el entorno SecureNova Labs. Elaboración propia (2026).

La evaluación del riesgo residual permitió estimar el nivel de exposición que permanecería después de la implementación de los controles de seguridad recomendados. Los resultados evidencian una reducción significativa de los riesgos inicialmente identificados, especialmente en las vulnerabilidades asociadas a MS17-010 y SMBv1. Sin embargo, algunos riesgos continúan requiriendo monitoreo permanente y procesos de mejora continua, debido a que la seguridad absoluta no puede garantizarse en ningún entorno tecnológico.

Priorización de Acciones Correctivas

A partir de la valoración de riesgos realizada, se definió un orden de prioridad para la implementación de medidas correctivas orientadas a reducir los riesgos identificados.

Tabla 17

Priorización de acciones de mitigación.

Prioridad	**Acción recomendada**	**Riesgo mitigado**
Alta	Aplicación de parches MS17-010	Crítico
Alta	Deshabilitación de SMBv1	Alto
Media	Restricción de servicios expuestos	Medio
Media	Endurecimiento de configuraciones	Medio
Baja	Optimización de políticas de monitoreo	Bajo

Nota. Priorización de acciones de mitigación establecida a partir de la valoración de riesgos realizada durante el ejercicio. Elaboración propia (2026).

La priorización permite orientar los esfuerzos organizacionales hacia aquellas acciones que generan una mayor reducción del riesgo y contribuyen de manera significativa al fortalecimiento de la seguridad.

Importancia de la Gestión de Riesgos en Ciberseguridad

La administración de riesgos representa un componente esencial dentro de cualquier estrategia de protección de la información, ya que permite identificar amenazas, evaluar vulnerabilidades y definir controles adecuados para proteger los activos organizacionales. Los resultados obtenidos durante el seminario evidencian que la correcta identificación y valoración de riesgos facilita la toma de decisiones y contribuye al fortalecimiento de la postura de seguridad institucional.

La integración de procesos de evaluación continua, monitoreo permanente y mejora de controles permite reducir significativamente la probabilidad de incidentes de seguridad y mejorar la resiliencia de las organizaciones frente a amenazas cada vez más sofisticadas.

La gestión de riesgos constituye uno de los componentes centrales del marco de ciberseguridad propuesto por el National Institute of Standards and Technology (NIST, 2024).

Comunicación de Resultados Técnicos

La utilidad de una evaluación de seguridad depende en gran medida de la capacidad para transformar los hallazgos técnicos en información comprensible y útil para quienes toman decisiones dentro de la organización. Una adecuada presentación de resultados facilita la comprensión de los riesgos identificados, la priorización de acciones correctivas y la implementación de estrategias orientadas al fortalecimiento de la seguridad institucional.

Durante el desarrollo del seminario se consolidaron los hallazgos obtenidos a través de las actividades Red Team y Blue Team, permitiendo generar una visión integral del estado de seguridad del entorno SecureNova Labs. Los resultados fueron organizados considerando las necesidades de los diferentes niveles organizacionales, desde la alta dirección hasta los equipos técnicos responsables de la administración de la infraestructura tecnológica.

Resumen Ejecutivo para la Alta Dirección

El análisis efectuado durante las prácticas permitió detectar vulnerabilidades de alta criticidad con potencial de afectar la seguridad de la infraestructura evaluada que podrían comprometer la confidencialidad, integridad y disponibilidad de la información almacenada en los sistemas evaluados. Entre los hallazgos más relevantes se destaca la presencia de la vulnerabilidad MS17-010, asociada al protocolo SMBv1, la cual representa un riesgo significativo debido a su potencial de explotación remota.

El análisis realizado permitió evidenciar la necesidad de fortalecer los procesos de gestión de vulnerabilidades, actualización de sistemas operativos, monitoreo continuo y aplicación de controles de seguridad orientados a reducir la superficie de ataque. Asimismo, se identificó la importancia de implementar estrategias de capacitación y concientización que contribuyan al fortalecimiento de la cultura organizacional de seguridad

Desde una perspectiva de gestión, los resultados obtenidos permiten concluir que la implementación de medidas preventivas y correctivas contribuiría significativamente a reducir el riesgo de incidentes de seguridad y mejorar la resiliencia tecnológica de la organización.

Reporte de Hallazgos para responsables de Seguridad

Con el propósito de facilitar la toma de decisiones por parte de los responsables de seguridad de la información, se consolidaron los principales hallazgos identificados durante el ejercicio práctico.

Tabla 18

Resumen ejecutivo de hallazgos identificado

Hallazgo	**Nivel de criticidad**	**Impacto potencial**	**Acción recomendada**
Vulnerabilidad MS17-010	Crítico	Compromiso total del sistema	Aplicar actualizaciones de seguridad
SMBv1 habilitado	Alto	Explotación de vulnerabilidades conocidas	Deshabilitar protocolo SMBv1
Sistemas desactualizados	Alto	Incremento de superficie de ataque	Implementar gestión de parches
Servicios expuestos	Medio	Acceso no autorizado	Restringir servicios innecesarios
Configuraciones inseguras	Medio	Exposición de recursos críticos	Aplicar endurecimiento de configuraciones

Nota. Resumen ejecutivo de hallazgos elaborado a partir de los resultados obtenidos durante las actividades Red Team y Blue Team. Elaboración propia (2026).

Los resultados permiten establecer una hoja de ruta para la implementación de acciones de mitigación orientadas a reducir los riesgos identificados y fortalecer la postura de seguridad institucional.

Comunicación de Resultados para Equipos Técnicos

Desde una perspectiva operativa, los resultados obtenidos durante la evaluación permiten identificar diversas oportunidades de mejora relacionadas con la administración de sistemas, gestión de vulnerabilidades y monitoreo de eventos de seguridad.

Los equipos técnicos responsables de la infraestructura tecnológica deben priorizar la aplicación de actualizaciones de seguridad, la eliminación de protocolos obsoletos y la implementación de mecanismos de monitoreo que permitan detectar oportunamente actividades sospechosas dentro de la red organizacional.

Adicionalmente, se recomienda realizar evaluaciones periódicas de vulnerabilidades y establecer procedimientos formales para la gestión de incidentes de seguridad, garantizando una respuesta oportuna ante posibles amenazas.

