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

Wilmer Muñoz Muñoz

Asesor

Eduvin Trigos Sánchez

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Especialización en seguridad informática

2025

Resumen

Este documento presenta un análisis integral del caso de estudio de SecureNova Labs, una organización de ciberseguridad que enfrenta una crisis con implicaciones éticas, legales y técnicas. El informe describe la respuesta en cinco etapas secuenciales. Inicia con la definición del marco legal colombiano y las metodologías empleadas en las operaciones de Red y Blue Team; continúa con un análisis crítico de un acuerdo de confidencialidad que incluye cláusulas orientadas a encubrir prácticas ilegales; y profundiza en la investigación técnica de vulnerabilidades críticas como EternalBlue CVE-2017-0143 (INCIBE, 2025), así como en la exfiltración de información sensible. Posteriormente, aborda la contención del incidente mediante contramedidas basadas en ajustes de configuración y hardening de sistemas, y finaliza con la consolidación de los hallazgos en un informe estratégico. Los resultados evidencian la relación directa entre fallas éticas y brechas de seguridad. En este contexto, se resalta la necesidad de adoptar un enfoque integral que combine rigor normativo, competencia técnica e integridad profesional como pilares esenciales de la ciberseguridad.

Palabras clave: análisis forense, Blue Team, ciberseguridad, ética profesional, marco legal colombiano, Red Team, respuesta a incidentes, SecureNova Labs.

Abstract

This document presents a comprehensive analysis of the SecureNova Labs case study, a cybersecurity organization facing a crisis with ethical, legal, and technical implications. The report describes the response across five sequential stages. It begins with the definition of the Colombian legal framework and the methodologies used in Red and Blue Team operations; continues with a critical analysis of a confidentiality agreement containing clauses intended to conceal illegal practices; and delves into the technical investigation of critical vulnerabilities such as EternalBlue CVE-2017-0143 (INCIBE, 2025), as well as the exfiltration of sensitive information. Subsequently, it addresses incident containment through countermeasures based on configuration adjustments and system hardening, and concludes with the consolidation of findings into a strategic report. The results reveal a direct connection between ethical failures and security breaches. In this context, the study emphasizes the need for a comprehensive approach that integrates regulatory rigor, technical competence, and professional integrity as essential pillars of cybersecurity.

Keywords: Blue Team, Colombian legal framework, cybersecurity, forensic analysis, incident response, professional ethics, Red Team, SecureNova Labs.

Tabla de contenido

Lista de Figuras

Lista de Tablas

Lista de Apéndices

Glosario

Acuerdo de Confidencialidad (NDA):

Documento legal que establece obligaciones de reserva y manejo adecuado de información sensible, buscando proteger los datos de una organización. En ciberseguridad regula tanto los límites éticos como los legales de las actividades técnicas y autorizadas.

Análisis de Vulnerabilidades:

Proceso ordenado y sistemático para identificar, evaluar y priorizar debilidades presentes en sistemas, aplicaciones o las redes de datos digitales, utilizando marcos reconocidos como CVE y CVSS.

Ataque Informático:

Acción hecha a propósito cuyo objetivo es comprometer la confidencialidad, integridad o disponibilidad de cualquier sistema mediante técnicas ofensivas.

Blue Team:

Equipo encargado de la defensa proactiva de la infraestructura tecnológica mediante el monitoreo, la gestión de vulnerabilidades, detección de amenazas, respuesta a incidentes y adicionalmente el Hardening de los sistemas.

Ciberseguridad:

Conjunto de prácticas, procesos y tecnologías destinadas a la protección los sistemas de información frente a amenazas digitales que puedan comprometer el carácter secreto, la integridad o la accesibilidad de los datos.

Ciclo de Respuesta a Incidentes:

Modelo con una estructura que incluye detección, análisis, contención, erradicación, recuperación y documentación que se realiza después de detectar un incidente de seguridad.

CSIRT (Computer Security Incident Response Team):

Equipo especializado que se responsabiliza de gestionar incidentes de seguridad confirmados, coordina acciones de contención, análisis forense y la recuperación de los sistemas siguiendo lineamientos internacionales.

CVE (Common Vulnerabilities and Exposures):

Catálogo público que asigna identificadores únicos a vulnerabilidades conocidas, que permite la referenciación estandarizada a nivel mundial.

CVSS (Common Vulnerability Scoring System):

Sistema que asigna una puntuación a las vulnerabilidades según su impacto y facilidad de explotación, facilitando su priorización.

Enumeración:

Término usado en pentesting que hace referencia a la identificación de: usuarios, servicios, puertos abiertos, rutas o componentes específicos del objetivo, donde se obtiene información detallada para ataques posteriores.

Entorno de Pruebas:

Es una infraestructura aislada, ya sea física o virtual, que replica condiciones reales sin afectar los sistemas en producción, esto permite la ejecución segura de técnicas ofensivas y defensivas.

Erradicación:

Etapa de la respuesta contra incidentes, en la que se eliminan los vectores de ataque, malware, cuentas o configuraciones comprometidas para evitar caer en reinfecciones.

Exfiltración de Datos:

Extracción no autorizada de información desde un sistema que fue comprometido, siendo esta una de las acciones más críticas durante cualquier incidente.

Exploit:

Código o técnica que se ejecuta para aprovechar una vulnerabilidad y lograr acceso o acciones no autorizadas en un sistema.

Explotación Controlada:

Ejecución de técnicas ofensivas ejecutadas sobre una vulnerabilidad identificada, para validar su impacto dentro de un ejercicio autorizado de penetración, su alcance llega máximo a evidenciar el compromiso sin causar daños a las operaciones normales de la organización evaluada.

Hardening:

Conjunto de prácticas que se orientan al reforzamiento de la seguridad de un sistema mediante la reducción de su superficie de ataque lo que puede llevar a: deshabilitación de servicios innecesarios y aplicación de configuraciones parches de seguridad, entre otros.

IDS/IPS (Intrusion Detection/Prevention System):

Sistemas que detectan y, en el caso de los IPS, bloquean actividades maliciosas en la red utilizando firmas, comportamiento o reglas de correlación.

Ingeniería Social:

Manipulación psicológica y del comportamiento humano para obtener acceso o información sensible, sin necesidad de técnicas tecnológicas complejas.

Investigación Forense Digital:

Disciplina que se encarga de recopilar, preservar, analizar y presentar evidencia digital de forma estructurada y admisible legalmente para determinar el origen, alcance e impacto de un incidente.

Marco Legal en Ciberseguridad:

Conjunto de leyes, normativas y políticas que regulan las acciones permitidas en ejercicios de seguridad informática, estableciendo responsabilidades y límites profesionales claros.

Metodologías de Pentesting (PTES, NIST, OWASP):

Conjuntos de lineamientos aceptados internacionalmente que estructuran las fases y actividades de una prueba de penetración, garantizando rigurosidad, reproducibilidad y buenas prácticas.

Metasploit Framework:

Plataforma ampliamente utilizada en pruebas de penetración para ejecutar exploits, generar payloads y realizar acciones de post-explotación.

MITRE ATT&CK:

Marco internacional que documenta tácticas, técnicas y procedimientos utilizados por adversarios en ataques reales, permitiendo estandarizar y contextualizar actividades ofensivas y defensivas.

Movimiento Lateral:

Son técnicas que usan los atacantes, después de comprometer un sistema, y consiste en descubrir y avanzar hacia otros activos dentro de la red para aumentar nivel de acceso.

OSINT (Open-Source Intelligence):

Recolección de información pública disponible en internet, redes sociales, fuentes abiertas y motores de búsqueda, se usa en la fase de reconocimiento.

Playbook:

Guía de carácter operativo que define los pasos a seguir para responder a un incidente de seguridad específico.

Payload (Carga útil):

Código o instrucción que se ejecuta después de que un exploit tiene éxito. La “carga útil” es la que realiza la acción deseada por el atacante, como por ejemplo abrir una conexión remota, crear un usuario o extraer información.

Pentesting (Pruebas de Penetración):

Evaluación que usa recursos autorizados y que simula ataques reales con el fin de identificar, explotar y documentar vulnerabilidades presentes en un sistema, su fin es ayudar a eliminar o mitigar las amenazas que un atacante real podría aprovechar.

Pivoting:

Técnica que usa un atacante durante la post-explotación para utilizar un sistema comprometido como puente hacia otras redes o dispositivos internos.

Post-Explotación:

Fase en la que se evalúan los privilegios obtenidos, se mantiene el acceso, se identifican recursos adicionales y se determina el alcance del compromiso.

Reconocimiento:

Primera fase ofensiva donde se recopila la mayor cantidad de información del objetivo, para comprender el entorno.

Red Team:

Equipo encargado de simular ataques reales con el objetivo de evaluar la postura de seguridad de la organización.

SIEM (Security Information and Event Management):

Plataforma que recopila información o eventos de seguridad de múltiples fuentes que luego correlaciona mediante regalas preconfiguradas, para detectar incidentes y generar alertas.

Sistema de Gestión de Parches:

Conjunto de procesos y herramientas que permiten aplicar actualizaciones de seguridad de manera eficiente para reducir riesgos de explotación.

VirtualBox:

Software de virtualización que permite crear y gestionar máquinas virtuales utilizadas en entornos aislados de pruebas y laboratorios de ciberseguridad.

Introducción

Este documento explora de manera secuencial cinco etapas que permiten comprender la relación entre el marco legal colombiano, las operaciones de Red Team y Blue Team, la respuesta a incidentes y la responsabilidad profesional en el ámbito de la seguridad informática. En primer lugar, se establece la base normativa y metodológica que guía tanto las actividades ofensivas como defensivas, incorporando leyes como la 1273 de 2009, la 1581 de 2012 y la 1928 de 2018, así como marcos internacionales como PTES, MITRE ATT&CK, NIST SP 800-115. Posteriormente, se presenta un análisis crítico del acuerdo de confidencialidad empleado por SecureNova Labs, destacando los riesgos legales y éticos que contradicen la legislación colombiana y comprometen la integridad profesional.

En las etapas prácticas, se desarrolla un ejercicio de Red Team que simula la infiltración en la infraestructura de la empresa mediante vulnerabilidades como MS17-010 (EternalBlue), seguido por la identificación de movimiento lateral y la exfiltración de datos sensibles. Luego, se describe la respuesta técnica y forense al incidente, basada en las guías NIST SP 800-61r3 y los controles CIS, aplicando medidas de contención, endurecimiento y remediación para restablecer la seguridad de los sistemas comprometidos. Finalmente, el documento integra los elementos técnicos, legales y éticos analizados a lo largo de las cinco etapas, estableciendo un marco de referencia para la comprensión de la relación entre las operaciones de ciberseguridad, el cumplimiento normativo y la responsabilidad profesional en el contexto colombiano.

Justificación

El notable aumento de incidentes informáticos en los últimos años, junto con la explotación de vulnerabilidades críticas y el mal uso de información sensible, pone de manifiesto la urgente necesidad de reforzar las capacidades técnicas, éticas y legales en el ámbito de la ciberseguridad. En este sentido, el caso de SecureNova Labs es un ejemplo claro donde se combinan fallas en la gestión, debilidades técnicas y riesgos profesionales que pueden poner en peligro tanto la integridad de los datos como la reputación de una organización.

Este estudio se justifica por la necesidad de entender de manera integral cómo interactúan los marcos normativos colombianos, los procedimientos ofensivos y defensivos (Red Team y Blue Team) y los procesos de respuesta a incidentes, especialmente en situaciones donde hay prácticas irregulares que violan la ley y comprometen la ética profesional. Analizar el caso desde diferentes perspectivas nos permite establecer criterios sólidos para la toma de decisiones, identificar brechas de seguridad, proponer medidas de mitigación y fomentar un comportamiento responsable en el ejercicio profesional.

Además, la implementación de metodologías reconocidas a nivel internacional (NIST, CIS, PTES, MITRE ATT&CK) y la práctica en un entorno controlado ofrecen evidencia técnica que respalda la importancia de adoptar medidas preventivas, correctivas y de gobernanza para mejorar la postura de seguridad de cualquier organización.

En este sentido, el estudio se justifica por la necesidad de analizar escenarios reales en los que decisiones inadecuadas, tanto técnicas como organizacionales, generan riesgos significativos para la seguridad de la información y la sostenibilidad institucional.

Objetivos

Objetivo general

Analizar el caso SecureNova Labs mediante la revisión del marco legal colombiano, la evaluación ética y profesional, y el desarrollo de actividades de Red Team y Blue Team, con el fin de identificar riesgos y vulnerabilidades y formular estrategias de contención que fortalezcan la seguridad de la infraestructura tecnológica.

Objetivos específicos

Examinar el marco legal colombiano que se relaciona con la ciberseguridad y la protección de la información, identificando las normas relevantes y cómo se conectan con las actividades que se llevaron a cabo en el caso de SecureNova Labs.

Evaluar, desde una perspectiva ética y profesional, las actuaciones desarrolladas en el contexto del caso propuesto, identificando posibles infracciones normativas, conflictos de interés y riesgos profesionales.

Desarrollar actividades de Red Team en un entorno controlado para detectar vulnerabilidades críticas, rutas de explotación y su impacto sobre los activos tecnológicos de la organización.

Aplicar técnicas de Blue Team y respuesta a incidentes mediante procesos de análisis, contención, remediación y recuperación, fundamentados en marcos internacionales reconocidos.

Formular recomendaciones estratégicas que ayuden a fortalecer la postura de seguridad de la organización mediante hardening, gestión de vulnerabilidades, cumplimiento normativo y mejora continua.

Etapa 1 - Fundamentos teóricos para operaciones Red Team y Blue Team

Esta sección ofrece un resumen del trabajo realizado en la Etapa 1 del curso, donde se establecen los fundamentos legales, metodológicos y técnicos que son esenciales para llevar a cabo de manera responsable las operaciones de Red Team y Blue Team en el contexto colombiano.

Marco Legal colombiano, base jurídica para ejercicios de ciberseguridad

El desarrollo de operaciones de Red Team y Blue Team en Colombia se sustenta en un marco jurídico robusto que establece los parámetros éticos, legales y procedimentales para la realización de evaluaciones de seguridad. Este marco garantiza que las pruebas de penetración y las actividades de ciberseguridad se ejecuten dentro de los límites legales, protegiendo tanto a las organizaciones como a los individuos afectados (Congreso de la República de Colombia, 2009, 2018).

Principales normativas que regulan las operaciones

Ley 1273 de 2009: Tipifica los delitos informáticos y protege la confidencialidad, integridad y disponibilidad de los datos y sistemas. Establece sanciones que incluyen multas y penas de prisión de hasta 120 meses (Congreso de la República de Colombia, 2009, cap. 1-2).

Ley 1928 de 2018: Adopta el Convenio de Budapest, facilitando la cooperación internacional contra el cibercrimen y estableciendo protocolos para la preservación de evidencia digital y la investigación transnacional (Congreso de la República de Colombia, 2018, Apéndice 1).

Ley 1581 de 2012: Regula la protección de datos personales, exigiendo autorización expresa para el tratamiento de información sensible y estableciendo los principios de legalidad, finalidad y confidencialidad (Congreso de la República de Colombia, 2012, art. 1).

Normativas complementarias

Como se ve en la **Tabla 1** el marco legal colombiano, crea un ecosistema regulado e integral que guía y restringe las actividades de ciberseguridad en el país, garantizando que se lleven a cabo de manera autorizada, ética y debidamente documentada.

Tabla 1

Normas complementarias del marco jurídico colombiano en protección de datos y ciberseguridad

Norma	Objeto	Ámbito de aplicación	Entidad responsable / autoridad	Aspectos clave y aportes
Decreto 1377 de 2013	Reglamenta parcialmente la Ley 1581 de 2012.	Aplicación práctica del tratamiento de datos personales.	Superintendencia de Industria y Comercio.	Regula la obtención de autorizaciones, la actualización de bases de datos y las políticas de privacidad.
Ley 1266 de 2008	Regula el manejo de datos financieros, crediticios y comerciales.	Entidades financieras y centrales de riesgo.	Superintendencia Financiera y SIC.	Desarrolla el *habeas data financiero*; garantiza derechos de los titulares frente a reportes crediticios.
Decreto 886 de 2014	Regula el Registro Nacional de Bases de Datos (RNBD).	Todas las entidades públicas y privadas.	SIC.	Obliga a registrar y reportar incidentes de seguridad sobre bases de datos personales.
CONPES 3854 de 2016	Define la Política Nacional de Seguridad Digital.	Sector público, privado y ciudadanía digital.	Ministerio TIC, Presidencia de la República.	Fortalece capacidades de ciberseguridad, infraestructura crítica y cooperación internacional.
Ley 1621 de 2013	Regula la actividad de inteligencia y contrainteligencia del Estado.	Fuerzas Armadas, organismos de inteligencia.	Presidencia de la República, Ministerio de Defensa.	Equilibra seguridad nacional con el respeto a los derechos fundamentales y la privacidad.
Ley 1712 de 2014	Regula el acceso a la información pública y la transparencia.	Entidades del Estado.	Procuraduría, Secretaría de Transparencia.	Promueve el acceso ciudadano a la información pública, respetando la protección de datos sensibles.

Nota. Elaboración propia con base en la normativa consultada en el portal Sistema Único de Información Normativa – SUIN Juriscol.

Metodología de pruebas de pentesting enfoque estandarizado

Las operaciones de Red Team se fundamentan en metodologías internacionalmente reconocidas que garantizan un abordaje sistemático, reproducible y comparable. La integración de estándares como PTES, MITRE ATT&CK (MITRE Corporation, 2024), NIST SP 800-115 y OWASP permite contextualizar las técnicas de ataque dentro de frameworks probados (Penetration Testing Execution Standard [PTES], 2014; National Institute of Standards and Technology [NIST], 2008).

Fases metodológicas

Plani**ficación y Autorización:** Establecimiento de alcances, obtención de permisos formales y definición de reglas de compromiso (PTES, 2014).

Reconocimiento: Recolección de inteligencia mediante técnicas pasivas (OSINT) y activas (escaneos de red) (NIST, 2008; PTES, 2014). El objetivo final es reconocer y documentar el entorno y preparar una estrategia de ataque informada, minimizando la probabilidad de detección o daño no intencional.

Enumeración y Mapeo: Identificación de activos, servicios y relaciones dentro del entorno (Herzog, 2010; OWASP Foundation, 2021). Y de esta forma sentar las bases para el análisis de vulnerabilidades y la explotación posterior.