Representación del Flujo de Comunicación de Resultados

La Figura 5 presenta el proceso de comunicación de resultados implementado para la presentación de hallazgos y recomendaciones derivadas de la evaluación de seguridad.

Figura 5

Proceso de comunicación de resultados técnicos.

Nota. Flujo de comunicación utilizado para transformar los hallazgos técnicos obtenidos durante la evaluación en acciones orientadas a la gestión y fortalecimiento de la seguridad organizacional. Elaboración propia (2026).

El flujo de comunicación permitió transformar los hallazgos técnicos obtenidos durante las actividades de reconocimiento, análisis de vulnerabilidades y evaluación de riesgos en información útil para la toma de decisiones. Este proceso facilitó la priorización de acciones correctivas y la definición de estrategias de mitigación orientadas al fortalecimiento de la seguridad del entorno evaluado.

Importancia de la Comunicación en la Gestión de la Ciberseguridad

El valor de una evaluación de seguridad está relacionado tanto con la detección de debilidades como con la capacidad de comunicar adecuadamente los resultados obtenidos, sino también de la capacidad para comunicar adecuadamente los resultados obtenidos. Un hallazgo técnico solo genera valor cuando puede ser comprendido, priorizado y gestionado por las personas responsables de la toma de decisiones.

La comunicación efectiva permite traducir información altamente técnica en recomendaciones claras y accionables, facilitando la implementación de controles de seguridad y la asignación adecuada de recursos para la mitigación de riesgos.

Asimismo, contribuye a fortalecer la cultura organizacional de seguridad, promoviendo la participación activa de todos los niveles de la organización en la protección de los activos de información.

Valor del Informe Técnico como Herramienta de Gestión

El informe técnico constituye un mecanismo fundamental para documentar los hallazgos obtenidos, respaldar la toma de decisiones y establecer planes de acción orientados a la mejora continua de la seguridad. Su adecuada elaboración garantiza la trazabilidad de las actividades realizadas y proporciona evidencia objetiva para futuras auditorías, evaluaciones y procesos de gestión del riesgo.

Los resultados obtenidos durante el seminario evidencian que la combinación de actividades Red Team, Blue Team, análisis de riesgos y comunicación efectiva constituye una estrategia integral para el fortalecimiento de la ciberseguridad organizacional.

Estrategias de Mitigación y Fortalecimiento de la Seguridad

La identificación de vulnerabilidades y riesgos durante el desarrollo de las actividades Red Team y Blue Team permitió establecer una serie de estrategias orientadas a reducir la exposición frente a amenazas y fortalecer la postura de seguridad del entorno evaluado. Estas estrategias se fundamentan en principios de defensa en profundidad, gestión de riesgos y mejora continua, buscando garantizar la protección de los activos de información y la continuidad de las operaciones organizacionales.

La implementación de medidas preventivas y correctivas constituye un elemento esencial dentro de cualquier programa de ciberseguridad, ya que permite disminuir la probabilidad de incidentes y mejorar la capacidad de detección y respuesta frente a eventos de seguridad.

Gestión de Vulnerabilidades y Actualización de Sistemas

Uno de los principales hallazgos identificados durante la evaluación estuvo relacionado con la presencia de vulnerabilidades conocidas asociadas a sistemas desactualizados. Esta situación evidencia la necesidad de implementar procesos formales de gestión de vulnerabilidades que permitan identificar, evaluar y corregir oportunamente las debilidades presentes en la infraestructura tecnológica.

Se recomienda establecer un programa de actualización periódica de sistemas operativos, aplicaciones y servicios críticos, garantizando la aplicación oportuna de parches de seguridad publicados por los fabricantes. Asimismo, es importante realizar evaluaciones periódicas de vulnerabilidades que permitan verificar la efectividad de las acciones implementadas y detectar nuevas amenazas emergentes.

Fortalecimiento de la Seguridad de Red

La seguridad de red constituye una de las principales líneas de defensa frente a amenazas externas e internas. Los resultados obtenidos durante el análisis evidenciaron la necesidad de fortalecer los mecanismos de control de acceso y protección del tráfico de red.

Entre las acciones recomendadas se encuentran la implementación de reglas de firewall más restrictivas, la segmentación de redes según funciones organizacionales, la eliminación de servicios innecesarios y la restricción de protocolos considerados inseguros. Estas medidas contribuyen a reducir la superficie de ataque y limitan las posibilidades de movimiento lateral dentro de la infraestructura tecnológica.

La aplicación de estrategias de defensa en profundidad permite implementar múltiples capas de protección orientadas a reducir la probabilidad de compromiso de los activos críticos (Stallings & Brown, 2018).

Tabla 19

Estrategias de fortalecimiento de la seguridad de red

Estrategia	**Acción implementada**	**Beneficio de seguridad**
Actualización de parches	Aplicar actualizaciones de seguridad de Windows y correcciones de vulnerabilidades críticas	Reduce el riesgo de explotación de vulnerabilidades conocidas
Deshabilitación de SMBv1	Eliminar versiones obsoletas del protocolo SMB	Previene ataques asociados a EternalBlue y MS17-010
Segmentación de red	Separar equipos críticos mediante VLAN y controles de acceso	Limita el movimiento lateral de atacantes

Configuración de firewall	Restringir puertos y servicios innecesarios	Disminuye la superficie de ataque
Control de privilegios	Aplicar el principio de mínimo privilegio	Reduce riesgos de escalamiento de privilegios
Autenticación multifactor (MFA)	Implementar un segundo factor de autenticación	Fortalece la protección de accesos
Monitoreo continuo	Supervisar eventos mediante SIEM y herramientas de seguridad	Permite detectar actividades sospechosas oportunamente
Gestión de servicios	Deshabilitar servicios innecesarios en los equipos	Minimiza posibles vectores de ataque

Nota. Estrategias propuestas para fortalecer la seguridad de red a partir de los hallazgos identificados durante la evaluación técnica. Elaboración propia (2026).

La implementación de estas medidas permitiría incrementar significativamente la capacidad de protección frente a amenazas que buscan explotar vulnerabilidades de red o configuraciones inseguras.

Implementación de Monitoreo y Detección Continua

La detección temprana de actividades sospechosas constituye un componente esencial dentro de las estrategias modernas de ciberseguridad. Por esta razón, se recomienda implementar mecanismos de monitoreo continuo que permitan identificar comportamientos anómalos y generar alertas oportunas frente a posibles incidentes de seguridad.

El monitoreo debe incluir la recopilación y correlación de eventos provenientes de servidores, estaciones de trabajo, dispositivos de red y aplicaciones críticas. Asimismo, es

recomendable establecer procedimientos de análisis de registros y revisión periódica de indicadores de compromiso que faciliten la identificación de amenazas en etapas tempranas.

Aprendizajes Obtenidos Durante las Actividades Red Team

El monitoreo continuo y la correlación de eventos permiten identificar comportamientos anómalos y fortalecer la capacidad de detección temprana frente a amenazas emergentes (ENISA, 2023).

Fortalecimiento de los Procesos de Gestión de Incidentes

La capacidad de respuesta ante incidentes representa uno de los factores más importantes para minimizar el impacto de una amenaza sobre los activos de información. En este sentido, es recomendable establecer procedimientos formales para la gestión de incidentes que definan claramente las responsabilidades, actividades y mecanismos de comunicación durante situaciones de emergencia.

La organización debe contar con planes de respuesta documentados, procedimientos de escalamiento y mecanismos de recuperación que permitan actuar de manera rápida y coordinada frente a eventos de seguridad.

Figura 6

Proceso de gestión y fortalecimiento de la seguridad

Nota. Ciclo de mejora continua al fortalecimiento de la seguridad organizacional mediante la identificación de vulnerabilidades, implementación de controles y gestión de incidentes. Elaboración propia (2026).

El ciclo representado en la Figura 6 refleja las actividades desarrolladas durante el laboratorio SecureNova Labs, donde la identificación de vulnerabilidades permitió definir

controles de mitigación, evaluar riesgos y proponer mecanismos de monitoreo y mejora continua orientados al fortalecimiento de la seguridad.

Capacitación y Concientización en Ciberseguridad

Los controles tecnológicos por sí solos no garantizan la protección efectiva de los activos de información. Una parte importante de los incidentes de seguridad tiene su origen en errores humanos, desconocimiento de procedimientos o prácticas inseguras por parte de los usuarios.

Por esta razón, se recomienda implementar programas permanentes de capacitación y concientización en ciberseguridad dirigidos a todos los niveles de la organización. Estas actividades deben abordar temas relacionados con gestión de contraseñas, identificación de correos maliciosos, protección de la información y respuesta ante incidentes.

La formación continua contribuye al fortalecimiento de la cultura organizacional de seguridad y reduce significativamente el riesgo asociado a amenazas basadas en ingeniería social.

Implementación de Controles de Seguridad Avanzados

Con el propósito de incrementar el nivel de protección de la infraestructura tecnológica, se recomienda evaluar la implementación de controles de seguridad avanzados que complementen los mecanismos tradicionales de protección.

Entre las tecnologías recomendadas se encuentran las soluciones de detección y respuesta en endpoints (EDR), sistemas de prevención de intrusiones (IPS), plataformas de gestión de eventos e información de seguridad (SIEM), mecanismos de autenticación multifactor (MFA) y soluciones de protección frente a ataques de denegación de servicio.

Tabla 20

Controles de seguridad recomendados.

Control de seguridad	Función principal	Beneficio esperado
EDR	Detección y respuesta en endpoints	Mayor visibilidad de amenazas
SIEM	Correlación de eventos de seguridad	Detección temprana de incidentes
MFA	Verificación adicional de identidad	Reducción de accesos no autorizados
IPS	Prevención de intrusiones	Bloqueo de ataques conocidos
Gestión de vulnerabilidades	Identificación continua de riesgos	Mejora permanente de la seguridad

Nota. Controles de seguridad recomendados para fortalecer la protección de la infraestructura tecnológica evaluada. Elaboración propia (2026).

Beneficios Esperados de las Estrategias Propuestas

La implementación de las estrategias de mitigación y fortalecimiento descritas permitiría reducir significativamente la probabilidad de explotación de vulnerabilidades, mejorar la capacidad de detección de amenazas y fortalecer los mecanismos de respuesta ante incidentes.

Asimismo, contribuiría al cumplimiento de buenas prácticas de seguridad, incrementaría la resiliencia organizacional frente a amenazas emergentes y facilitaría la protección de los activos críticos de información. Estas acciones constituyen una base sólida para el desarrollo de programas de ciberseguridad alineados con los objetivos estratégicos de las organizaciones.

Lecciones Aprendidas

El desarrollo del Seminario Especializado en Ciberseguridad permitió fortalecer conocimientos teóricos y prácticos relacionados con la protección de activos de información, la

identificación de vulnerabilidades, la gestión de incidentes y la aplicación de principios éticos dentro del ejercicio profesional. A través de las diferentes etapas desarrolladas, fue posible comprender la importancia de integrar capacidades ofensivas y defensivas para lograr una visión más completa de la seguridad informática en entornos organizacionales.

Las actividades realizadas facilitaron la aplicación práctica de conceptos asociados a pruebas de penetración, análisis de vulnerabilidades, evaluación de riesgos y respuesta ante incidentes, permitiendo consolidar competencias fundamentales para el desempeño profesional en el ámbito de la ciberseguridad.

Aprendizajes Relacionados con los Fundamentos de la Ciberseguridad

Durante las primeras etapas del seminario se fortaleció la comprensión de los conceptos fundamentales de la ciberseguridad, incluyendo la protección de la información, la gestión de riesgos y la importancia de la tríada de seguridad conformada por la confidencialidad, integridad y disponibilidad. Estos conocimientos constituyeron la base conceptual necesaria para comprender las actividades prácticas desarrolladas posteriormente.

Asimismo, se evidenció que la seguridad informática no depende exclusivamente de herramientas tecnológicas, sino también de procesos organizacionales, políticas institucionales y una adecuada cultura de seguridad que involucre a todos los actores de la organización.

Aprendizajes Relacionados con la Ética Profesional y el Marco Normativo

El análisis de escenarios relacionados con la ética profesional permitió comprender la responsabilidad que tienen los profesionales de la ciberseguridad frente al manejo de información sensible y la utilización de herramientas de análisis y explotación de vulnerabilidades.