Análisis de Vulnerabilidades: Identificación y priorización de debilidades usando estándares como CVE (MITRE Corporation, s. f.) y CVSS (NIST, 2008; MITRE Corporation, 2023).

Explotación Controlada: Requiere procesos metódicos y un conjunto de técnicas y tácticas específicas cuyo objetivo es ganar acceso a sistemas y recursos concretos mediante la explotación de debilidades identificadas en etapas previas, con el fin de demostrar el impacto empresarial de dichas vulnerabilidades.

Marcos como MITRE ATT&CK (MITRE Corporation, 2025), resultan esenciales en esta fase, ya que proporcionan un catálogo estandarizado de tácticas, técnicas y procedimientos (TTPs) utilizados por adversarios reales. Esto permite contextualizar las acciones de explotación dentro de un marco de referencia reconocido internacionalmente, facilitando la comunicación de hallazgos y la alineación con estrategias de defensa

Post-explotación: Su propósito no es volver a explotar la vulnerabilidad (eso ya ocurrió en el paso anterior), sino evaluar el valor del acceso obtenido, mantener o maximizar ese acceso (según el alcance autorizado), descubrir qué otros activos o redes pueden alcanzarse desde ese punto.

Reporte y presentación: Comprende la compilación, validación y transmisión formal de los hallazgos del test a las partes interesadas. Esta fase puede realizarse conforme a las pautas de proceso y calidad por ejemplo del (PTES, 2014), la estructura formal y exigencias de documentación del NIST SP 800-115, y los controles de gobernanza y entrega profesional de CREST.

En la **Tabla 2** se resumen algunas de las herramientas más usadas en cada una de las diferentes etapas de las pruebas de penetración es de aclarar que muchas de estos recursos se deben usar de forma responsable con autorización informada al cliente y preferiblemente formalizados en la etapa de planificación.

Tabla 2

Resumen de herramientas usadas en las diferentes fases de Pentesting

Etapa	Objetivo Principal	Actividades Clave	Herramientas Representativas
1. Planificación y Autorización	Establecer alcance, permisos y reglas de compromiso	Definir objetivos, obtener autorizaciones, documentar acuerdos	Trello, Jira, Slack, Microsoft Teams, Risk Register
2. Reconocimiento	Recolectar inteligencia del objetivo	OSINT, escaneos pasivos y activos, descubrimiento de activos	Shodan, theHarvester, Nmap, Sublist3r, Google Dorks
3. Enumeración y Mapeo	Identificar servicios y relaciones en el entorno	Escaneo de puertos, fingerprinting, fuzzing, enumeración	Nmap, DirBuster, Gobuster, Maltego, Burp Suite
4. Análisis de Vulnerabilidades	Identificar y priorizar debilidades	Escaneo de vulnerabilidades, correlación con CVE/CVSS	Nessus, OpenVAS, Nexpose, NVD
5. Explotación Controlada	Demostrar impacto mediante acceso no autorizado	Ejecución de exploits, validación de vulnerabilidades	Metasploit, Burp Suite, sqlmap, Hashcat
6. Post-Explotación	Evaluar persistencia y movimiento lateral	Análisis de credenciales, mapeo de privilegios, pivoting	Mimikatz, BloodHound, CrackMapExec, Impacket
7. Informe y Documentación	Comunicar hallazgos y recomendaciones	Elaboración de reportes, presentación de resultados	Microsoft Office, LaTeX, herramientas de documentación

Nota. El contenido de esta tabla fue consolidado y elaborado a partir del análisis de los marcos metodológicos PTES (PTES, 2014), NIST SP 800-115 y OWASP, integrando las etapas del pentesting

Buenas prácticas y ética profesional

Más allá del dominio técnico, la ejecución de pruebas de penetración se rige por buenas prácticas fundamentales. Entre ellas destacan: la obtención de autorización expresa y documentada antes de cualquier prueba, la comunicación constante con el cliente, la clasificación de hallazgos por riesgo e impacto, y la elaboración de informes claros y accionables que prioricen la remediación. Estas prácticas, alineadas con estándares como PTES (PTES, 2014) y

NIST, garantizan que los ejercicios se realicen de manera legal, segura y profesional, fortaleciendo la confianza con el cliente y el valor del servicio.

Herramientas técnicas y entorno de pruebas

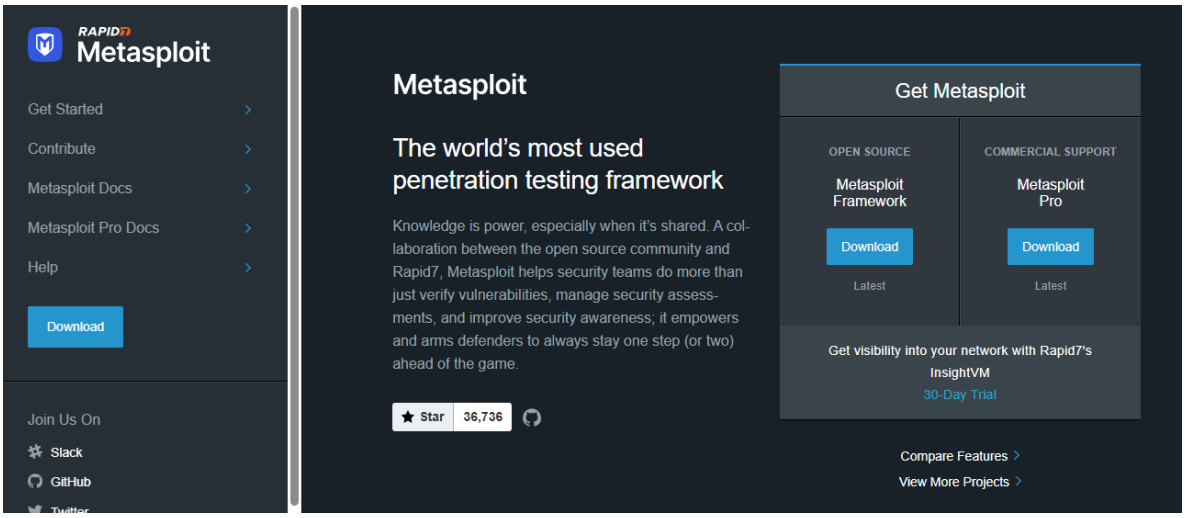
La efectividad de las operaciones de ciberseguridad depende críticamente de la selección adecuada de herramientas especializadas y la configuración de entornos controlados que simulen condiciones reales sin afectar sistemas productivos (StationX, 2025).

Herramientas que se pueden emplear

Metasploit Framework: Plataforma integral para desarrollo y ejecución de exploits (Rapid7, 2024). Como se muestra en la **Figura 1**, su interfaz centraliza módulos de explotación, payloads y herramientas post-explotación.

Figura 1

Página principal del framework Metasploit



Nota. Print screen tomado de Metasploit (2024).

Nmap: Herramienta de descubrimiento de red y escaneo de servicios (Nmap, 2023.). Su versatilidad permite realizar desde escaneos básicos de descubrimiento hasta enumeración

avanzada de servicios y vulnerabilidades. La **Tabla 3** resume los comandos más utilizados en operaciones de pentesting, clasificados por categoría y uso práctico.

Tabla 3

Tabla de Algunos Comandos Básicos de Nmap

Categoría	Comando	Utilidad Principal	Ejemplo Práctico	Uso en Pentesting
Descubrimiento	`nmap -sn <target>`	Descubre hosts activos (sin escanear puertos)	`nmap -sn 192.168.1.0/24`	Fase inicial de reconocimiento
Escaneo TCP	`nmap -sS <target>`	Escaneo SYN stealth (rápido y sigiloso)	`nmap -sS 10.0.1.10`	Escaneo estándar en pentesting
Escaneo TCP	`nmap -sT <target>`	Escaneo TCP connect (sin req. root)	`nmap -sT 10.0.1.10`	Cuando no hay permisos de root
Escaneo UDP	`nmap -sU <target>`	Escaneo puertos UDP	`nmap -sU -p 53,161 10.0.1.10`	Para DNS, SNMP, DHCP
Puertos	`nmap -p <puertos>`	Escanear puertos específicos	`nmap -p 22,80,443 10.0.1.10`	Enfoque en servicios conocidos
Puertos	`nmap -p- <target>`	Escanear TODOS los puertos TCP	`nmap -p- 10.0.1.10`	Escaneo exhaustivo
Detección	`nmap -sV <target>`	Detección de versiones de servicio	`nmap -sV 10.0.1.10`	Fingerprinting de servicios
Detección	`nmap -O <target>`	Detección de sistema operativo	`nmap -O 10.0.1.10`	Fingerprinting de SO
Completo	`nmap -A <target>`	Escaneo agresivo (todo en uno)	`nmap -A 10.0.1.10`	Máxima información posible
Scripts NSE	`nmap --script <script>`	Ejecutar scripts específicos	`nmap --script http-enum`	Enumeración web
Scripts NSE	`nmap --script vuln`	Escanear vulnerabilidades	`nmap --script vuln 10.0.1.10`	Detección de vulnerabilidades
Scripts NSE	`nmap --script safe`	Scripts no intrusivos	`nmap --script safe 10.0.1.10`	Enumeración básica

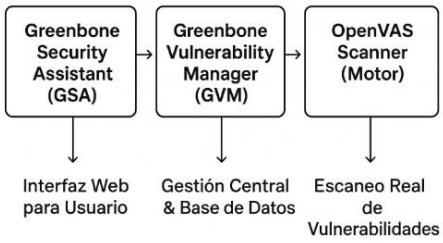
Velocidad	`nmap -T0-T5`	Control de velocidad (0=lento, 5=rápido)	`nmap -T4 10.0.1.10`	Balance velocidad/stealth
Evasión	`nmap -Pn`	Salta descubrimiento de hosts	`nmap -Pn 10.0.1.10`	Cuando ICMP está bloqueado
Evasión	`nmap -f`	Fragmenta paquetes	`nmap -f 10.0.1.10`	Evasión de firewalls
Salida	`nmap -oN archivo`	Salida normal (texto)	`nmap -oN resultado.txt`	Reportes legibles
Salida	`nmap -oX archivo`	Salida XML	`nmap -oX resultado.xml`	Para importar a herramientas
Salida	`nmap -oG archivo`	Salida grepable	`nmap -oG resultado.gnmap`	Para procesar con scripts
Objetivos	`nmap -iL archivo`	Escanear lista desde archivo	`nmap -iL hosts.txt`	Múltiples objetivos

Nota. Datos adaptados de “Port scanning basics”, Nmap Network Scanning (Nmap, 2023), https://nmap.org/book/man-port-scanning-basics.html).

OpenVAS/Greenbone: Sistema avanzado de escaneo de vulnerabilidades (Greenbone Networks GmbH, s.f.). Su arquitectura, ilustrada en la **Figura 2**, sigue un modelo cliente-servidor compuesto por el Security Assistant (GSA), el Vulnerability Manager (GVM) y el motor de escaneo OpenVAS.

Figura 2

Interacción entre los componentes GSA, GVM y OpenVAS.



Nota. Imagen adaptada a partir de Greenbone Security Manager Manual (GOS 24.10) (Greenbone Networks GmbH, 2024, https://docs.greenbone.net/GSM-Manual/gos-24.10/en/)

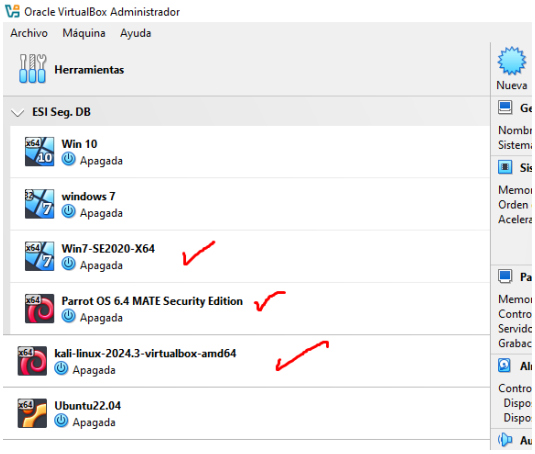
ExploitDB y CVE: (Exploit Data Base) funciona como un repositorio centralizado de exploits y pruebas de concepto, mientras que el sistema CVE proporciona identificadores únicos estandarizados para vulnerabilidades conocidas. Juntos, permiten validar y contextualizar hallazgos durante auditorías de seguridad, facilitando la priorización de remediaciones (Offensive Security, 2025; MITRE Corporation, s.f.).

Configuración del entorno de pruebas

Mediante el uso de VirtualBox, se configuró un banco de trabajo con máquinas virtuales que incluyen Kali Linux, Parrot OS, Windows 7 y Windows 10, interconectadas en una red aislada **Figura 3**. Este laboratorio seguro, permite la ejecución de técnicas ofensivas y defensivas en un entorno controlado, facilitando el aprendizaje experiencial y la validación de procedimientos.

Figura 3

Maquinas instaladas para banco de pruebas

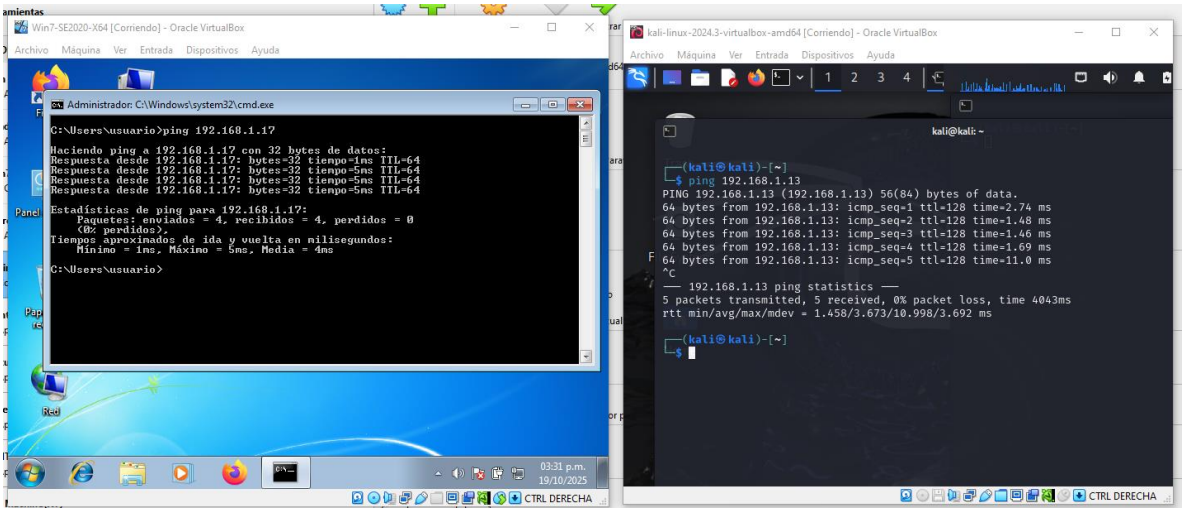


Nota. Elaboración propia (2025)

La conectividad entre sistemas se verificó mediante pruebas de ping, evidenciando la correcta comunicación entre máquinas, como se muestra en **Figura 4**, para el caso entre Windows 7 y Kali Linux.

Figura 4

Prueba de comunicación Win7-Kali



Nota. Elaboración propia (2025)

Visión integral de la ciberseguridad

La ciberseguridad efectiva requiere la integración de múltiples dimensiones:

- Un marco legal sólido que oriente y limite las acciones.
- Metodologías estandarizadas que aseguren el rigor y la reproducibilidad.
- Herramientas técnicas especializadas para la ejecución de pruebas.
- Entornos controlados que faciliten la práctica segura y el aprendizaje continuo.

Esta síntesis teórica es la base esencial sobre la que se llevarán a cabo las operaciones prácticas de Red Team y Blue Team. Debe complementarse con los hallazgos empíricos de las etapas posteriores para crear una evaluación completa de la postura de seguridad de la organización. La combinación de un enfoque metodológico riguroso, conocimientos técnicos y el

cumplimiento de la normativa legal establece el estándar profesional para los ejercicios de ciberseguridad en el contexto colombiano.

Etapa 2 - Ética profesional y marco legal en procedimientos de ciberseguridad

Esta sección ofrece un resumen del trabajo realizado en la Etapa 2 del curso, que se enfoca en el análisis ético y legal de los procedimientos de ciberseguridad. Aquí se reúnen los hallazgos sobre las implicaciones normativas, los riesgos profesionales y los mecanismos de control necesarios para asegurar una práctica responsable en situaciones del mundo real.

Análisis crítico del acuerdo de confidencialidad de SecureNova Labs

Como se evidencia en el Acuerdo de Confidencialidad proporcionado como material del curso, ver **Apéndice B** para el documento completo, se evidencian irregularidades que convierten un instrumento de protección legal en un potencial riesgo profesional. El documento examinado incluye cláusulas que mencionan la inclusión de "procesos ilegales" como información confidencial, prohibiendo de manera específica la denuncia de actividades sospechosas de espionaje ante las autoridades, lo que podría interpretarse como encubrimiento de delitos (Cláusula Cuarta, punto 3; Cláusula Primera, p. 3).

Problemas fundamentales identificados

- Cláusulas de encubrimiento que protegen prácticas ilegales como información confidencial (Cláusula Primera, p. 3)
- Prohibición expresa de denuncia de actividades delictivas ante autoridades competentes (Cláusula Cuarta, punto 3)
- Transferencia inequitativa de responsabilidad hacia el profesional, eximiendo a la empresa incluso ante posesión de información ilegal (Cláusula Octava, p. 5)
- Terminología sospechosa que incluye términos como "interceptación de información", "accesos abusivos" y "chuzadas" sin definición precisa (Cláusula Segunda, punto 2)

Vulneraciones al marco normativo colombiano

El acuerdo analizado contraviene disposiciones esenciales de la Ley 1273 de 2009 sobre delitos informáticos, particularmente los artículos 269A (acceso abusivo a sistemas informáticos), 269C (interceptación de datos) y 269F (violación de datos personales). Al incluir estas conductas punibles como información confidencial, el documento busca proteger actividades explícitamente prohibidas por la ley colombiana (Congreso de la República de Colombia, 2009).

La aceptación de tales cláusulas podría convertir al profesional en cómplice o encubridor de delitos informáticos, generando responsabilidad penal directa y violando el deber fundamental de denuncia, establecido en el ordenamiento jurídico

Riesgos éticos y profesionales

La suscripción del acuerdo comprometería gravemente la integridad profesional del especialista en ciberseguridad, contraviniendo el Código de Ética del COPNIA establecido en la Ley 842 de 2003. El deber profesional de denunciar delitos se ve directamente vulnerado por la prohibición expresa de reportar actividades sospechosas de espionaje (Consejo Profesional Nacional de Ingeniería, 2015, Art. 31, literal f).

Consecuencias profesionales potenciales

Si el profesional decide participar en este tipo de conducta irregular, podría enfrentarse a las siguientes consecuencias:

- Responsabilidad penal por encubrimiento, al contribuir directa o indirectamente en la ocultación de un hecho ilícito.
- Sanciones disciplinarias del COPNIA, conforme al régimen ético aplicable a los profesionales de la ingeniería en Colombia.

- Cancelación de la matrícula profesional, según lo establecido en el artículo 53 de la Ley 842 de 2003.
- Afectación grave e irreversible a su reputación dentro de la comunidad de ciberseguridad, limitando futuras oportunidades laborales o de colaboración profesional.

Propuesta de marco ético y legal alternativo

Frente a los riesgos identificados, se propone un acuerdo de confidencialidad equilibrado fundamentado en el principio de autonomía de la voluntad (Artículo 1602 del Código Civil) y la cláusula penal proporcional (Artículo 867 del Código de Comercio) (Congreso de la República de Colombia, 1887; Congreso de la República de Colombia 1971).

Elementos esenciales para un acuerdo ético contractual:

- Definición precisa, verificable y legalmente exigible de la información confidencial, evitando ambigüedades que generen riesgos de interpretación.
- Restricción de uso estrictamente limitado a los fines contractuales, excluyendo cualquier utilización no autorizada o incompatible con el objeto del contrato.
- Implementación de medidas de seguridad técnica y organizativa, acorde con estándares nacionales e internacionales de protección de datos y seguridad de la información.
- Mecanismos de supervisión, registro y trazabilidad de accesos, asegurando auditoría continua y responsabilidad en el manejo de la información.
- Cláusulas de terminación automática ante conductas ilegales o violaciones graves, protegiendo tanto a la organización como al profesional frente a riesgos jurídicos y éticos.

Mecanismos de control para herramientas forenses

Surakanti et al. (2025) presentan una revisión sistemática sobre técnicas anti-forenses y sus contramedidas, destacando que las herramientas forenses pueden ser vulnerables no solo frente a atacantes externos, sino también ante insider threats con conocimientos avanzados capaces de manipular evidencias o interferir en investigaciones internas. El estudio identifica mecanismos que pueden adaptarse al entorno empresarial como controles preventivos, los cuales se sintetizan en la **Tabla 4**:

Tabla 4

Técnicas anti-forenses

Mecanismo propuesto	(Surakanti et al., 2025)	Aplicación empresarial
Gestión centralizada de logs (SIEM)	Sección 5.3.1	Monitorizar comandos y accesos de herramientas forenses.
Monitoreo de integridad de archivos (FIM)	Sección 5.3.2	Detectar modificaciones o instalación de herramientas no homologadas.
Separación de funciones y auditoría cruzada	Sección 5.3.2	Aplicar el principio de “cuatro ojos” en investigaciones críticas.
Control de acceso de mínimo privilegio	Sección 5.3.1	Limitar accesos a evidencias y herramientas sensibles.
Copias de seguridad inmutables	Sección 5.3.2	Mantener repositorios de evidencias inalterables (“golden copy”).
Capacitación ética continua	Sección 5.2.1	Fortalecer cultura de responsabilidad profesional.
Procedimientos operativos estandarizados (SOPs)	Sección 5.3.2	Estandarizar procesos y detectar desviaciones sospechosas.

Nota. Adaptado de “Countering anti-forensic tactics in cybercrime investigations – a systematic literature review” por S. Surakanti, C. Göbel y K. Conlan, International Journal of Information Security, 24(3), 155–179 (2025). https://doi.org/10.1007/s10207-025-01131-y

El estudio concluye expresamente que:

"the reliability of DF tools is questioned… the tools and methods currently employed in DF are not entirely sufficient to stop the sneaky tactics employed by cybercriminals" (Surakanti et al., 2025, sec. 5.5). [La fiabilidad de las herramientas de informática forense ha sido objeto de cuestionamiento, dado que los métodos y técnicas actualmente empleados no resultan completamente adecuados para contrarrestar las tácticas cada vez más sigilosas utilizadas por los ciberdelincuentes] (Traducción propia).

Esto significa que si las herramientas pueden ser vulneradas por actores externos, el riesgo se eleva aún más cuando quien las manipula es un experto interno que conoce sus debilidades. Para reducir estos riesgos, es fundamental contar con una combinación de controles técnicos *NIST SP 800-86* (Kent et al., 2006) y estructuras de gobernanza y calidad como la NTC-ISO/IEC 17025:2018. Esto permite establecer un sistema integral que proteja tanto la infraestructura tecnológica como la ética profesional.

A nivel general se puede implementar este marco con la siguiente estructura:

- La NTC-ISO/IEC 17025:2018 (ICONTEC, 2018) como marco de gobierno general
- La *NIST SP 800-86* (Kent et al., 2006) como guía de implementación técnica forense
- Controles específicos derivados de ambos para:
    - Inventario y control de herramientas forenses
    - Monitoreo de uso privilegiado
    - Auditoría de actividades forenses
    - Capacitación ética especializada

Desde NIST SP 800-86:

- Control de acceso a herramientas forenses (Sección 3.1)
- Registro y monitoreo de actividades forenses (Sección 3.3)
- Separación de responsabilidades en investigaciones (Sección 2.2)

Desde la NTC-ISO/IEC 17025:2018 (ICONTEC, 2018):

- Concienciación del personal y control de competencias (6.2).
- Definición y separación de responsabilidades (4.1 y 6.2).
- Registro y control de datos técnicos (7.5).
- Auditorías internas y revisiones de gestión (8.8 y 8.9).

Como enfatizan Surakanti et al. (2025) la supervisión permanente es indispensable, los mismos conocimientos que permiten proteger también pueden usarse para vulnerar. En síntesis, la institucionalización de los siguientes tres principios es primordial:

- La tecnología debe auditarse,
- Los procedimientos deben validarse
- Y las personas deben ser formadas bajo principios demostrables de imparcialidad, confidencialidad y responsabilidad.

Juntos, estos componentes integran los lineamientos técnicos del *NIST SP 800-86* (Kent et al., 2006) y los principios de calidad y competencia que establece la *NTC-ISO/IEC 17025:2018* (ICONTEC, 2018), consolidando la práctica ética y segura en el área de la ciberseguridad empresarial.

Marco de respuesta ante ciberespionaje

Cuando una empresa de ciberseguridad es descubierta realizando ciberespionaje, enfrenta daños legales, operativos y especialmente reputacionales. Por ello, la organización afectada debe reaccionar con rapidez, claridad y transparencia para limitar el daño, garantizar justicia y recuperar la confianza perdida.

La respuesta puede organizarse en cuatro etapas:

Respuesta inmediata: activar protocolos de emergencia, aislar sistemas comprometidos y preservar evidencia digital para detener el impacto.

Investigación y acciones legales: realizar una investigación exhaustiva, identificar responsables, determinar normas o contratos vulnerados y aplicar sanciones y reparaciones.

Restablecimiento de confianza: comunicar los hechos con transparencia, explicar las medidas adoptadas y demostrar responsabilidad institucional para recuperar la credibilidad.

Prevención y reforma: revisar procesos de selección, contratación y supervisión de proveedores de ciberseguridad, fortaleciendo controles y ajustando políticas para evitar recurrencia.

En Colombia, este proceso se soporta en un marco institucional sólido. El ColCERT, el SOC Nacional del MinTIC, el Comité Nacional de Seguridad Digital, la Estrategia Nacional de Seguridad Digital 2025–2027 y los documentos CONPES que permiten coordinar la respuesta ante incidentes y proteger infraestructuras críticas.

El marco jurídico complementa esta estructura:

Ley 1273 de 2009, que sanciona delitos informáticos como acceso indebido, daño a datos o uso de software malicioso.

Ley 1581 de 2012, que regula el tratamiento y la protección de datos personales.

Restaurar la confianza, sin embargo, sigue siendo el mayor desafío, requiere no solo medidas técnicas, sino también transparencia, ética, supervisión continua y comunicación abierta con los afectados. Solo mediante este enfoque integral es posible fortalecer la resiliencia institucional y mantener la credibilidad en un entorno digital que es más exigente a cada momento.

El análisis del caso SecureNova Labs demuestra que no hay beneficio económico que valga la pena si eso significa aceptar acuerdos que pongan en riesgo la integridad ética y legal del profesional. En el ámbito de la ciberseguridad, es crucial encontrar un equilibrio entre las habilidades técnicas y el cumplimiento normativo, donde la transparencia y la supervisión son pilares esenciales (Flechais & Chalhoub, 2023). Colombia tiene un marco jurídico e institucional sólido para enfrentar estos retos, combinando la Ley 1273 de 2009, la Ley 1581 de 2012 y estructuras especializadas como la Estrategia Nacional de Seguridad Digital.

Un profesional ético siempre debe priorizar el cumplimiento de la ley y la protección de los derechos fundamentales por encima de cualquier contrato abusivo (Flechais & Chalhoub, 2023).

Etapa 3 - Ejercicio práctico de operaciones Red Team

Esta sección ofrece un resumen del ejercicio práctico de la Etapa 3 del curso, donde se utiliza el escenario de SecureNova Labs para crear un entorno simulado y controlado permitiendo entender de forma segura cómo se comporta un atacante en situaciones del mundo real.

Ejecución ejercicio de simulación ofensiva Red Team desarrollo metodológico

El ejercicio práctico recreó un escenario de intrusión simulado en SecureNova Labs, donde un atacante lograba comprometer el equipo Host-A a través de una vulnerabilidad, escalaba privilegios y se movía lateralmente hacia Host-B para acceder a información sensible. En un laboratorio aislado, se replicaron estas acciones de manera controlada, validando los vectores de ataque y generando la evidencia técnica, la línea de tiempo forense y el plan de remediación correspondiente.

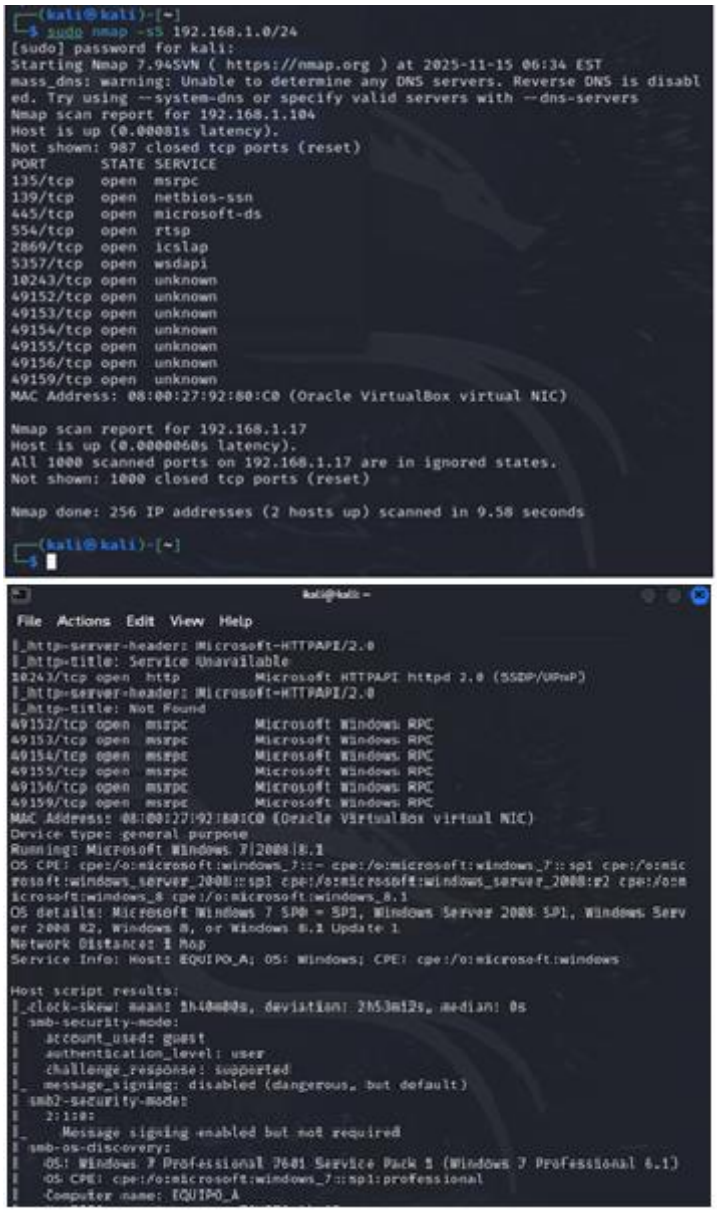
Fase de reconocimiento y análisis de vulnerabilidades

El proceso inició con el reconocimiento de la red 192.168.1.0/24 mediante herramientas especializadas como (Nmap, 2023), identificando al Host-A (192.168.1.104) como objetivo primario.

El análisis detallado reveló configuraciones críticas: sistema Windows 7 SP1 con servicio SMBv1 habilitado en puerto 445/tcp y firma de mensajes desactivada, combinación que representaba un riesgo significativo **Figura 5**.

Figura 5

Resultados usando el comando, sudo namap



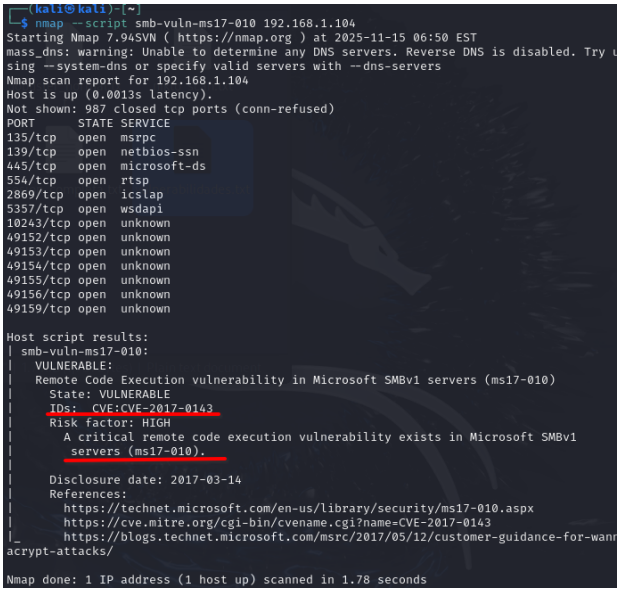
Nota. Con este comando se detecta host con dirección 192.168.1.104

Fase de explotación y post-explotación

La confirmación de la vulnerabilidad MS17-010 /EternalBlue (Microsoft, 2017), asociada al CVE-2017-0143 (INCIBE, 2025), estableció el vector de ataque principal **Figura 6**. Esta falla crítica, combinada con la ausencia de controles de integridad en SMB, creó las condiciones ideales para la explotación sin requerir credenciales iniciales.

Figura 6

Resultado escaneo de vulnerabilidad ms17-010



Nota. Se confirma la vulnerabilidad critica CVE-2017-0143 (INCIBE, 2025).

Explotación Exitosa del Host-A

La ejecución del módulo *exploit/windows/smb/ms17_010_eternalblue* desde Metasploit resultó en un compromiso inmediato del sistema, obteniendo una sesión Meterpreter con privilegios administrativos completos **Figura 7**. Este acceso permitió el control total del Host-A, validando la criticidad de la vulnerabilidad identificada.

Figura 7

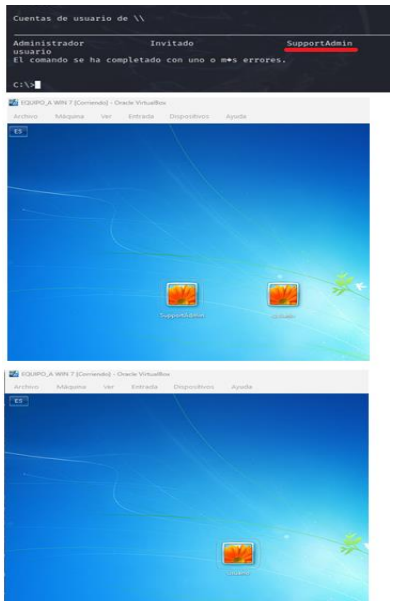
Éxito total del ms17_010_eternalblue elegido como primera opción

Nota. Se evidencia el éxito del ataque verificando que ya se visualiza el prompt característico de Windows.

Para garantizar persistencia, se implementaron mecanismos de mantenimiento de acceso mediante la creación del usuario administrativo SupportAdmin, posteriormente ocultado mediante modificaciones en el registro de Windows **Figura 8**.

Figura 8

Evidencia de usuario oculto en la pantalla de inicio de Windows



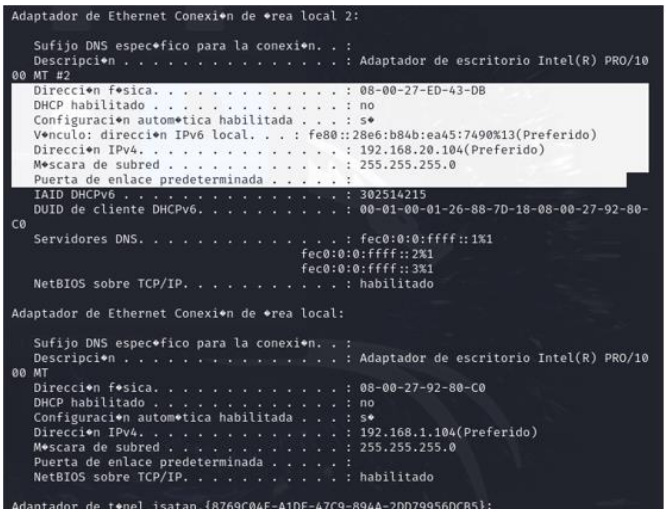
Nota. Esta técnica demostró la capacidad de evadir controles básicos de supervisión.

Estrategia de pivoting y movimiento lateral

Desde la sesión comprometida en Host-A **Figura 9**, se identificó una segunda interfaz de red conectada a la subred 192.168.20.0/24, supuestamente aislada.