De igual forma, se fortaleció el conocimiento sobre la legislación colombiana aplicable a delitos informáticos y protección de la información, destacando la importancia de desarrollar

actividades de seguridad dentro de marcos legales claramente definidos y respetando principios éticos asociados al ejercicio profesional de la ingeniería.

Aprendizajes Obtenidos Durante las Actividades Red Team

Las actividades ofensivas desarrolladas dentro del entorno de laboratorio permitieron comprender la metodología utilizada por los equipos Red Team para identificar vulnerabilidades y evaluar el nivel de exposición de una infraestructura tecnológica.

El uso de herramientas especializadas como Nmap, Netdiscover y Metasploit facilitó la comprensión de las fases de reconocimiento, enumeración, análisis de vulnerabilidades y validación de hallazgos. Asimismo, se evidenció la importancia de una adecuada planificación y documentación durante la ejecución de pruebas de seguridad.

El análisis de vulnerabilidades realizado durante el laboratorio permitió aplicar metodologías utilizadas en pruebas de penetración profesionales para la identificación de debilidades explotables (Weidman, 2014).

Tabla 21

Principales aprendizajes obtenidos durante las actividades Red Team

Actividad desarrollada	**Aprendizaje obtenido**
Reconocimiento de red	Identificación de activos y servicios expuestos
Escaneo de puertos	Descubrimiento de superficies de ataque
Enumeración de servicios	Obtención de información técnica relevante
Análisis de vulnerabilidades	Identificación de debilidades explotables
Validación de hallazgos	Confirmación de riesgos de seguridad

Nota. Aprendizajes obtenidos durante la ejecución de actividades ofensivas dentro del entorno de laboratorio. Elaboración propia (2026).

Los resultados obtenidos permitieron comprender la importancia de identificar vulnerabilidades antes de que estas puedan ser aprovechadas por actores maliciosos.

Aprendizajes Obtenidos Durante las Actividades Blue Team

Las actividades defensivas permitieron desarrollar competencias relacionadas con la identificación de indicadores de compromiso, análisis de eventos de seguridad, evaluación de riesgos y definición de medidas de mitigación.

La experiencia adquirida evidenció la importancia del monitoreo continuo, la gestión adecuada de incidentes y la implementación de controles preventivos para reducir la probabilidad de afectación de los activos de información.

Tabla 22

Principales aprendizajes obtenidos durante las actividades Blue Team

Actividad desarrollada	**Aprendizaje obtenido**
Identificación de incidentes	Detección temprana de amenazas
Análisis de evidencias	Comprensión del comportamiento de los eventos
Evaluación de riesgos	Priorización de acciones correctivas
Contención de incidentes	Reducción del impacto potencial
Fortalecimiento de controles	Mejora continua de la seguridad

Nota. Aprendizajes obtenidos durante las actividades defensivas desarrolladas en el entorno de laboratorio. Elaboración propia (2026).

La integración de procesos de monitoreo, análisis y respuesta permitió comprender el papel estratégico de los equipos Blue Team dentro de los programas modernos de ciberseguridad.

Importancia de la Integración entre Red Team y Blue Team

Uno de los principales aprendizajes obtenidos durante el seminario fue comprender que las actividades ofensivas y defensivas no deben considerarse procesos independientes, sino componentes complementarios dentro de una estrategia integral de seguridad.

Las actividades Red Team permitieron identificar vulnerabilidades y evaluar riesgos potenciales, mientras que las actividades Blue Team facilitaron la implementación de mecanismos orientados a la detección, contención y mitigación de amenazas. Esta integración favorece el fortalecimiento continuo de la postura de seguridad organizacional.

Figura 7

Integración de capacidades Red Team y Blue Team

Nota. Representación del ciclo de mejora continua generado por la integración de actividades Red Team y Blue Team dentro de una estrategia de ciberseguridad organizacional. Elaboración propia (2026).

Lecciones Aprendidas para el Ejercicio Profesional

La experiencia obtenida durante el seminario permitió fortalecer competencias técnicas, analíticas y éticas necesarias para el ejercicio profesional en áreas relacionadas con la seguridad de la información. Asimismo, facilitó la comprensión de la importancia de la actualización permanente frente a la evolución constante de las amenazas cibernéticas.

Entre los principales aprendizajes se destaca la necesidad de adoptar enfoques preventivos, implementar mecanismos de monitoreo continuo, fortalecer los procesos de gestión de riesgos y promover una cultura organizacional orientada a la protección de la información.

Reflexión Final del Proceso Formativo

El seminario permitió integrar conocimientos teóricos y prácticos mediante el desarrollo de escenarios controlados que simularon situaciones reales de ciberseguridad. Esta experiencia contribuyó significativamente al fortalecimiento de competencias relacionadas con el análisis técnico, la identificación de vulnerabilidades, la respuesta ante incidentes y la toma de decisiones basadas en riesgos.

Los conocimientos adquiridos constituyen una base sólida para afrontar futuros desafíos profesionales relacionados con la protección de infraestructuras tecnológicas y la gestión de la seguridad de la información en entornos organizacionales.

Conclusiones

El desarrollo del Seminario Especializado en Ciberseguridad permitió cumplir el objetivo de identificar vulnerabilidades presentes en un entorno controlado mediante la aplicación de metodologías y herramientas utilizadas en ejercicios de seguridad ofensiva y defensiva. Durante las actividades de reconocimiento y enumeración se identificó la exposición del servicio SMB sobre el puerto TCP 445, así como la presencia del sistema operativo Windows 7 Professional SP1, condiciones que permitieron detectar la vulnerabilidad MS17-010 asociada al protocolo SMBv1.

Los resultados obtenidos mediante Nmap, scripts NSE y Metasploit permitieron confirmar técnicamente la existencia de la vulnerabilidad EternalBlue (MS17-010), evidenciando que un atacante con acceso a la red podría explotar el servicio vulnerable para ejecutar código de forma remota y comprometer la confidencialidad, integridad y disponibilidad de la información. Esta situación demostró el impacto que pueden generar los sistemas desactualizados y los protocolos obsoletos dentro de una infraestructura tecnológica.

Las actividades desarrolladas permitieron analizar el impacto de las vulnerabilidades identificadas sobre la tríada CIA. La exposición del servicio SMB y la posibilidad de explotación de MS17-010 representan riesgos directos para la confidencialidad de la información almacenada, la integridad de los sistemas comprometidos y la disponibilidad de los servicios afectados, confirmando la importancia de implementar controles preventivos y correctivos para proteger los activos de información.

Desde la perspectiva Blue Team, el ejercicio permitió evaluar mecanismos de detección, contención y mitigación orientados a reducir los riesgos identificados. Adicionalmente, la adecuada recolección, preservación y análisis de evidencias digitales constituye un elemento

esencial para la investigación de incidentes de seguridad y el apoyo a procesos forenses posteriores (Casey, 2011). La aplicación de parches de seguridad para corregir MS17-010, la deshabilitación de SMBv1, la segmentación de red, el endurecimiento de configuraciones y la implementación de controles de monitoreo fueron identificados como medidas efectivas para disminuir significativamente la probabilidad de explotación y el impacto potencial de las vulnerabilidades detectadas.

El análisis de riesgos realizado permitió clasificar la vulnerabilidad MS17-010 como un riesgo crítico debido a su facilidad de explotación y a las consecuencias que podría generar sobre la infraestructura tecnológica. Asimismo, se determinó que la presencia de sistemas desactualizados, servicios expuestos y configuraciones inseguras incrementa considerablemente la superficie de ataque y requiere acciones correctivas prioritarias para fortalecer la postura de seguridad organizacional.

El estudio de los aspectos éticos y normativos permitió comprender que las actividades de análisis de seguridad deben desarrollarse dentro de entornos autorizados y controlados, respetando los principios de legalidad, confidencialidad y uso responsable de herramientas especializadas. La experiencia evidenció que la aplicación de principios éticos constituye un componente fundamental para el ejercicio profesional de la ciberseguridad.

La integración de capacidades Red Team y Blue Team permitió obtener una visión integral del estado de seguridad del entorno SecureNova Labs, demostrando que la identificación de vulnerabilidades debe complementarse con mecanismos de monitoreo, respuesta y fortalecimiento continuo de controles. Esta interacción evidenció la importancia de combinar enfoques ofensivos y defensivos para fortalecer la gestión del riesgo y mejorar la resiliencia de las organizaciones frente a amenazas cibernéticas.

Finalmente, el seminario permitió consolidar competencias relacionadas con el análisis técnico de vulnerabilidades, la evaluación de riesgos, la gestión de incidentes y la formulación de estrategias de mitigación, cumpliendo los objetivos planteados para el desarrollo del ejercicio académico. Los conocimientos adquiridos proporcionan una base sólida para la aplicación de buenas prácticas de ciberseguridad en escenarios organizacionales reales y para la protección efectiva de infraestructuras tecnológicas frente a amenazas emergentes.

Recomendaciones

Como acción prioritaria e inmediata, se recomienda aplicar los parches de seguridad correspondientes a la vulnerabilidad MS17-010 identificada durante el laboratorio, debido a que representa el riesgo de mayor criticidad dentro del entorno evaluado. La evidencia obtenida mediante Nmap, scripts NSE y Metasploit permitió confirmar la exposición del sistema a ataques de ejecución remota de código. Posteriormente, debe verificarse la efectividad de la corrección mediante nuevos escaneos de vulnerabilidades que confirmen la ausencia de la condición identificada.

De igual manera, se recomienda deshabilitar el protocolo SMBv1 en todos los sistemas donde se encuentre habilitado, dado que su utilización incrementa significativamente la superficie de ataque y facilita la explotación de vulnerabilidades conocidas. Esta medida debe complementarse con revisiones periódicas de configuración y validaciones técnicas que permitan comprobar la eliminación efectiva del protocolo vulnerable.

Como parte de las acciones de corto y mediano plazo, resulta necesario fortalecer los controles de acceso mediante la restricción de servicios innecesarios, la implementación de reglas de firewall más restrictivas y la segmentación de red. Estas medidas permitirán limitar accesos no autorizados y reducir las posibilidades de movimiento lateral dentro de la infraestructura tecnológica. Su efectividad puede verificarse mediante nuevos procesos de reconocimiento y pruebas controladas de conectividad.

Asimismo, se recomienda implementar un programa formal de gestión de vulnerabilidades que permita identificar, evaluar, priorizar y corregir oportunamente las debilidades presentes en los sistemas de información. Este proceso debe incluir evaluaciones

periódicas de seguridad y mecanismos de seguimiento que permitan medir la reducción progresiva de vulnerabilidades críticas y de alto riesgo.

Con el fin de mejorar la capacidad de detección temprana de amenazas, se recomienda fortalecer los mecanismos de monitoreo mediante la implementación de soluciones SIEM, EDR e IDS/IPS. Estas herramientas permitirán correlacionar eventos, identificar comportamientos anómalos y generar alertas oportunas frente a posibles incidentes de seguridad. La efectividad de estos controles puede evaluarse mediante simulaciones controladas, análisis de alertas y revisión periódica de registros de seguridad.

Adicionalmente, se recomienda fortalecer los procesos de gestión de incidentes mediante la definición de procedimientos documentados, mecanismos de escalamiento y planes de recuperación que permitan responder de manera rápida y coordinada ante eventos de seguridad. La validación de estos procesos debe realizarse mediante ejercicios de simulación y pruebas periódicas de respuesta ante incidentes. Asimismo, es fundamental que la organización establezca políticas, procedimientos y estándares de seguridad claramente definidos, ya que estos constituyen la base para una gestión consistente y eficaz de la seguridad de la información (Peltier, 2016).

De forma permanente, la organización debe desarrollar programas de capacitación y concientización en ciberseguridad dirigidos a usuarios, administradores y responsables de la infraestructura tecnológica. Esta medida contribuirá a disminuir riesgos asociados al factor humano, fortalecer la cultura organizacional de seguridad y mejorar el cumplimiento de buenas prácticas relacionadas con la protección de la información.

Igualmente, se recomienda integrar la gestión de riesgos dentro de los procesos estratégicos de la organización, garantizando que las decisiones relacionadas con seguridad de la

información se encuentren respaldadas por análisis técnicos, evaluación de impacto y criterios objetivos de priorización.

Finalmente, se recomienda mantener una estrategia de mejora continua basada en auditorías de configuración, evaluaciones periódicas de vulnerabilidades, seguimiento de indicadores de seguridad y ejercicios de validación Red Team y Blue Team. Estas actividades permitirán verificar la efectividad de los controles implementados, identificar nuevas amenazas y fortalecer de manera permanente la resiliencia organizacional frente a un entorno de riesgos cada vez más dinámico y sofisticado.