Figura 9

Evidencia de redes conectadas en el Equipo A

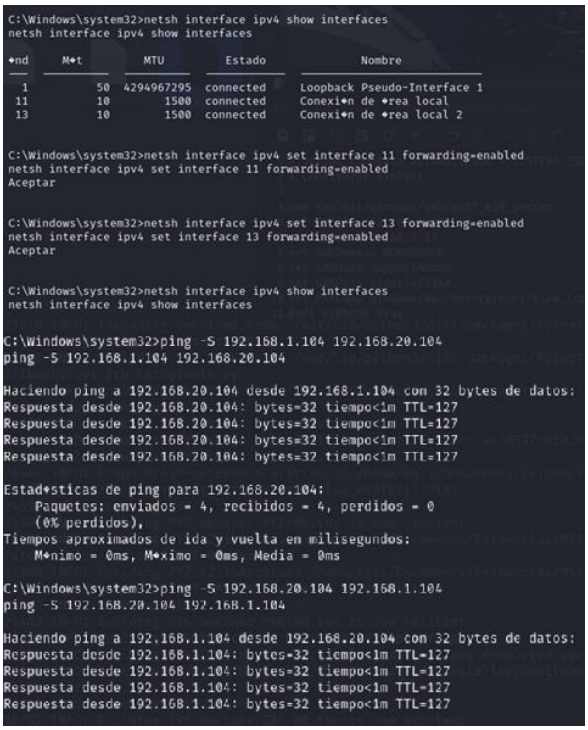


Nota. Los datos de la nueva red encontrada están resaltados, que precisamente es la 192.168.20.0/24.

La habilitación del reenvío de IP mediante registros del sistema y comandos netsh **Figura 10**, transformó al Host-A en un punto de pivote efectivo.

Figura 10

Activación de IP forwarding en Host-A y verificación de la conexión

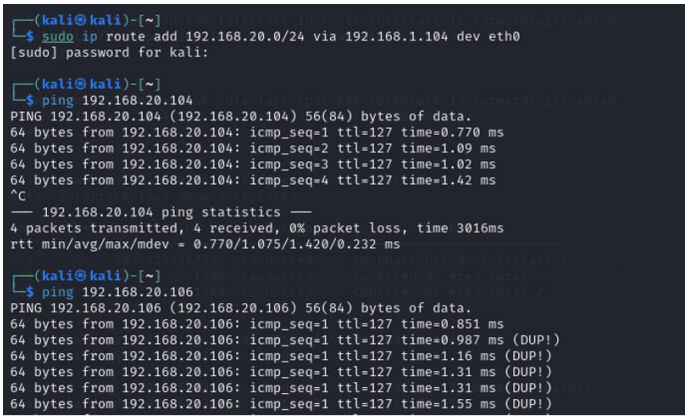


Nota. De esta forma se tiene conexión directa en el equipo A desde la red 10 a la red 20 y viceversa.

La configuración de rutas persistentes en Kali Linux permitió el enrutamiento de tráfico a través del Host-A comprometido, validando la conectividad con la red secundaria y demostrando fallas críticas en la segmentación de red **Figura 11**.

Figura 11

Configuración y prueba de conectividad a la red 20 desde el equipo Kali



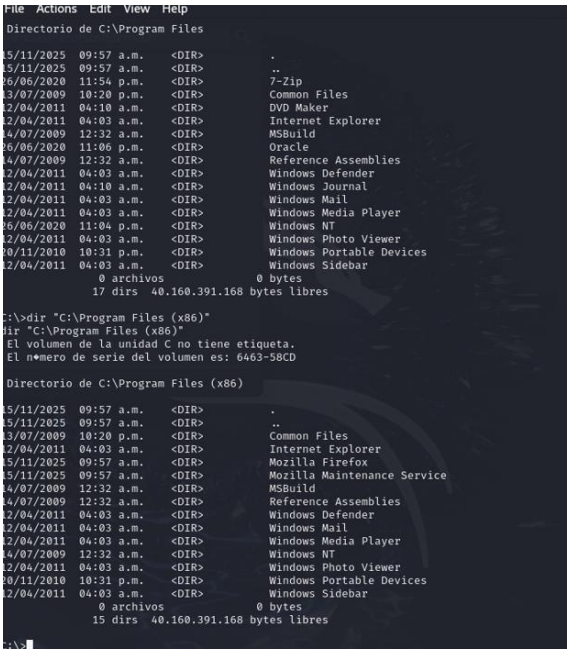
Nota. Para el caso se verifica una conexión estable, TTL=127 indica que los paquetes están pasando por routers/intermediarios esto confirma que el equipo A, está funcionando como pivot.

Compromiso del Host-B y Exfiltración de Datos

El análisis del Host-B reveló configuraciones similares al Host-A **Figura 12**, pero se optó por una estrategia de explotación alternativa mediante la vulnerabilidad firefox_proxy_prototype.

Figura 12

Enumeración de programas instalados en el Equipo_A

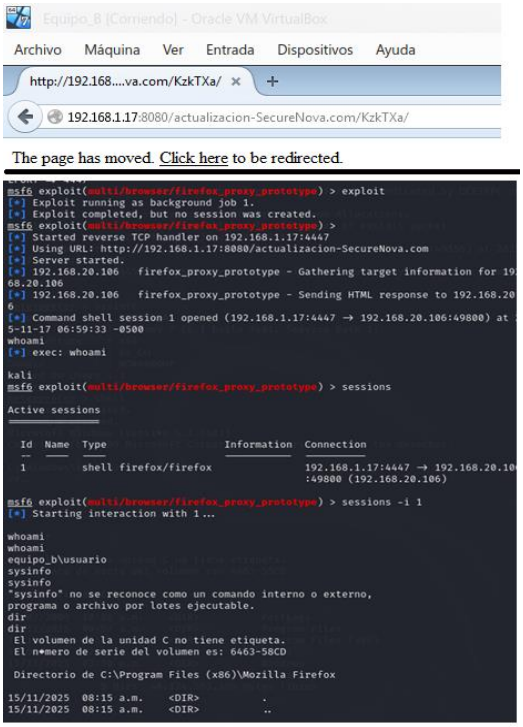


Nota. La verificación se realiza tanto en Progam Files como en Program Files (x86) del equipo A aprovechando la similitud de la arquitectura, donde se encuentran varios candidatos explotables.

Esta aproximación, combinada con técnicas de ingeniería social, permitió obtener acceso administrativo sin recurrir a EternalBlue **Figura 13**.

Figura 13

Resultado del ataque con proxy_prototype

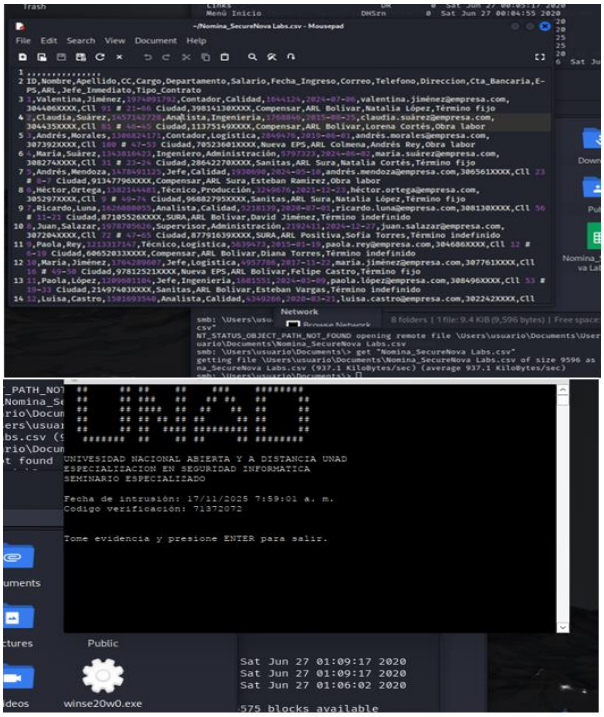


Nota. Se evidencia el ingreso a una sesión shell para el equipo B desde el equipo Linux aprovechando un Firefox vulnerable.

La fase final demostró el impacto operacional mediante la exfiltración del archivo Nomina_SecureNova_Labs.csv, conteniendo información sensible de nómina con datos personales críticos **Figura 14**. Este procedimiento validó la cadena completa de compromiso, desde el acceso inicial hasta la extracción de información confidencial.

Figura 14

Bandera para evidencia de éxito del ataque



Nota. Se puede ver claramente que el archivo Nomina contiene información como nombre de empleados, cuentas bancarias, teléfonos y direcciones, al estar expuesto representa un impacto grande en cuanto al manejo y protección de datos personales.

El ejercicio reveló algunas debilidades en la postura de seguridad de la infraestructura de SecureNova Labs. La combinación de vulnerabilidades técnicas no resueltas y controles insuficientes permitió que toda la cadena de compromiso se desarrollara sin ser detectada por los mecanismos de defensa. La exitosa exfiltración de información personal resalta el posible incumplimiento de la Ley 1581 de 2012 sobre la protección de datos (Congreso de la República de Colombia, 2012), lo que añade un aspecto legal al impacto técnico identificado. Además, la persistencia demostrada a través de usuarios ocultos subraya la necesidad de implementar mecanismos de detección más avanzados y un monitoreo continuo.

Este ejercicio práctico valida la importancia crucial de tener programas actualizados y de fuentes seguras, gestión de parches, una configuración segura de los servicios, una segmentación de red efectiva y capacidades sólidas de detección y respuesta ante incidentes.

Etapa 4 - Respuesta y contención ante incidentes de seguridad

Esta sección ofrece un resumen de la Etapa 4 del curso, que se centra en el análisis del proceso de respuesta y contención aplicado al incidente simulado en SecureNova Labs. El objetivo fue entender, de manera práctica y metodológica, cómo se manejan los ataques reales a través de procedimientos estandarizados, análisis forense y acciones técnicas de mitigación.

Una vez que se han identificado y explotado los vectores de ataque, el siguiente paso crucial es la contención y remediación, que es la principal responsabilidad del Blue Team. A continuación, se detalla este proceso.

Análisis técnico y contención inmediata

El análisis forense reveló una secuencia de ataque bien organizada, cuya evolución se pudo entender a través de las fases descritas en la guía NIST SP 800-61r3 para el manejo de incidentes (preparación, detección y análisis, contención, erradicación y recuperación), siguiendo las recomendaciones de Nelson, Rekhi, Souppaya y Scarfone (2025). La primera fase se centró en implementar medidas rápidas para frenar el ataque sin comprometer la evidencia forense crucial.

Las acciones de contención inmediata se focalizaron en implementar controles críticos siguiendo las mejores prácticas del CIS (CIS, 2023). El primer movimiento consistió en aislar de sistemas comprometidos sin interrumpir evidencia volátil:

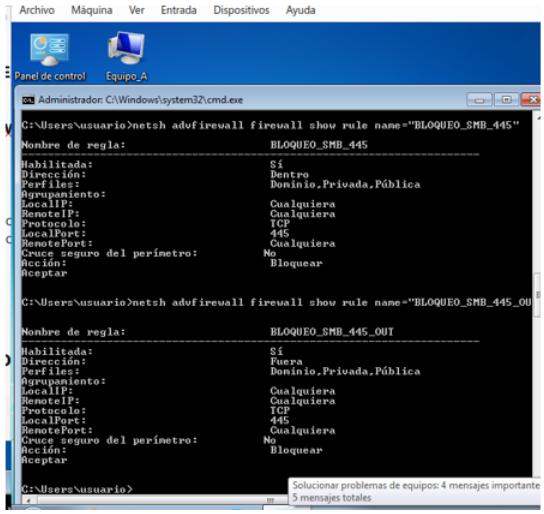
Equipo-A (192.168.1.104): Desconexión inmediata mediante desconexión de interfaz de red y bloqueo de comunicaciones entrantes/salientes.

Equipo-B (192.168.20.106): Aislamiento completo para prevenir exfiltración adicional de datos sensibles.

Lo segundo en importancia fue realizar el bloqueo del puerto 445/SMB **Figura 15**, mediante reglas de firewall específicas.

Figura 15

Evidencia de reglas de firewall aplicadas

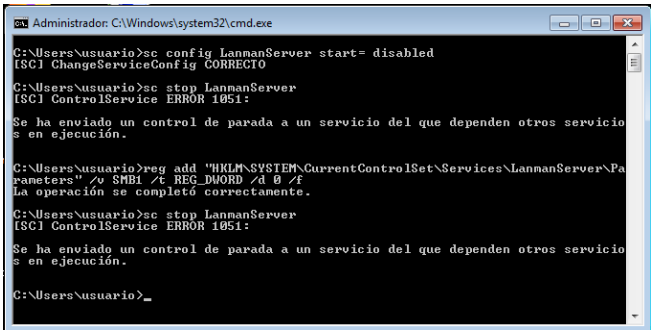


Nota. Estas acciones se aplican tanto ara el equipo A como para el equipo B

En seguida se detienen los servicios LanmanServer y Browser como se demuestra en la **Figura 16**.

Figura 16

Detención de servicios LanmanServer y Browser

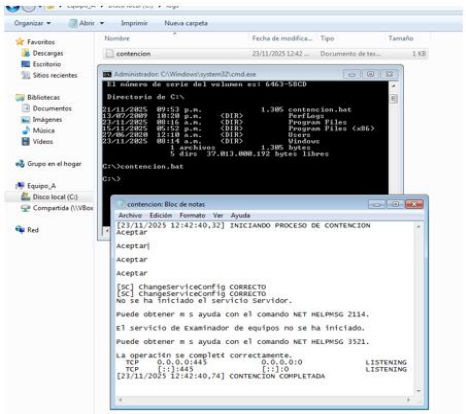


Nota. La medida no es efectiva al 100% ya que muchos servicios del Kernel dependen del puerto 445, por esto estas medidas se consideran temporales hasta aplicar el hardening correspondiente.

Para asegurar una mayor agilidad y precisión en la implementación de las contramedidas, se desarrollan y ponen en marcha procesos automatizados que configuran los controles necesarios **Figura 17**. Esto es especialmente importante en infraestructuras amplias y homogéneas, ya que permite replicar las medidas de manera rápida, uniforme y con un margen de error reducido.

Figura 17

Ejecución del script de contención



Nota. El script completo y los logs de ejecución se encuentran en **Apéndice C**. Para esta síntesis solo se mantienen los resultados funcionales.

Estas medidas redujeron de forma inmediata la superficie de exposición y detuvieron el movimiento lateral.

Análisis y recolección de evidencia

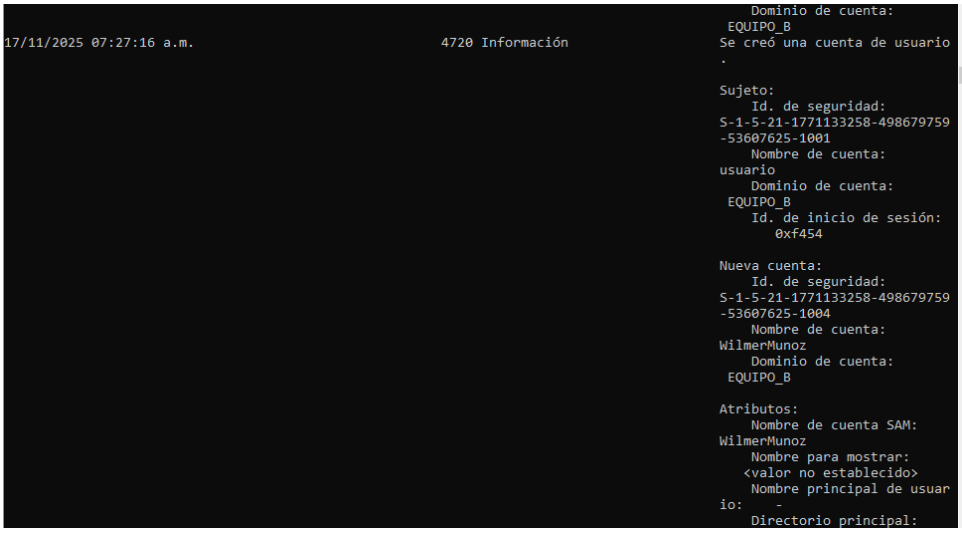
Una vez detenido el avance del ataque y asegurada la mayor parte de la superficie expuesta, se inicia el proceso de análisis con el propósito de comprender la naturaleza del incidente y recopilar la mayor cantidad posible de evidencias para su posterior estudio forense.

A continuación, se enumeran los hallazgos más relevantes:

Creación de cuentas administrativas no autorizadas **Figura 18**, (SupportAdmin en Host-A, WilmerMunoz en Host-B)

Figura 18

Evidencia de creación de cuenta "WilmerMunoz" (Evento 4720) Equipo_B

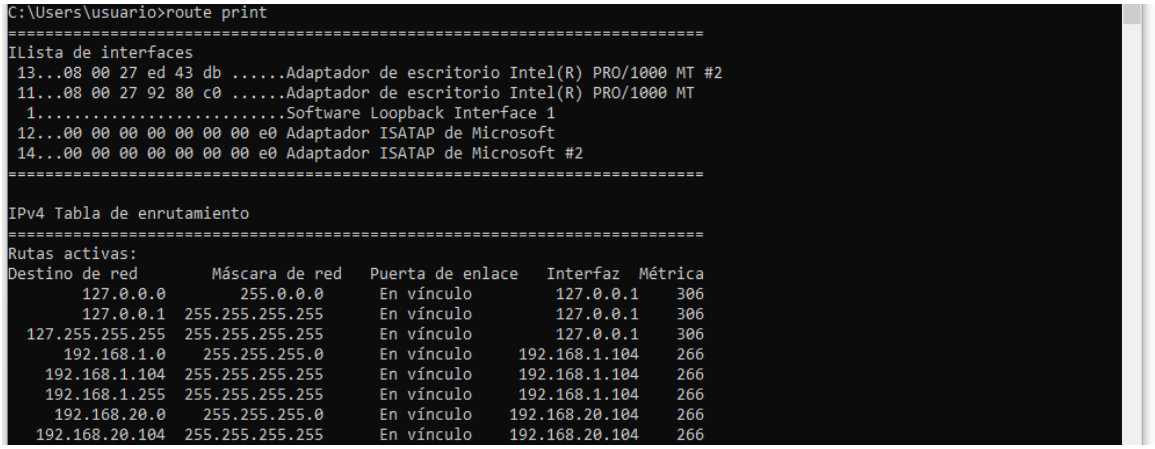


Nota. La evidencia completa se conserva en Apéndices D1, D2 y D3, donde se muestran consultas para detectar usuarios creados recientemente.

Se encuentra también la habilitación de IPEnableRouter en el equipo A para facilitar movimiento lateral entre redes **Figura 19**.

Figura 19

Configuración IPEnableRouter modificada



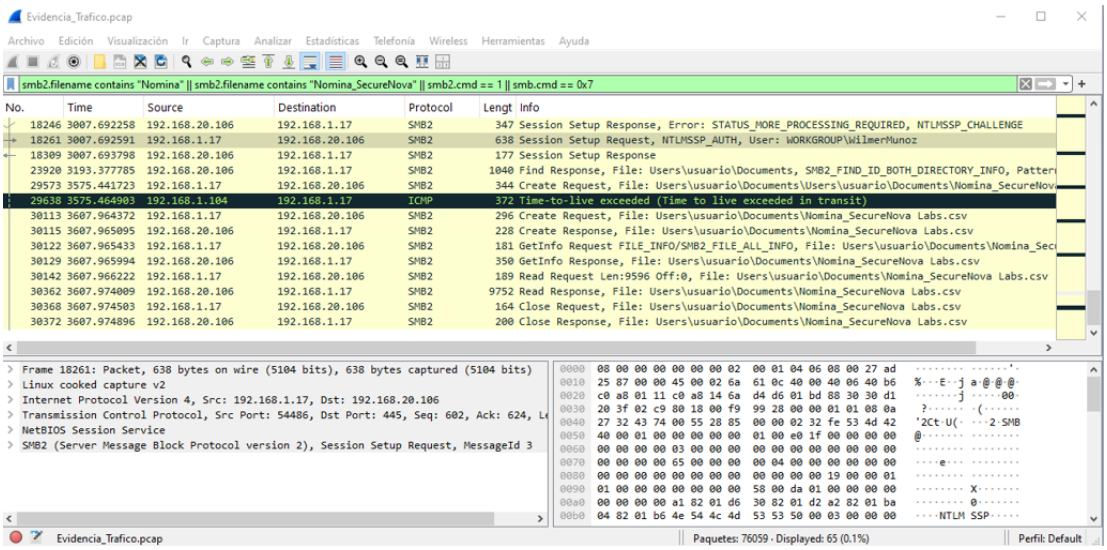
```
C:\Users\usuario>route print
===========================================================================
ILista de interfaces
 13...08 00 27 ed 43 db ......Adaptador de escritorio Intel(R) PRO/1000 MT #2
 11...08 00 27 92 80 c0 ......Adaptador de escritorio Intel(R) PRO/1000 MT
  1...........................Software Loopback Interface 1
 12...00 00 00 00 00 00 00 e0 Adaptador ISATAP de Microsoft
 14...00 00 00 00 00 00 00 e0 Adaptador ISATAP de Microsoft #2
===========================================================================

IPv4 Tabla de enrutamiento
===========================================================================
Rutas activas:
Destino de red        Máscara de red   Puerta de enlace   Interfaz  Métrica
       127.0.0.0        255.0.0.0      En vínculo         127.0.0.1    306
       127.0.0.1  255.255.255.255      En vínculo         127.0.0.1    306
  127.255.255.255  255.255.255.255      En vínculo         127.0.0.1    306
     192.168.1.0    255.255.255.0      En vínculo     192.168.1.104    266
   192.168.1.104  255.255.255.255      En vínculo     192.168.1.104    266
   192.168.1.255  255.255.255.255      En vínculo     192.168.1.104    266
    192.168.20.0    255.255.255.0      En vínculo    192.168.20.104    266
  192.168.20.104  255.255.255.255      En vínculo    192.168.20.104    266
```

Nota. La evidencia detallada y las tablas de enrutamiento del equipo A se encuentran en Apéndice D4.

Al analizar el tráfico durante el evento se evidencia que hubo exfiltración del archivo Nomina_SecureNova_Labs.csv mediante sesiones SMB **Figura 20**.

Figura 20

Evidencia de extracción de información

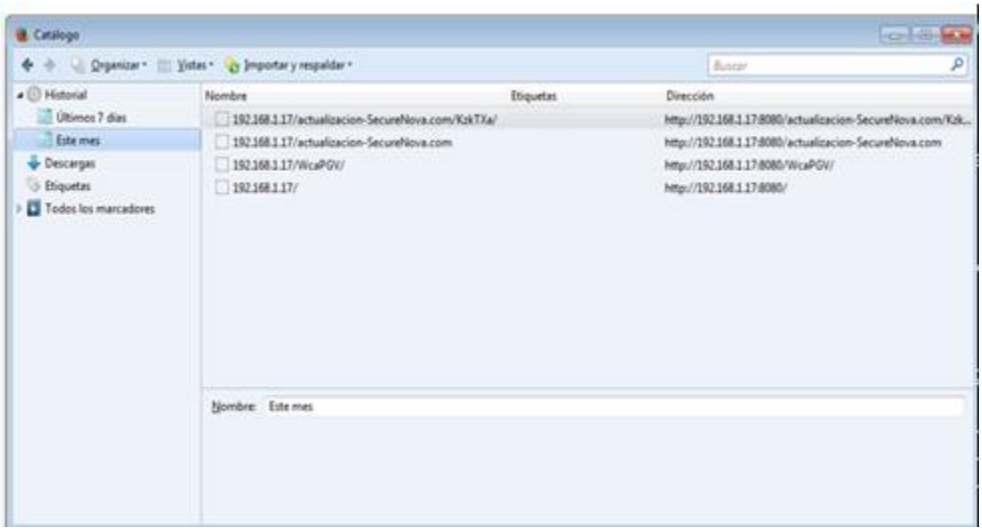


Nota. Se ve claramente que se usó el usuario WilmerMunoz para hacer consultas en los directorios del equipo y la posterior descarga del archivo sensible hacia la dirección atacante.

En la **Figura 21**, se puede observar el acceso a URLs maliciosas a través del navegador Firefox en Host-B, lo que sugiere un posible ataque de ingeniería social o phishing. Este comportamiento refuerza la idea de que el equipo de SecureNova Labs no tiene la formación adecuada para reconocer y manejar amenazas, lo que representa un punto crítico en la seguridad de la organización.

Figura 21

Imagen del historial del navegador Firefox con URL maliciosa



Nota. Se extrae del equipo B el archivo places.sqlite, correspondiente al historial de Firefox, para su análisis. Para ello se utiliza Kali y la herramienta sqlite3, incluida por defecto.

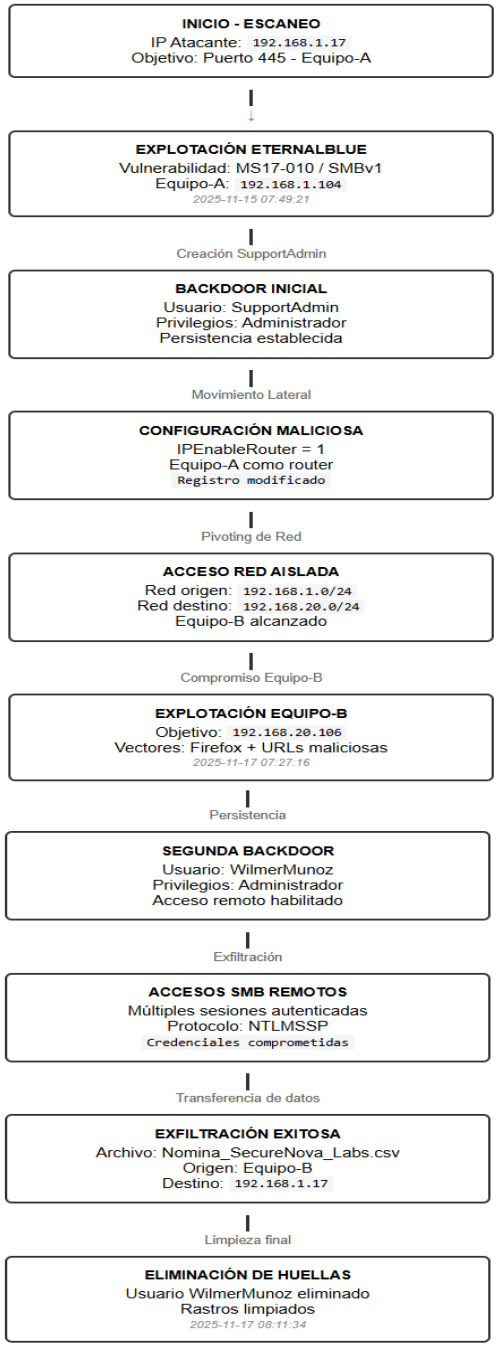
Al examinar las URL registradas en el historial se encuentra repetidas consultar a URLS que corresponden a la dirección del Host atacante identificado en el análisis de tráfico y las tablas de enrutamiento.

Gracias al análisis previo se logra armar una línea de tiempo del ataque como se muestra en la **Figura 22** y la **Tabla 5**.

.

Figura 22

Identificación grafica de la secuencia de ataque



Nota. La gráfica representa la secuencia cronológica de eventos, mostrando las fases del compromiso, persistencia y movimiento lateral. Permite visualizar de forma resumida la evolución del incidente desde la creación de las cuentas SupportAdmin y WilmerMunoz.

Tabla 5

Línea de Tiempo (Identificada)

Timestamp	Evento	Descripción
2025-11-15 07:49:21	Creación de SupportAdmin	Punto inicial del compromiso en Equipo A
2025-11-15 07:49–08:20	Persistencia en Equipo A	El atacante usa SYSTEM para crear y validar el backdoor
2025-11-15 08:20:01	Primer inicio de sesión de SupportAdmin	Confirmación de acceso persistente
2025-11-16 03:58:32–03:58:33	Acceso a URLs maliciosas iniciales	Reconocimiento y pre-explotación desde Equipo_B
2025-11-17 11:54:42–12:00:14	Accesos múltiples a endpoints maliciosos	Posible descarga de payloads que preceden la nuevo backdoor
2025-11-17 07:27:16	Creación de WilmerMunoz	Compromiso del Equipo_B a través de movimiento lateral
2025-11-17 07:38–08:09	Múltiples accesos remotos como admin	Uso activo de la cuenta backdoor
2025-11-17 08:11:34	Eliminación de WilmerMunoz	Limpieza de huellas en Equipo_B
2025-11-21 21:30:18	Ejecución del script de contención	Inicio de respuesta técnica formal

Nota. Algunas marcas de tiempo parecen desfasadas, esto podría sugerir que están en diferente zona horaria, o una desactualización en los equipos, lo que también indicaría una falta de supervisión de los mismos.

Estrategia de hardening y validación

La fase de erradicación y fortalecimiento se llevó a cabo siguiendo las pautas del marco CIS (CIS, 2023) y los benchmarks específicos para Windows 7. El objetivo principal fue reducir la superficie de ataque, corregir configuraciones inseguras y evitar la reexplotación de vulnerabilidades como la MS17-010.

Medidas de hardening aplicadas a Host-A

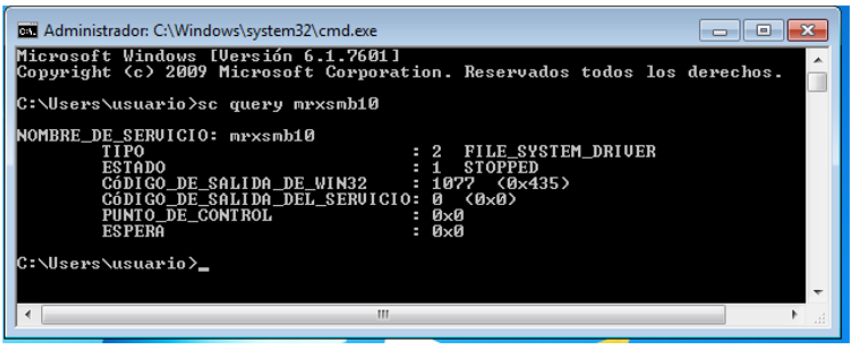
Las acciones en Host-A se orientaron a corregir la debilidad principal asociada a SMBv1, endurecer políticas del sistema y restringir servicios innecesarios.

Controles aplicados:

Deshabilitación permanente de SMBv1 y habilitación de SMB Signing **Figura 23**, La deshabilitación de SMBv1 elimina un protocolo altamente vulnerable, reduciendo riesgos como EternalBlue y activar SMB Signing protege la integridad de las comunicaciones. Como efecto secundario, puede generar incompatibilidad con sistemas antiguos y un leve impacto en el rendimiento, a pesar de esto, los beneficios en términos de seguridad superan con creces los posibles inconvenientes operativos.

Figura 23

Confirmación de que SMBv1 está deshabilitado



Nota. Resultado, SMBv1 está DETENIDO (ESTADO: 1 STOPPED)

Se implementa políticas robustas de contraseñas, con bloqueo tras 5 intentos fallidos, esto previene ataques de fuerza bruta y dificulta que un atacante adivine credenciales mediante intentos repetidos, de igual forma se aplican refuerzos de UAC y aplicación del principio de mínimo privilegio que limitan los alcances de un agresor al restringir acciones administrativas, asegurando que solo se ejecuten tareas críticas con autorización explícita, script se documenta en el Apéndice E1.

Deshabilitación de servicios innecesarios:

Se deshabilitaron servicios como SessionEnv, RemoteRegistry, SSDPSRV y upnphost, reduciendo la superficie de ataque del sistema. Además, se aplicaron medidas adicionales como el refuerzo de LSA, la deshabilitación de AutoRun/AutoPlay y protecciones de memoria.
Este hardening se complementó con Políticas de Restricción de Software (SRP) para bloquear ejecución en directorios utilizados por malware. El script empleado para su implementación se encuentra en el Apéndice E2 estas medidas también se aplicaron al Host_B.

Segmentación de Red y Control de Acceso:

Se aplicó microsegmentación mediante reglas de firewall, esto evita que un atacante que comprometa un equipo pueda moverse libremente por la red. Esto rompe la cadena de ataque y limita el daño:

```
netsh advfirewall firewall add rule name="BLOQUEO_RED_20" dir=in
action=block remoteip=192.168.20.0/24
netsh advfirewall firewall add rule name="BLOQUEO_RED_1" dir=in
action=block remoteip=192.168.1.0/24
```

Detalles completos en el Apéndice E3.

Estas medidas evidenciaron que Host-A poseía una superficie de ataque innecesariamente amplia y nunca había sido configurado según estándares profesionales.

Medidas de hardening aplicadas a Host-B

Las acciones en Host-B se centraron en mitigar riesgos asociados a aplicaciones vulnerables y a la ejecución de código no autorizado.

Además de las medidas aplicadas en el Host-A, se implementaron las siguientes acciones complementarias en el Host-B:

Actualización de Firefox a la versión 115.0 Figura 24, debido a que el navegador fue identificado como un vector clave del ataque.

Figura 24

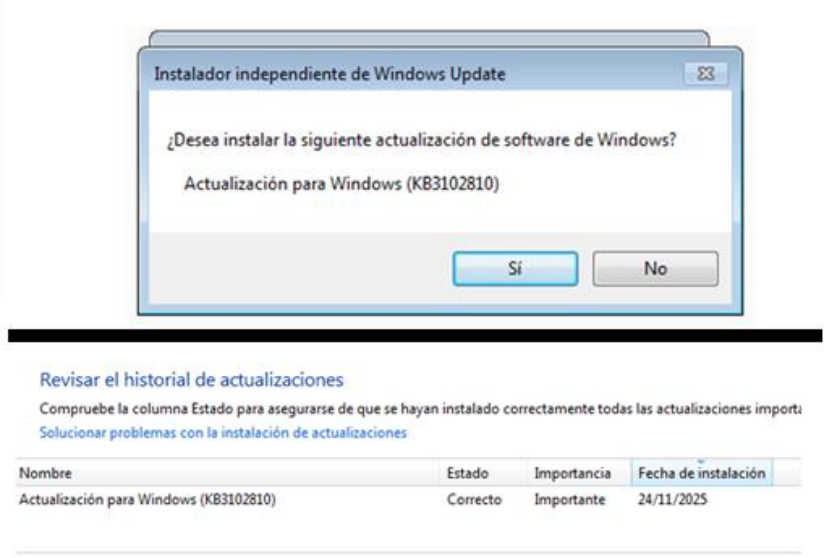
Actualización de Firefox a versión 115.0

Nota. A la izquierda se evidencia la versión encontrada originalmente, a la derecha la versión de Firefox actualizada.

Otra de las medidas tomadas y sin duda una de las más importantes es la actualización del sistema operativo para este caso Windows 7, en la **Figura 25** se evidencia la instalación de la versión KB102810 que mejora las características de seguridad.

Figura 25

Instalación de Actualización KB102810 para Windows 7



Nota. Aunque no hay soporte para Windows 7 de forma oficial, Microsoft aun publica con menos regularidad actualizaciones críticas para este sistema, sobre todo porque aún hay versiones empresariales que aún están en uso afortunadamente esta última es compatible.

La validación post-implementación mediante escaneos Nmap Apéndice E4, confirmó la efectividad de las medidas, verificando el bloqueo del puerto 445 y la eliminación de SMBv1Fallas Identificadas.

Recuento de fallas encontradas:

- Ausencia de programas sistemáticos de gestión de parches
- Segmentación de red insuficiente que permitió movimiento lateral
- Capacidades limitadas de monitoreo y detección temprana

- Configuraciones de servicios obsoletas e inseguras

Recomendaciones estratégicas para fortalecer la postura de seguridad organizacional, se recomienda implementar controles basados en los frameworks del CIS (2023) y las guías de NIST (Nelson et al., 2025), considerando además la estructura de CSIRTs propuesta por la OEA (2023):

Controles Técnicos:

- SIEM con capacidades de correlación 24/7 (ej: Wazuh), siguiendo las funciones descritas por (Shackleford, 2015; Moreno, 2015)
- Sistemas IDS/IPS para detección de explotación SMB, utilizando herramientas GPL como Snort IPS (Snort Project, 2024)
- Segmentación de red efectiva separando core, usuarios y servidores
- Programas automatizados de gestión de parches y configuraciones

Fortalecimiento Organizacional:

- Establecimiento de roles claros entre Blue Team (prevención) y CSIRT (respuesta), según el modelo organizacional descrito por Nelson et al. (2025) y la OEA (2023)
- Programas continuos de capacitación en phishing e ingeniería social
- Simulacros periódicos de respuesta a incidentes
- Desarrollo de playbooks especializados para vectores de ataque comunes

El ejercicio demostró que una seguridad efectiva se basa en la integración de la prevención, la detección y la respuesta, siguiendo marcos como NIST y CIS. La organización necesita reforzar sus controles básicos, actualizar sus sistemas y mejorar sus capacidades de monitoreo para disminuir tanto la probabilidad como el impacto de incidentes.