Evidencias de Sustentación

En cumplimiento de los requisitos establecidos para la Etapa 5 del Seminario Especializado en Ciberseguridad, se realizó la sustentación del informe técnico final mediante la presentación de los resultados obtenidos durante el desarrollo de las actividades académicas y prácticas. La sustentación permitió exponer las metodologías utilizadas, los hallazgos identificados, las estrategias implementadas por los equipos Red Team y Blue Team, así como las conclusiones y recomendaciones derivadas del análisis realizado.

Video de sustentación del informe final:

https://youtu.be/c-Vw9vWMkvk

Nota. El video de sustentación presenta una síntesis de las actividades desarrolladas durante las cinco etapas del seminario, incluyendo el entorno de laboratorio implementado, las pruebas realizadas, los resultados obtenidos y las principales lecciones aprendidas durante el proceso formativo.

Referencias Bibliográficas

Andress, J., & Winterfeld, S. (2014). *Cyber warfare: Techniques, tactics and tools for security practitioners* (2nd ed.). Elsevier.

Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers and the Internet* (3rd ed.). Academic Press.

Easttom, C. (2018). *Computer security fundamentals* (4th ed.). Pearson

European Union Agency for Cybersecurity (ENISA). (2023). *Threat landscape 2023*. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

Kim, D., & Solomon, M. G. (2018). *Fundamentals of information systems security* (3rd ed.). Jones & Bartlett Learning.

Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado de la protección de la información y de los datos y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones. Diario Oficial No. 47.223. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

Manson, D., Carlin, A., Ramos, S., & Gyger, J. (2014). *Cyber security essentials.* CRC Press.

National Institute of Standards and Technology (NIST). (2024). *Cybersecurity framework (CSF) 2.0.* U.S. Department of Commerce. https://www.nist.gov/cyberframework

OccupyTheWeb. (2021). *Linux basics for hackers* (2nd ed.). No Starch Press.

Open Web Application Security Project (OWASP). (2021). *OWASP Top 10: The ten most critical web application security risks.* https://owasp.org/www-project-top-ten

Peltier, T. R. (2016). *Information security policies, procedures, and standards*. Auerbach Publications.

Scarfone, K., & Mell, P. (2007). *Guide to intrusion detection and prevention systems (IDPS).* National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-94.pdf

Stallings, W., & Brown, L. (2018). *Computer security: Principles and practice* (4th ed.). Pearson

Tanenbaum, A. S., & Wetherall, D. J. (2013). *Computer networks* (5th ed.). Pearson.

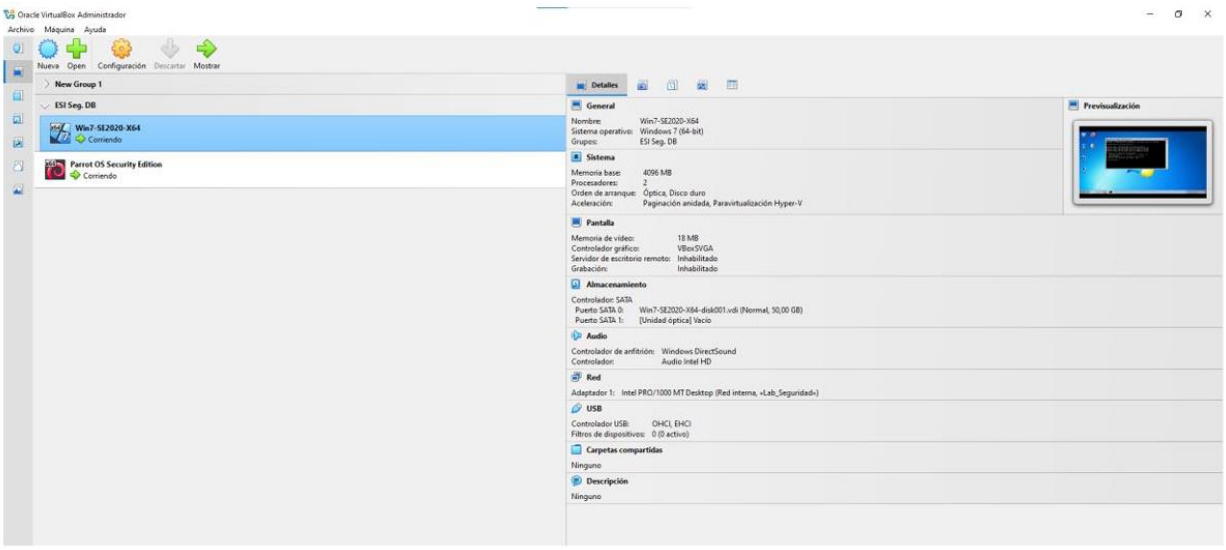
Weidman, G. (2014). *Penetration testing: A hands-on introduction to hacking*. No Starch Press.

Apéndices

A continuación, se presentan los apéndices que contienen las evidencias técnicas recopiladas durante el desarrollo del seminario y que respaldan los resultados expuestos en el presente informe.