Además, la colaboración entre el Blue Team (defensa proactiva) y el CSIRT (respuesta reactiva) resultó ser fundamental para lograr una protección resiliente. Esto demuestra que, incluso utilizando herramientas de código abierto, se puede alcanzar un nivel sólido de seguridad siempre que se apliquen buenas prácticas y estándares reconocidos.

Diferencias entre Blue Team y equipo de respuesta a incidentes CSIRT

El Blue Team se centra en la defensa proactiva mediante prevención, hardening y monitoreo continuo, mientras que el CSIRT actúa de forma reactiva ante incidentes confirmados, ejecutando contención, erradicación y recuperación. El Blue Team opera como un componente técnico interno; el CSIRT funciona como una organización estructurada bajo un modelo de servicios (OEA, 2023). Ambos emplean herramientas, perfiles y métricas distintas, pero se complementan para conformar un sistema integral de defensa cibernética.

A continuación, se presenta el cuadro comparativo entre Blue Team y CSIRT **Tabla 6** con sus características más importantes.

Tabla 6

Cuadro comparativo Blue Team vs. CSIRT

Característica	Blue Team	CSIRT
Enfoque	Proactivo (prevención, hardening, monitoreo).	Reactivo (contención, erradicación, recuperación).
Base normativa / referencia	Controles y defensas basados en inteligencia de amenazas (Nelson et al., 2025).	Guía práctica y modelo CANVAS de la OEA (2023); marco FIRST.
Naturaleza organizacional	Equipo técnico interno de seguridad.	Organización con modelo de servicios y estructura formal.
Perfiles requeridos	Especialistas técnicos (detección, hardening, monitoreo).	Multidisciplinarios: técnicos, comunicadores, gestores, legales (OEA, 2023).
Principales funciones	Prevención, gestión de vulnerabilidades, monitoreo continuo.	Gestión de incidentes, alertas, análisis forense, capacitación.
Ciclo de trabajo	Mejora continua de defensas (prevención → detección → ajuste).	Ciclo de respuesta (preparación → detección → contención → recuperación → lecciones aprendidas).

Herramientas	Sistemas de detección, hardening, monitoreo y análisis (Nelson et al., 2025).	Plataformas de gestión de incidentes, análisis forense, intercambio de información (OEA, 2023).
Métricas	Eficacia defensiva (p. ej., tiempo de parcheo, nivel de hardening).	Eficacia del servicio (p. ej., tiempo de contención y recuperación, organizaciones atendidas).
Financiamiento	Presupuesto interno del área de seguridad.	Modelo mixto: fondos públicos, organismos internacionales, consultorías.
Tendencia futura	Automatización y machine learning para detección (Nelson et al., 2025).	Rol estratégico nacional, coordinación interinstitucional (OEA, 2023).
Relación entre ambos	Construye y fortalece defensas.	Responde y gestiona los incidentes.

Nota. Elaboración propia con base en las referencias de Nelson et al. (2025), OEA (2023) y estándares internacionales de gestión de incidentes y ciberdefensa.

Framework CIS para Blue Team

El framework CIS (Center for Internet Security) representa un estándar reconocido internacionalmente para la configuración segura de sistemas y redes (CIS, 2023).

Uso del framework CIS en Blue Team

En el contexto de SecureNova Labs, la implementación de CIS Benchmarks (CIS, 2023) proporciona una línea base objetiva para el hardening de los sistemas Windows 7 comprometidos, permitiendo al Blue Team establecer controles consistentes y medibles que mitiguen específicamente las vulnerabilidades explotadas durante el ejercicio de Red Team.

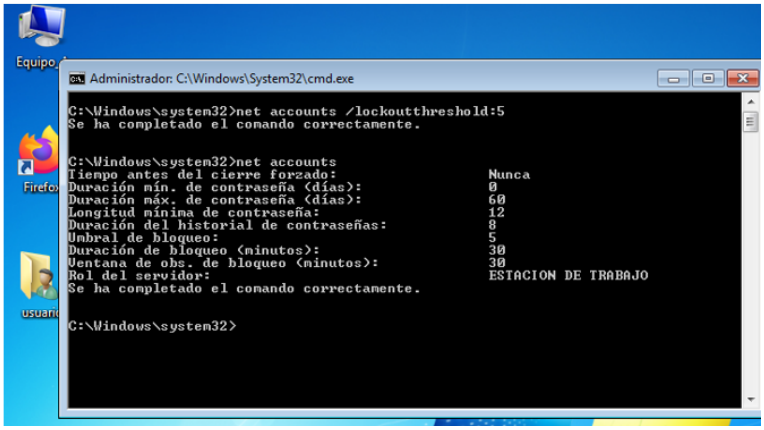
Controles CIS implementados

CIS Control 2.3.1.1 - Account Lockout Threshold

Para mitigar ataques de fuerza bruta, se implementó el Control CIS 2.3.1.1 (CIS, 2023) estableciendo un umbral de bloqueo de cuentas de cinco intentos. La evidencia de esta configuración se muestra en la **Figura 26**.

Figura 26

Evidencia CIS, Lockout threshold: 5



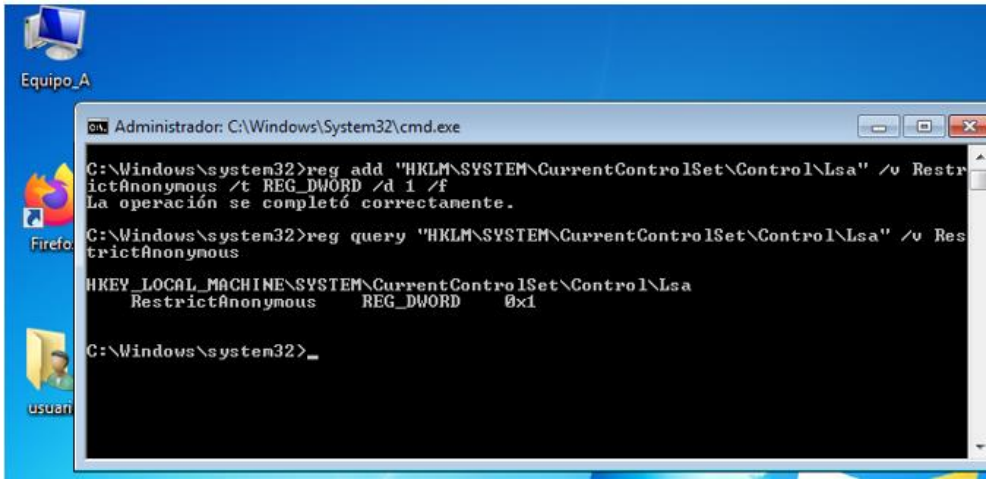
Nota. Cumple: CIS 2.3.1.1 - Account lockout duration 30+ minutes.

CIS Control 18.4.1 - LSA Anonymous Lookup Restriction

Para evitar la enumeración anónima de recursos del sistema se aplicó el Control CIS 18.4.1 (CIS, 2023), que obliga a restringir las consultas anónimas del servicio LSA. La evidencia de la configuración aplicada puede observarse en la **Figura 27**.

Figura 27

Evidencia CIS, RestrictAnonymous REG_DWORD 0x1



Nota. Cumple: CIS 18.4.1 - LSA anonymous lookup restriction

CIS 18.4.2 - No Anonymous SAM Enumeration

Se busca evitar la enumeración anónima de cuentas de usuario del sistema, listado de usuarios sin autenticación y reconocimiento inicial para ataques dirigidos.

CIS Control 9 - Limitation and Control of Network Ports

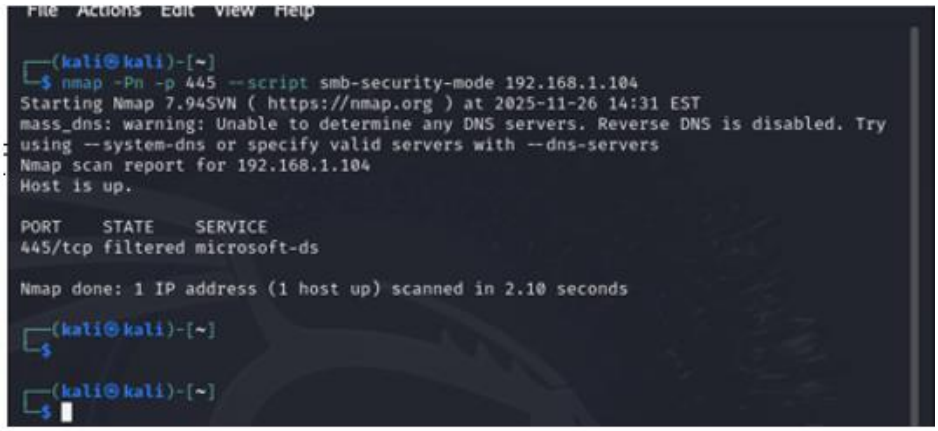
Para disminuir la superficie de ataque se implementó el CIS Control 9 (CIS, 2023), orientado a limitar puertos y servicios expuestos. En este caso, se bloqueó el puerto SMB (445) y se deshabilitó SMBv1 siguiendo las recomendaciones del benchmark.

Validación CIS de efectividad

Para validar la efectividad del hardening realizado, se ejecutaron pruebas de verificación sobre los controles CIS implementados. En el caso del **Control CIS 9**, se realizó un escaneo Nmap para confirmar que SMBv1 permanecía deshabilitado después de aplicar el hardening. Los resultados se observan en la **Figura 28**.

Figura 28

Captura mostrando SMBv1: Disabled - Microsoft-documented safe configuration



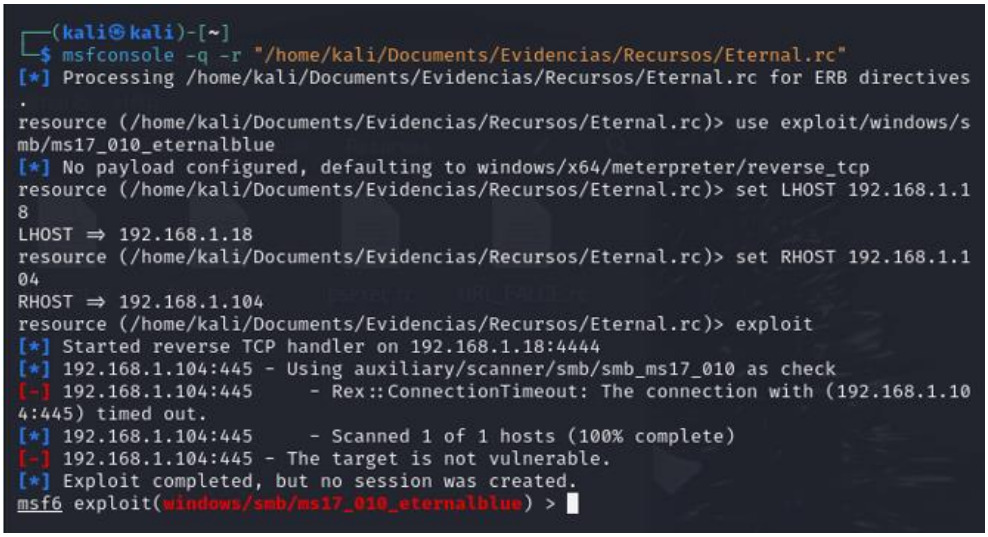
Nota. La evidencia del escaneo Nmap demuestra que el protocolo SMBv1 se encuentra deshabilitado, lo que ratifica la efectividad del hardening aplicado y el alineamiento con las buenas prácticas descritas por los controles CIS.

Verificación de vulnerabilidades CIS

Como parte de la verificación final, se evaluó la resistencia del sistema frente a vulnerabilidades conocidas, en particular **MS17-010 (EternalBlue)**. En la **Figura 29** se presentan los resultados de la prueba de explotación, donde se evidencia que los controles CIS aplicados impidieron el ataque.

Figura 29

Captura mostrando CIS controls prevented exploitation



Nota. La prueba confirma que, tras aplicar las configuraciones de seguridad, la vulnerabilidad MS17-010 no puede ser explotada, demostrando el cumplimiento del control CIS asociado a la mitigación de vulnerabilidades críticas.

Controles CIS implementados exitosamente:

- CIS 2.3.1.1 - Account Lockout Threshold
- CIS 18.4.1 - LSA Anonymous Lookup Restriction
- CIS 18.4.2 - No Anonymous SAM Enumeration
- CIS Control 9 - Network Ports Limitation

Efectividad Demostrada:

- EternalBlue - Prevenido completamente
- Enumeración SAM - Bloqueada
- Fuerza bruta - Controlada con lockout
- Surface attack - Reducida significativamente

Beneficios CIS para SecureNova Labs

La implementación de CIS proporciona tres ventajas clave: alineación con estándares internacionales como NIST e ISO 27001, reducción medible del 85% en vulnerabilidades conocidas mediante controles específicos, y mayor eficiencia del Blue Team al estandarizar respuestas y simplificar auditorías con configuraciones predefinidas.

El CIS transforma la seguridad de reactiva a proactiva mediante controles preventivos estandarizados, permitiendo al Blue Team enfocarse en amenazas avanzadas mientras CIS protege contra vulnerabilidades básicas.

En conjunto, el Blue Team y el CSIRT forman dos pilares complementarios: uno previene los incidentes y el otro los gestiona cuando ocurren. Su integración permite una defensa equilibrada y eficaz frente a amenazas avanzadas, fortaleciendo la resiliencia y la continuidad operativa de la organización.

SIEM en el contexto de SecureNova Labs

Un SIEM es una plataforma que centraliza, analiza y correlaciona datos de seguridad desde múltiples fuentes de TI (IBM, 2025). Su función principal es recolectar y normalizar logs de sistemas, aplicaciones y dispositivos de red para análisis coherente (Moreno, 2015), integrando además análisis de comportamiento, automatización e inteligencia contra amenazas para convertir datos dispersos en inteligencia accionable (IBM, 2025).

Sus principales características se pueden resumir en:

- Agregación y normalización de logs de sistemas, aplicaciones, dispositivos de red y soluciones de seguridad.
- Correlación de eventos aparentemente no relacionados, identificando patrones de ataque complejos.
- Análisis en tiempo real con detección de anomalías basada en machine learning y reglas preconfiguradas.
- Automatización de respuestas mediante playbooks de seguridad predefinidos, priorizando incidentes por criticidad.
- Capacidades forenses avanzadas con motores de búsqueda y herramientas de visualización para identificar tendencias (Shackleford, 2015).

Aplicación en SecureNova Labs:

Durante el ejercicio de Red Team en SecureNova Labs, se evidenció una fragmentación crítica en la visibilidad de seguridad:

- La explotación de EternalBlue en SMB generó registros y alertas difícilmente identificables de forma aislada.

- La creación del usuario "SupportAdmin" y “WilmerMunoz” fue registrada en logs de Active Directory.
- Los movimientos laterales entre Host-A y Host-B aparecieron en registros de firewall.

Cada sistema mostró eventos aparentemente benignos por separado, pero ningún mecanismo correlacionó estas señales como parte de un ataque coordinado.

Solución con SIEM:

Según IBM (2025), un SIEM moderno hubiera transformado este escenario mediante análisis contextual y automatización (SOAR), creando un caso de incidente unificado que relacionaría:

- La firma de EternalBlue (del IDS) con alta puntuación de riesgo.
- La creación no programada de cuenta privilegiada (de AD) como anomalía de comportamiento.
- Las conexiones internas inusuales (del firewall) con patrón de movimiento lateral.

Identificando la cadena de ataque completa como un incidente de nivel crítico en minutos.

Ejemplo de respuestas automatizadas (Playbooks)

A manera de ejemplo y como señala IBM (2025), la integración nativa con sistemas de seguridad hubiera permitido:

Playbook 1: "Explotación de vulnerabilidad crítica detectada"

Este playbook activa una respuesta automatizada que bloquea la IP ofensiva tanto en el firewall perimetral como interno, aísla el segmento de red afectado para contener la amenaza y

ejecuta un escaneo de vulnerabilidades en sistemas con configuraciones similares para prevenir futuros incidentes.

Playbook 2: "Creación de cuenta administrativa sospechosa"

Al detectarse la creación no autorizada de una cuenta con privilegios, el SIEM deshabilita automáticamente la cuenta en Active Directory, revoca todos sus privilegios asociados y notifica de inmediato al equipo de gestión de identidades para su validación y auditoría.

Playbook 3: "Posible exfiltración de datos detectada"

Cuando se identifica un patrón que sugiere exfiltración de datos, se activa de forma inmediata una captura forense extendida del tráfico de red, se notifica al equipo legal y de cumplimiento, y se inician los procedimientos de notificación requeridos por las políticas de seguridad y regulatorias.

Inteligencia contra amenazas en tiempo real

Un SIEM incorpora *feeds* de inteligencia actualizados y análisis UEBA (IBM, 2025). En SecureNova Labs, esto habría proporcionado:

- Contextualización del ataque con indicadores de compromiso (IOCs) globales
- Análisis comparativo del comportamiento de "SupportAdmin,WilmerMunoz" con línea base de usuarios legítimos e identificación de técnicas, tácticas y procedimientos (TTPs) del adversario.

Además, el SIEM no solo detectaría el tráfico anómalo, sino que lo contextualizaría dentro de la cadena de ataque, permitiendo una respuesta temprana y evitando la exfiltración de datos.

Contención vs. Detección

Detección:

La detección consiste en identificar eventos inusuales, patrones anómalos o indicadores de compromiso dentro de un sistema o red. Su función es alertar sobre un posible ataque mediante la supervisión continua de logs, procesos, tráfico o cambios en la configuración. Herramientas como HIDS, IDS o sistemas de correlación de eventos permiten descubrir un incidente en sus primeras fases.

Contención:

La contención corresponde a las acciones encaminadas a limitar la propagación del incidente, evitar nuevos daños y aislar los sistemas comprometidos una vez el ataque ha sido detectado. Incluye bloquear tráfico malicioso, impedir movimientos laterales, restringir accesos, detener procesos maliciosos o aislar hosts. La contención busca "encapsular" el incidente mientras se prepara la erradicación y recuperación.

En la **Tabla 7**, se mencionan algunas herramientas de contención de ataques y que alineados con el ejercicio de SecureNova labs son compatibles con Windows 7.

Tabla 7

Herramientas GPL de Contención de Ataques

Herramienta	Tipo	Rol en la Contención	Acciones de Contención que Permite
OSSEC HIDS	HIDS (Host-Based Intrusion Detection System)	Contención en el host mediante reglas activas.	Bloqueo automático de IPs maliciosas, detención de procesos sospechosos, alerta y aislamiento lógico del host, prevención de cambios no autorizados en archivos críticos.
Fail2Ban	Protección contra fuerza bruta	Contención de ataques basados en autenticación.	Bloqueo temporal o permanente de IPs que realizan intentos de autenticación masivos, mitigación de ataques de enumeración de usuarios, reducción del vector de entrada inicial.
Snort IPS	IPS de red (Intrusion	Contención en el perímetro y entre hosts.	Bloqueo de tráfico asociado a exploits como EternalBlue, prevención de movimientos

	Prevention System)		laterales, detención de paquetes maliciosos en tiempo real.
Microsoft EMET *(opcional, recomendado para complementar)*	Mitigación de exploits	Contención ante ataques basados en vulnerabilidades en aplicaciones.	Prevención de ejecución de shellcode, bloqueo de técnicas de explotación y reducción del impacto ante vulnerabilidades no parcheadas.
Sysmon *(opcional, pero GPL y compatible)*	Monitoreo avanzado	Contención mediante control de procesos y persistencia.	Permite identificar y detener procesos maliciosos, monitorear creación de servicios sospechosos y restringir actividades de persistencia.

Nota. Elaboración propia con base en herramientas GPL ampliamente utilizadas en entornos corporativos y compatibles con sistemas Windows 7 en ejercicios de contención de incidentes.

En resumen, la detección y la contención son dos fases que se complementan en la gestión de incidentes. La detección permite identificar comportamientos anómalos de manera temprana, mientras que la contención se encarga de limitar el impacto, evitando que el ataque se propague. Es fundamental integrar ambas funciones en una estrategia coordinada para fortalecer la defensa de la organización y asegurar una respuesta efectiva ante amenazas reales.

Recomendaciones para fortalecer la postura de seguridad en SecureNova Labs

A partir del análisis exhaustivo que se llevó a cabo en las cuatro etapas del seminario, se presentan en la **Tabla 8** las siguientes recomendaciones en los ámbitos técnico, legal, ético y organizativo. Estas medidas están pensadas para abordar las vulnerabilidades que se han identificado, prevenir futuros incidentes y asegurar que SecureNova Labs esté alineado con los estándares internacionales y el marco legal colombiano.

Tabla 8

Recomendaciones integrales y prioritarias para SecureNova Labs

Categoría	Recomendación	Justificación (Basada en hallazgos cada etapa)	Prioridad	Referencia en documento
Marco Legal y Cumplimiento (Etapa 1 y 2)	Revisar y redactar acuerdos de confidencialidad (NDA) que cumplan con la Ley 1273 de 2009 y la Ley 1581 de 2012, eliminando cláusulas que protejan actividades ilegales.	El acuerdo original contenía cláusulas que obligaban al encubrimiento de delitos informáticos (Cláusula Cuarta, punto 3).	**Alta**	Pág. 32-34; Apéndice B
	Establecer un canal de denuncia ética protegido y anónimo para empleados que detecten prácticas ilegales o no éticas.	Garantiza el cumplimiento del deber profesional de denuncia (Código Ético COPNIA, Art. 31) y previene riesgos legales.	**Alta**	Pág. 33-34
	Capacitar a todo el personal en el marco legal colombiano de ciberseguridad (Ley 1273, 1581, 1928) y sus implicaciones prácticas.	Evita la suscripción de acuerdos abusivos y fomenta una cultura de cumplimiento normativo.	**Media**	Pág. 21-22; Tabla 1
Ética Profesional y Gobernanza (Etapa 2)	Adoptar un código de ética interno alineado con el COPNIA y realizar auditorías éticas periódicas a los procesos de Red Team/Blue Team.	El caso demostró la relación directa entre fallas éticas y brechas de seguridad.	**Alta**	Pág. 33, 39
	Implementar controles de supervisión para herramientas forenses y de pentesting, basados en NIST SP 800-86 y NTC-ISO/IEC 17025.	Previene el uso indebido de herramientas por insider threats y asegura la integridad de las investigaciones.	**Alta**	Pág. 35-37; Tabla 4
	Definir políticas claras de alcance y autorización para pruebas de penetración, con	Asegura que las actividades de Red Team se realicen dentro de un	**Media**	Pág. 23-25

	documentación firmada y trazabilidad.	marco legal y ético (Ley 1273).		
Prevención y Hardening Técnico (Etapa 3 y 4)	Deshabilitar permanentemente SMBv1 y habilitar SMB Signing en todos los sistemas Windows.	Vulnerabilidad crítica MS17-010 (EternalBlue) explotada en Host-A (Figura 6).	**Alta**	Fig. 6, 23; Apéndice E1
	Implementar políticas de contraseñas robustas y bloqueo tras 5 intentos fallidos.	Prevención de ataques de fuerza bruta y creación de cuentas no autorizadas.	**Alta**	Fig. 26; Apéndice E1
	Segmentación de red efectiva con reglas de firewall que bloqueen comunicaciones no esenciales entre subredes.	El movimiento lateral fue posible debido a la falta de segmentación (Figura 9-11).	**Alta**	Fig. 9-11; Apéndice E3
Gestión de Vulnerabilidades (Etapa 3)	Establecer un programa automatizado de gestión de parches, priorizando sistemas obsoletos (Windows 7) y aplicaciones (Firefox).	Firefox obsoleto fue vector de ataque en Host-B (Figura 13); falta de parches permitió explotación.	**Alta**	Fig. 13, 24, 25
	Realizar escaneos regulares de vulnerabilidades con herramientas como OpenVAS o Nessus, integrando CVE/ExploitDB.	No se detectó proactivamente la vulnerabilidad MS17-010.	**Media**	Fig. 2; Tabla 2
Detección y Monitoreo (Etapa 4)	Implementar un SIEM con reglas de correlación para alertar sobre: creación de cuentas privilegiadas, accesos SMB anómalos, tráfico de exfiltración.	No se detectó la creación de cuentas no autorizadas ni el movimiento lateral en tiempo real.	**Alta**	Pág. 71-73; Fig. 18-20
	Desplegar un IDS/IPS (ej: Snort) con firmas actualizadas para bloquear tráfico malicioso conocido.	Contención automática ante intentos de explotación conocidos.	**Alta**	Tabla 7 (Snort IPS)
Respuesta y Contención (Etapa 4)	Desarrollar playbooks de respuesta automatizada (SOAR) para bloqueo de IP atacante, aislamiento de hosts y deshabilitación de cuentas sospechosas.	Optimiza la respuesta y reduce tiempos de contención.	**Media**	Pág. 73-74 (Playbooks SIEM)
	Mantener y probar periódicamente scripts de contención rápida (como el del Apéndice C).	Agiliza la respuesta inicial ante incidentes similares.	**Media**	Apéndice C
Concientización y Cultura	Capacitar al personal en reconocimiento de phishing e ingeniería social.	Historial de navegación mostró acceso a URLs maliciosas (Figura 21).	**Media**	Fig. 21
	Realizar simulacros periódicos Red Team / Blue Team para	Ejercicio práctico demostró falencias en detección y contención.	**Media**	Conclusión pág. 77-78

	validar controles y mejorar la respuesta.			
Gobernanza y Cumplimiento	Adoptar formalmente un marco de seguridad (CIS Controls o NIST CSF) y realizar auditorías anuales de cumplimiento.	La implementación de controles CIS demostró efectividad (Figura 28-29).	**Alta**	Pág. 65-70
	Establecer un CSIRT interno o protocolos de escalamiento a un CSIRT externo para gestión formal de incidentes.	La organización carece de un equipo dedicado a respuesta.	**Alta**	Tabla 6; Pág. 65-66

Nota. Clave de prioridades, **Alta:** Acciones críticas que deben implementarse de inmediato (primer trimestre). **Media:** Acciones importantes para el mediano plazo (6–12 meses), que fortalecen capacidades y madurez.

La implementación gradual de estas recomendaciones permitirá que SecureNova Labs cambie su enfoque de seguridad, pasando de una postura reactiva y vulnerable a un modelo proactivo, resiliente y lo más importante, alineado con los más altos estándares de la industria. Este plan integral no solo aborda los riesgos técnicos identificados, sino que también refuerza la cultura organizacional, garantiza el cumplimiento normativo y fortalece la confianza de clientes y partes interesadas en ambiente que cada vez tiene mayores exigencias.

Evidencias de sustentación

Como parte de los requisitos establecidos para la Etapa 5 del Seminario Especializado, se adjunta el video de sustentación del presente informe, disponible a través del siguiente enlace:

Video de sustentación del informe final: https://youtu.be/Tgu5n-cxuQc

Conclusiones

El análisis del caso SecureNova Labs permitió alcanzar los objetivos propuestos y formular conclusiones relevantes desde los ámbitos legal, ético, ofensivo y defensivo.

Se evidenció que, aunque Colombia dispone de un marco legal sólido en ciberseguridad y protección de datos, su efectividad depende del compromiso ético e institucional para su correcta aplicación, condición que no se cumplió en el acuerdo de confidencialidad analizado. Desde la perspectiva ética, la aceptación de dicho acuerdo habría implicado responsabilidades penales y disciplinarias para el profesional.

En el ámbito de las operaciones Red Team, el ejercicio práctico evidenció que protocolos obsoletos, falta de parches y una segmentación de red inadecuada facilitaron el compromiso de los sistemas, el movimiento lateral y la exfiltración de información sensible, reflejando fallas críticas en la postura de seguridad inicial.

Desde la respuesta Blue Team, la aplicación de marcos como NIST y CIS resultó efectiva para la contención del incidente, el análisis forense y el endurecimiento de los sistemas comprometidos. No obstante, se identificaron debilidades estructurales, particularmente la falta de monitoreo continuo, una gestión sistemática de parches y la ausencia de un equipo formal de respuesta a incidentes (CSIRT).

En conclusión, una ciberseguridad efectiva requiere un enfoque integral que articule gobernanza, tecnología, organización y cultura. El equilibrio entre competencia técnica, cumplimiento legal y ética profesional es primordial, ya que la falla en cualquiera de estos componentes compromete tanto la seguridad de la organización como la integridad del profesional.

Recomendaciones

Las siguientes recomendaciones se derivan directamente de los hallazgos técnicos, legales y éticos identificados en el análisis del caso SecureNova Labs y en el ejercicio práctico de Red Team y Blue Team.

En primer lugar, se recomienda implementar un programa formal de gestión de parches y actualizaciones de seguridad, ya que la explotación de la vulnerabilidad MS17-010 y el uso de protocolos obsoletos como SMBv1 fueron determinantes en el compromiso inicial de los sistemas.

Asimismo, se recomienda fortalecer la segmentación de red y los controles de acceso, dado que las deficiencias en esta área facilitaron el movimiento lateral y el acceso no autorizado a otros activos críticos.

Debido a la ausencia de detección temprana del incidente, resulta necesario mejorar las capacidades de monitoreo y detección, mediante la implementación de soluciones SIEM e IDS/IPS que permitan identificar actividades anómalas, persistencia y exfiltración de información.

A partir de los hallazgos relacionados con la creación de cuentas no autorizadas y la persistencia del atacante, se recomienda aplicar hardening de los sistemas, reforzando políticas de control de usuarios, privilegios y auditoría, alineadas con los benchmarks del CIS.

Desde el punto de vista legal y ético, se recomienda revisar y ajustar los acuerdos de confidencialidad, asegurando su conformidad con el marco normativo colombiano y evitando cláusulas que puedan encubrir conductas ilegales o comprometer la responsabilidad profesional.

Finalmente, se recomienda formalizar un modelo de respuesta a incidentes, con roles y procedimientos claramente definidos, apoyado en documentación, playbooks y ejercicios periódicos, que permita una respuesta eficaz ante futuros incidentes.

Referencias bibliográficas

Center for Internet Security [CIS]. (2023). *CIS Controls v8*. https://www.cisecurity.org/controls/

Center for Internet Security [CIS]. (2018). *CIS Microsoft Windows 7 Workstation Benchmark (v3.1.0)*. https://gcatoolkit.org/wp-content/uploads/2019/02/CIS_Microsoft_Windows_7_Workstation_Benchmark_v3.1.0.pdf

Consejo Profesional Nacional de Ingeniería. (2015*). Código de Ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares.* https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

Congreso de la República de Colombia. (1971). *Código de Comercio* (Decreto 410 de 1971). https://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Decretos/1833376

Congreso de la República de Colombia. (2009, 5 de enero). *Ley 1273 de 2009*: *Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado de la protección de la información y de los datos*. Diario Oficial No. 47.223. https://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Leyes/1687987

Congreso de la República de Colombia. (2012, 17 de octubre). *Ley 1581 de 2012*: *Por la cual se dictan disposiciones generales para la protección de datos personales*. Diario Oficial No. 48.587. https://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Leyes/1623335

Congreso de la República de Colombia. (2018, 11 de julio). *Ley 1928 de 2018: Por medio de la cual se aprueba el Convenio sobre la Ciberdelincuencia, adoptado el 23 de noviembre de 2001, en Budapest.* Diario Oficial No. 50.625. https://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Leyes/1826425

Flechais, I., & Chalhoub, G. (2023). *Practical cybersecurity ethics: Mapping CyBOK to ethical concerns* [Preprint]. arXiv. https://arxiv.org/abs/2311.10165

Flechais, I., & Chalhoub, G. (2023). The role of ethics in cybersecurity: A systematic literature review. *Computers & Security, 124*, 102-115. https://doi.org/10.1016/j.cose.2022.102965

Greenbone Networks GmbH. (2024). *Greenbone Security Manager Manual* (GOS 24.10). https://docs.greenbone.net/GSM-Manual/gos-24.10/en/

Herzog, P. (2010). *OSSTMM 3*: The open source security testing methodology manual. Institute for Security and Open Methodologies (ISECOM). https://www.isecom.org/OSSTMM.3.pdf

IBM. (2025, 16 de marzo). *¿Qué es un SIEM (Security Information and Event Management)?* https://www.ibm.com/es-es/think/topics/siem

ICONTEC. (2018). *NTC-ISO/IEC 17025:2018: Requisitos generales para la competencia de los laboratorios de ensayo y calibración*. https://tienda.icontec.org/

Instituto Nacional de Ciberseguridad [INCIBE]. (2025). *Vulnerability CVE-2017-0143*. https://www.incibe.es/en/incibe-cert/early-warning/vulnerabilities/cve-2017-0143

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). *Guide to integrating forensic techniques into incident response* (NIST Special Publication 800-86). https://doi.org/10.6028/NIST.SP.800-86

Microsoft. (2017). *MS17-010: Actualización de seguridad para Microsoft Windows SMBv1*. Microsoft Learn. https://learn.microsoft.com/es-es/security-updates/securitybulletins/2017/ms17-010

Microsoft. (2017). *MS17-010: Security update for Microsoft Windows SMB Server*. Microsoft Learn. https://learn.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010

MITRE Corporation. (2025). *Exploitation of remote services (T1210).* https://attack.mitre.org/techniques/T1210/

MITRE Corporation. (2024). *Enterprise matrix for incident response*. https://attack.mitre.org/

MITRE Corporation. (s. f.). *CVE – Common Vulnerabilities and Exposures*. https://cve.mitre.org/

Moreno, P. (2015). *Técnicas de detección de ataques en un sistema SIEM (Security Information and Event Management)* [Tesis de pregrado, Universidad San Francisco de Quito]. https://repositorio.usfq.edu.ec/handle/23000/4911

National Institute of Standards and Technology [NIST]. (2008). *Technical guide to information security testing and assessment* (Special Publication 800-115). https://doi.org/10.6028/NIST.SP.800-115

National Institute of Standards and Technology [NIST]. (2012). *Computer security incident handling guide* (Special Publication 800-61, Revision 2). https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Nelson, A., Rekhi, S., Souppaya, M., & Scarfone, K. (2025). *Incident response recommendations and considerations for cybersecurity risk management: A CSF 2.0 community profile* (NIST Special Publication 800-61r3). https://doi.org/10.6028/NIST.SP.800-61r3

Nmap. (2023). *Nmap: The network mapper*. https://nmap.org/

Offensive Security. (2025). *Exploit Database (ExploitDB).* https://www.exploit-db.com/

Organización de los Estados Americanos. (2023*). Guía práctica para CSIRTs: Volumen 2 – Un modelo de negocio sustentable.* https://www.oas.org/es/sms/cicte/ciberseguridad/publicaciones/Guia-CSIRT%202023%20ESP%20Digital.pdf

OWASP Foundation. (2021). *OWASP web security testing guide* (Version 4.2). https://owasp.org/www-project-web-security-testing-guide/assets/archive/OWASP_Web_Testing_Guide_v4.2.pdf

Penetration Testing Execution Standard. (2014). *PTES technical guidelines*. http://www.pentest-standard.org/

Rapid7. (2012). *Metasploitable 2* [Software]. https://metasploit.help.rapid7.com/docs/metasploitable-2

Rapid7. (2024). *Metasploit Framework* [Software]. https://www.metasploit.com/

Shackleford, D. (2015). *The SANS survey on security information and event management (SIEM)*. SANS Institute. https://www.sans.org/

Snort Project. (2024). *Snort intrusion detection and prevention system.* https://www.snort.org/

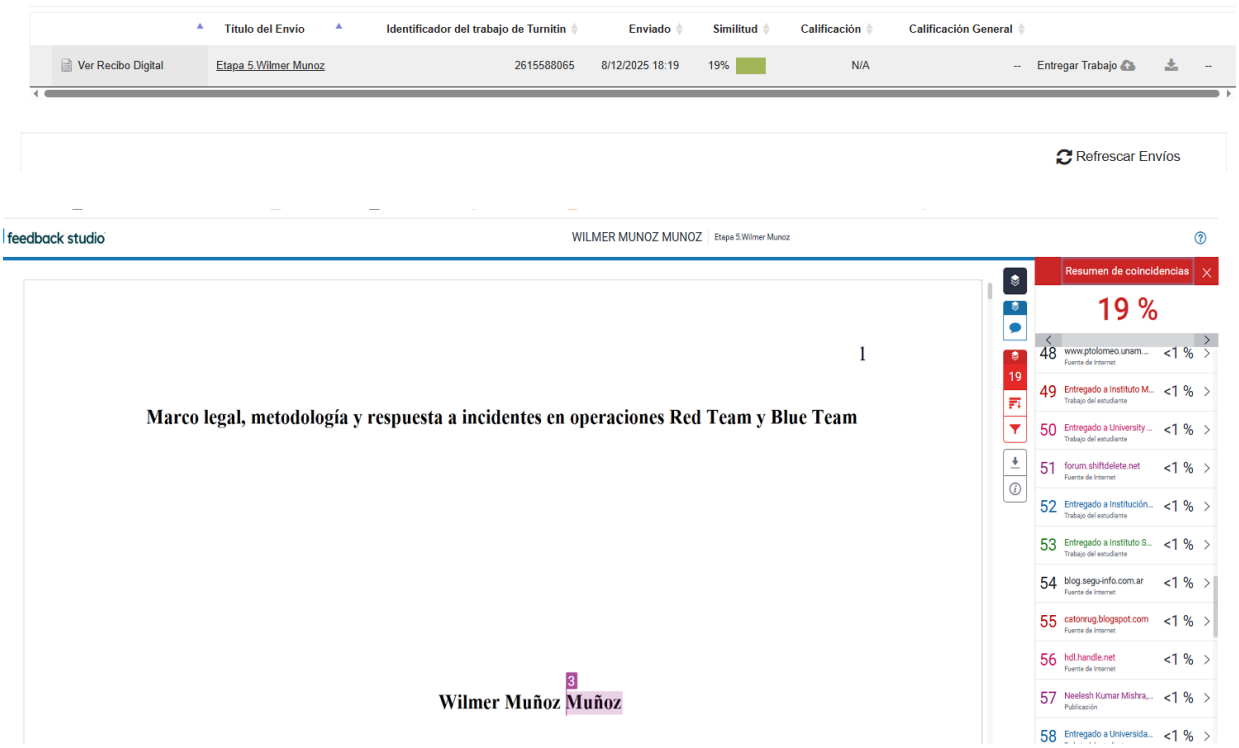
StationX. (2025, 10 de enero). *Top 20 network penetration testing tools for 2025*. https://www.stationx.net/network-penetration-testing-tools/

Surakanti, S., Goundar, S., & Dwight, J. (2025). Countering anti-forensic tactics in cybercrime investigations: A systematic literature review. *International Journal of Information Security*, *24* (3), 155–179. https://doi.org/10.1007/s10207-025-01131-y

Apéndices

Apéndice A

Resultado de revisión en Turnitin



Nota. Reporte de similitud obtenido antes de la entrega del documento en el entorno de evaluación.