Apéndice A

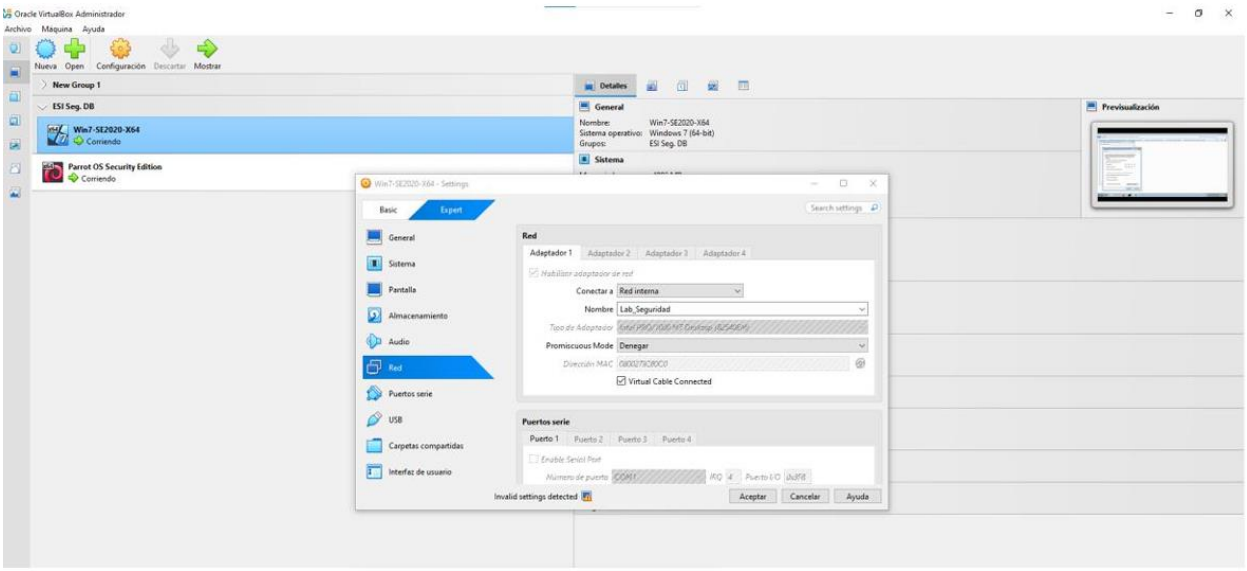
Configuración del entorno de laboratorio.



Nota. Evidencia de la configuración inicial del entorno de laboratorio, incluyendo las máquinas virtuales Kali Linux, Host-A y Host-B empleadas para las actividades de reconocimiento, análisis de vulnerabilidades y validación de controles de seguridad. Elaboración propia (2026).

Apéndice B

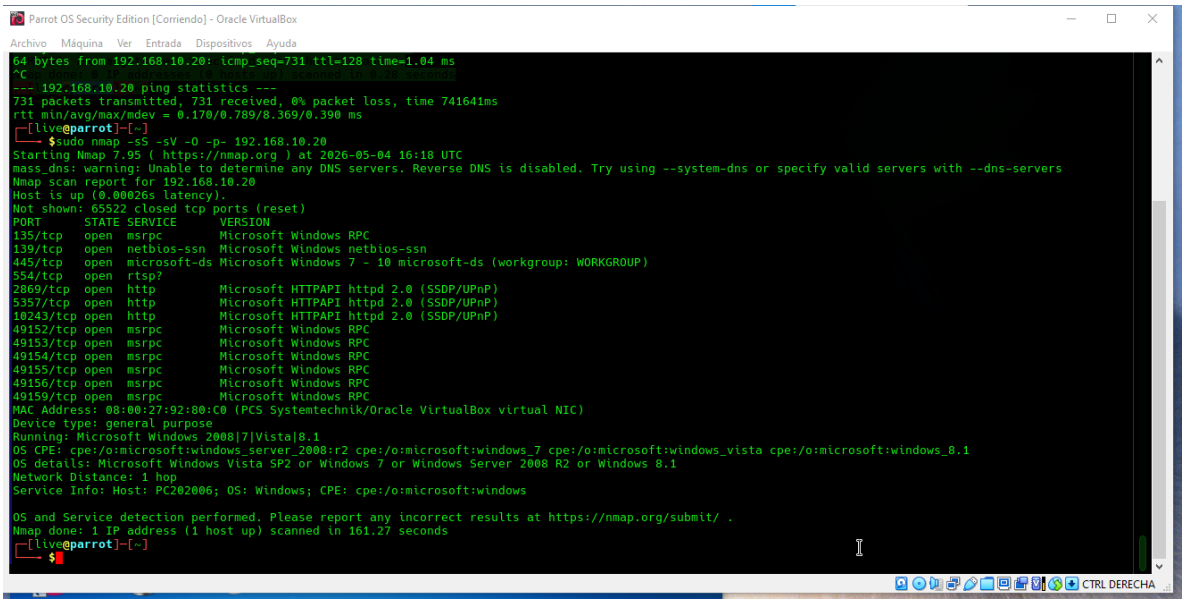
Validación de conectividad de red.



Nota. Evidencia de las pruebas de conectividad realizadas entre los equipos del entorno de laboratorio, validando la correcta comunicación de red necesaria para la ejecución de las actividades Red Team y Blue Team. Elaboración propia (2026).

Apéndice C

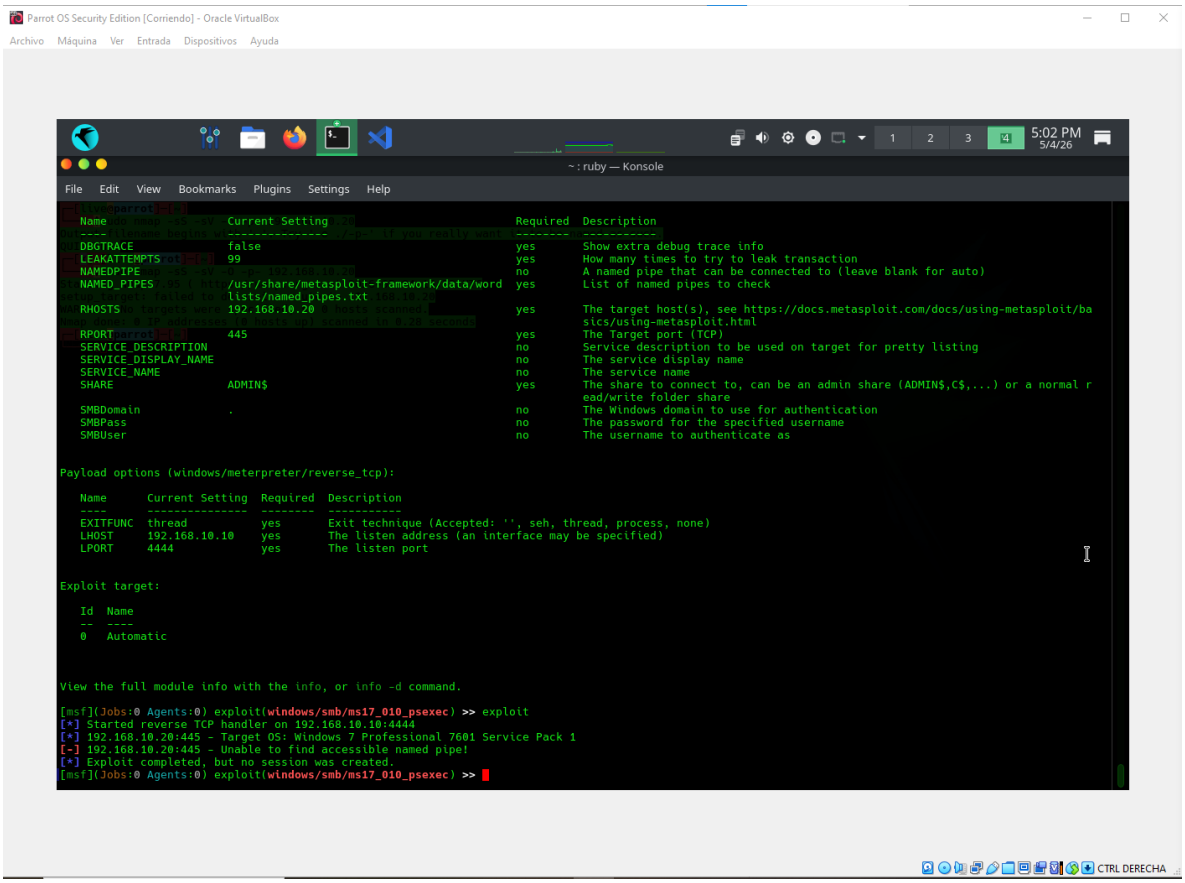
Reconocimiento y enumeración



Nota. Evidencias del proceso de reconocimiento realizado sobre el entorno evaluado, permitiendo identificar hosts activos, puertos expuestos y servicios accesibles utilizados posteriormente en las actividades de análisis de vulnerabilidades. Elaboración propia (2026).

Apéndice D

Explotación y validación técnica



Nota. Evidencias de la fase de explotación controlada realizada mediante herramientas de seguridad ofensiva, permitiendo validar la vulnerabilidad MS17-010 (EternalBlue) identificada durante las actividades de reconocimiento y análisis de vulnerabilidades. Elaboración propia (2026).

Apéndice E

Análisis Blue Team

Tabla 1

Acciones de contención implementadas durante el incidente de seguridad.

Fase	Acción ejecutada	Herramienta utilizada	Resultado esperado
Detección	Identificación de actividad anómala en la red	Wazuh / Sysmon	Generación de alertas de seguridad
Análisis	Revisión de logs y conexiones SMB	Event Viewer / Wireshark	Identificación del origen del ataque
Contención	Aislamiento de Host-A de la red	pfSense / Firewall Windows	Evitar propagación lateral
Bloqueo	Restricción del puerto 445 y tráfico SMB	Firewall / IDS	Interrupción del vector de ataque
Monitoreo	Supervisión de otros dispositivos internos	Snort / Suricata	Detección de nuevos intentos
Remediación	Aplicación de parches de seguridad	Windows Update	Eliminación de vulnerabilidades
Recuperación	Restablecimiento seguro de servicios	SIEM / Antivirus	Retorno controlado a operación

Nota. La tabla presenta las principales fases ejecutadas por el equipo Blue Team durante el proceso de contención del ataque. Elaboración propia (2026).

Tabla 2

Resultados obtenidos durante el análisis de contención del incidente.

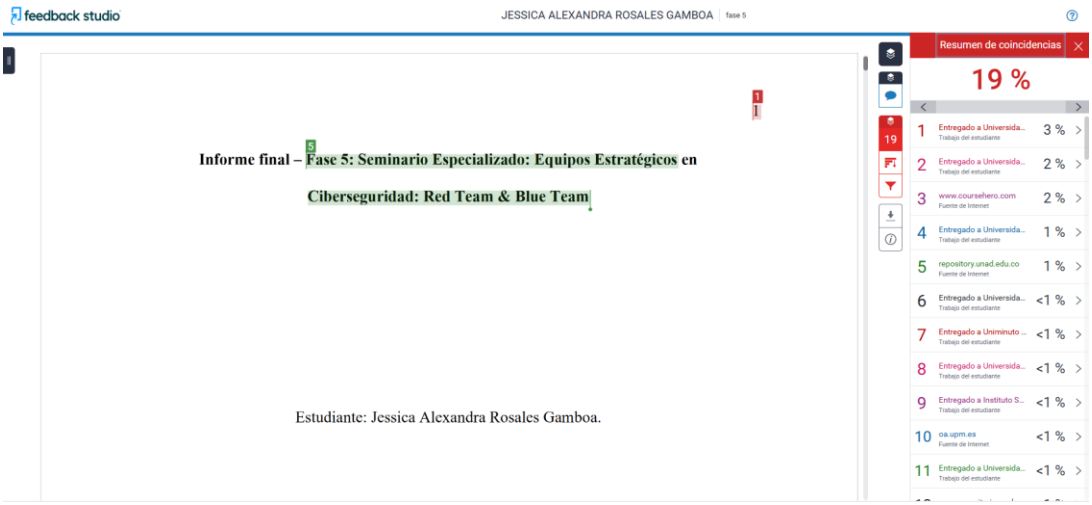
Elemento analizado	Resultado obtenido	Impacto sobre la seguridad
Puerto 445	Tráfico SMB sospechoso detectado	Alto riesgo de explotación
Host-A	Equipo comprometido parcialmente	Riesgo de escalamiento
Host-B	No se evidenció compromiso directo	Riesgo moderado
Usuarios del sistema	No se identificaron nuevos administradores	Contención parcial exitosa
Servicios críticos	Permanecieron operativos	Disponibilidad conservada
Segmentación de red	Limitó propagación lateral	Reducción del impacto

Nota. Los resultados reflejan el comportamiento observado durante la ejecución de medidas defensivas sobre la infraestructura tecnológica analizada. Elaboración propia (2026).

Nota. Evidencias empleadas para el análisis Blue Team, permitiendo establecer controles de mitigación, mecanismos de monitoreo y estrategias de fortalecimiento de la seguridad orientadas a reducir los riesgos identificados durante la evaluación del entorno. Elaboración propia (2026).

Apéndice F

Resultado de similitud Turnitin



Nota. Evidencia del índice de similitud generado por la plataforma de verificación de originalidad utilizada para evaluar la versión final del documento, como mecanismo de validación del cumplimiento de criterios de integridad académica. Elaboración propia (2026).