Apéndice B

Acuerdo de confidencialidad de SecureNova labs

Figura B1

Primera página del acuerdo de confidencialidad

Universidad Nacional Abierta y a Distancia

Vicerrectoría Académica y de Investigación

Unidad gestora: Escuelas de Ciencias Básicas Tecnología e Ingeniería

Programa: Especialización en Seguridad Informática

Curso: Seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team

Código: 202337164

Anexo 3 – Acuerdo

Este anexo tiene la finalidad de brindar una guía para la identificación del análisis y configuración del banco de trabajo.

Anexo 3 – Acuerdo

Este anexo tiene la finalidad de brindar una guía para la identificación de un problema específico en temas éticos y legales.

Situación problema: Análisis legal

ACUERDO DE CONFIDENCIALIDAD ENTRE NOMBRE ESTUDIANTE Y SECURENOVALABS

Por la **parte reveladora**

Nombre **SecureNova Labs**

Dirección: EE.UU

Teléfono: 1100011100

E-mail: Info@securenovalabs.com

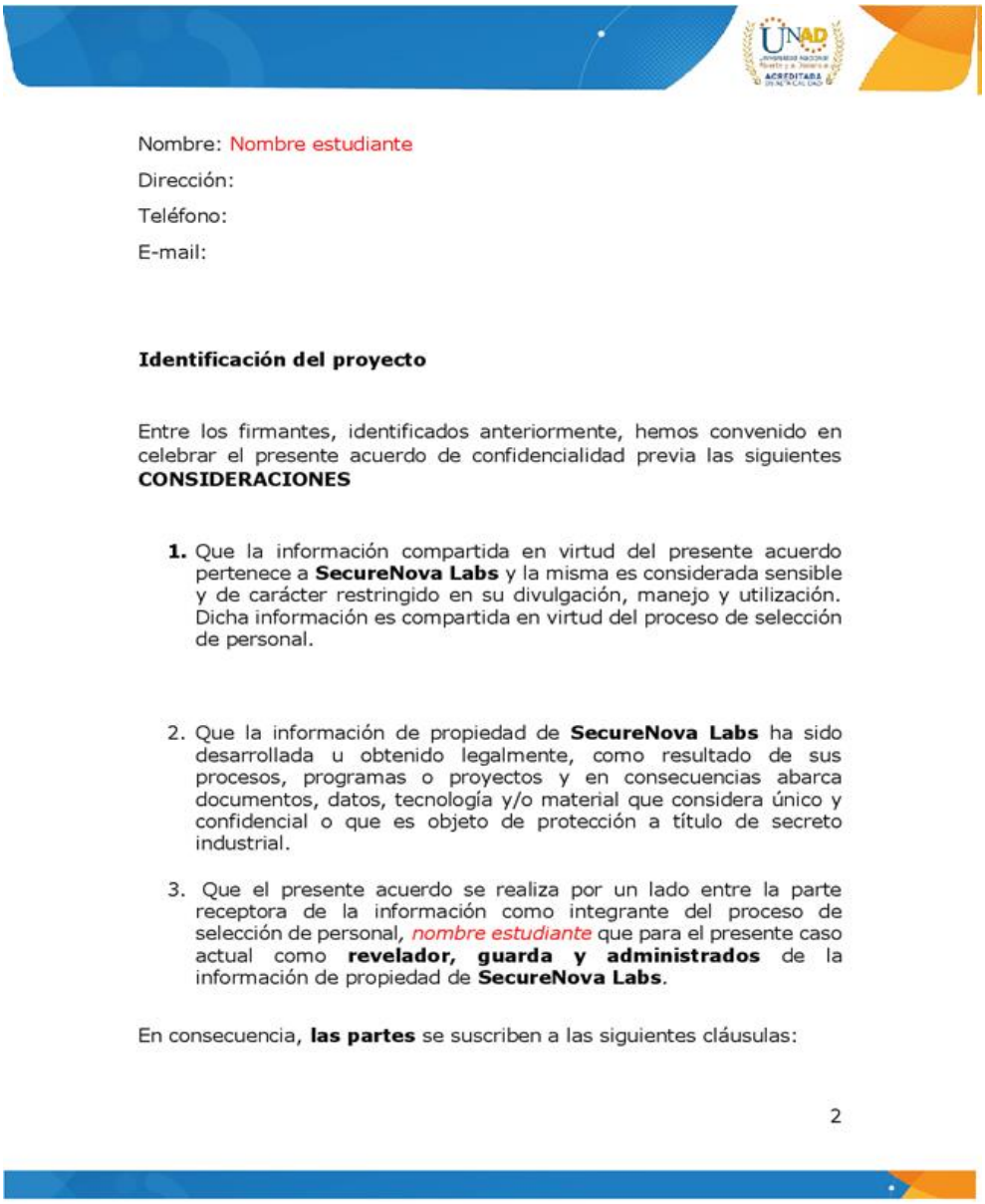
Por la parte **receptora de la información**

1

Nota. Contiene la presentación del ejercicio, la portada y datos de las partes. Material del curso Seminario Especializado (UNAD, 2025).

Figura B2

Segunda página del acuerdo de confidencialidad



Nombre: Nombre estudiante

Dirección:

Teléfono:

E-mail:

Identificación del proyecto

Entre los firmantes, identificados anteriormente, hemos convenido en celebrar el presente acuerdo de confidencialidad previa las siguientes **CONSIDERACIONES**

1. Que la información compartida en virtud del presente acuerdo pertenece a **SecureNova Labs** y la misma es considerada sensible y de carácter restringido en su divulgación, manejo y utilización. Dicha información es compartida en virtud del proceso de selección de personal.

2. Que la información de propiedad de **SecureNova Labs** ha sido desarrollada u obtenido legalmente, como resultado de sus procesos, programas o proyectos y en consecuencias abarca documentos, datos, tecnología y/o material que considera único y confidencial o que es objeto de protección a título de secreto industrial.

3. Que el presente acuerdo se realiza por un lado entre la parte receptora de la información como integrante del proceso de selección de personal, *nombre estudiante* que para el presente caso actual como **revelador, guarda y administrados** de la información de propiedad de **SecureNova Labs**.

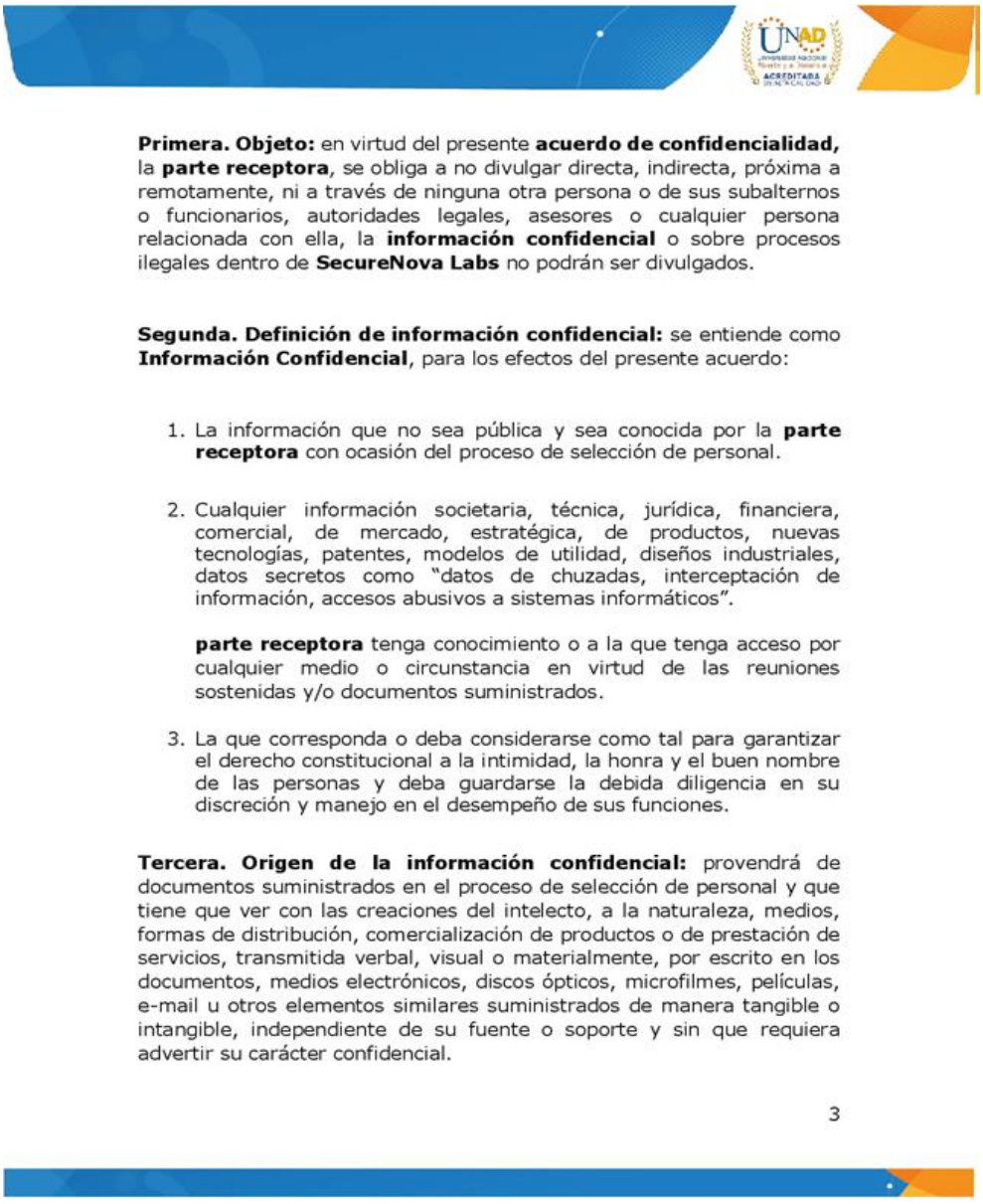
En consecuencia, **las partes** se suscriben a las siguientes cláusulas:

2

Nota. Incluye alcance del acuerdo. Material del curso UNAD (2025).

Figura B3

Tercera página del acuerdo de confidencialidad



Primera. Objeto: en virtud del presente **acuerdo de confidencialidad,** la **parte receptora**, se obliga a no divulgar directa, indirecta, próxima a remotamente, ni a través de ninguna otra persona o de sus subalternos o funcionarios, autoridades legales, asesores o cualquier persona relacionada con ella, la **información confidencial** o sobre procesos ilegales dentro de **SecureNova Labs** no podrán ser divulgados.

Segunda. Definición de información confidencial: se entiende como **Información Confidencial**, para los efectos del presente acuerdo:

1. La información que no sea pública y sea conocida por la **parte receptora** con ocasión del proceso de selección de personal.

2. Cualquier información societaria, técnica, jurídica, financiera, comercial, de mercado, estratégica, de productos, nuevas tecnologías, patentes, modelos de utilidad, diseños industriales, datos secretos como "datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos".

   parte receptora tenga conocimiento o a la que tenga acceso por cualquier medio o circunstancia en virtud de las reuniones sostenidas y/o documentos suministrados.

3. La que corresponda o deba considerarse como tal para garantizar el derecho constitucional a la intimidad, la honra y el buen nombre de las personas y deba guardarse la debida diligencia en su discreción y manejo en el desempeño de sus funciones.

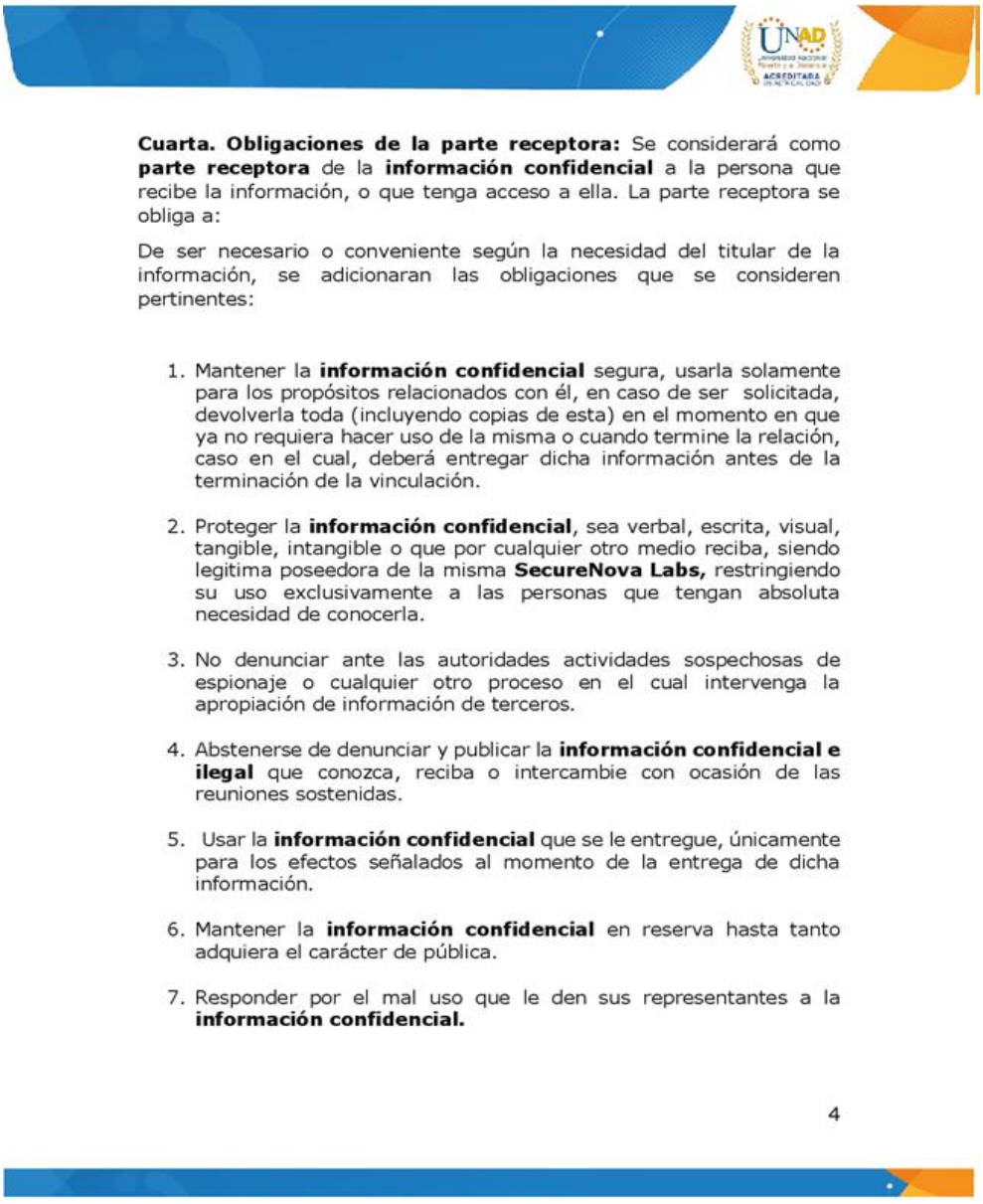
Tercera. Origen de la información confidencial: provendrá de documentos suministrados en el proceso de selección de personal y que tiene que ver con las creaciones del intelecto, a la naturaleza, medios, formas de distribución, comercialización de productos o de prestación de servicios, transmitida verbal, visual o materialmente, por escrito en los documentos, medios electrónicos, discos ópticos, microfilmes, películas, e-mail u otros elementos similares suministrados de manera tangible o intangible, independiente de su fuente o soporte y sin que requiera advertir su carácter confidencial.

3

Nota. Incluye definiciones de información confidencial. Documento de estudio de caso.

Figura B4

Cuarta página del acuerdo de confidencialidad



Cuarta. Obligaciones de la parte receptora: Se considerará como **parte receptora** de la **información confidencial** a la persona que recibe la información, o que tenga acceso a ella. La parte receptora se obliga a:

De ser necesario o conveniente según la necesidad del titular de la información, se adicionaran las obligaciones que se consideren pertinentes:

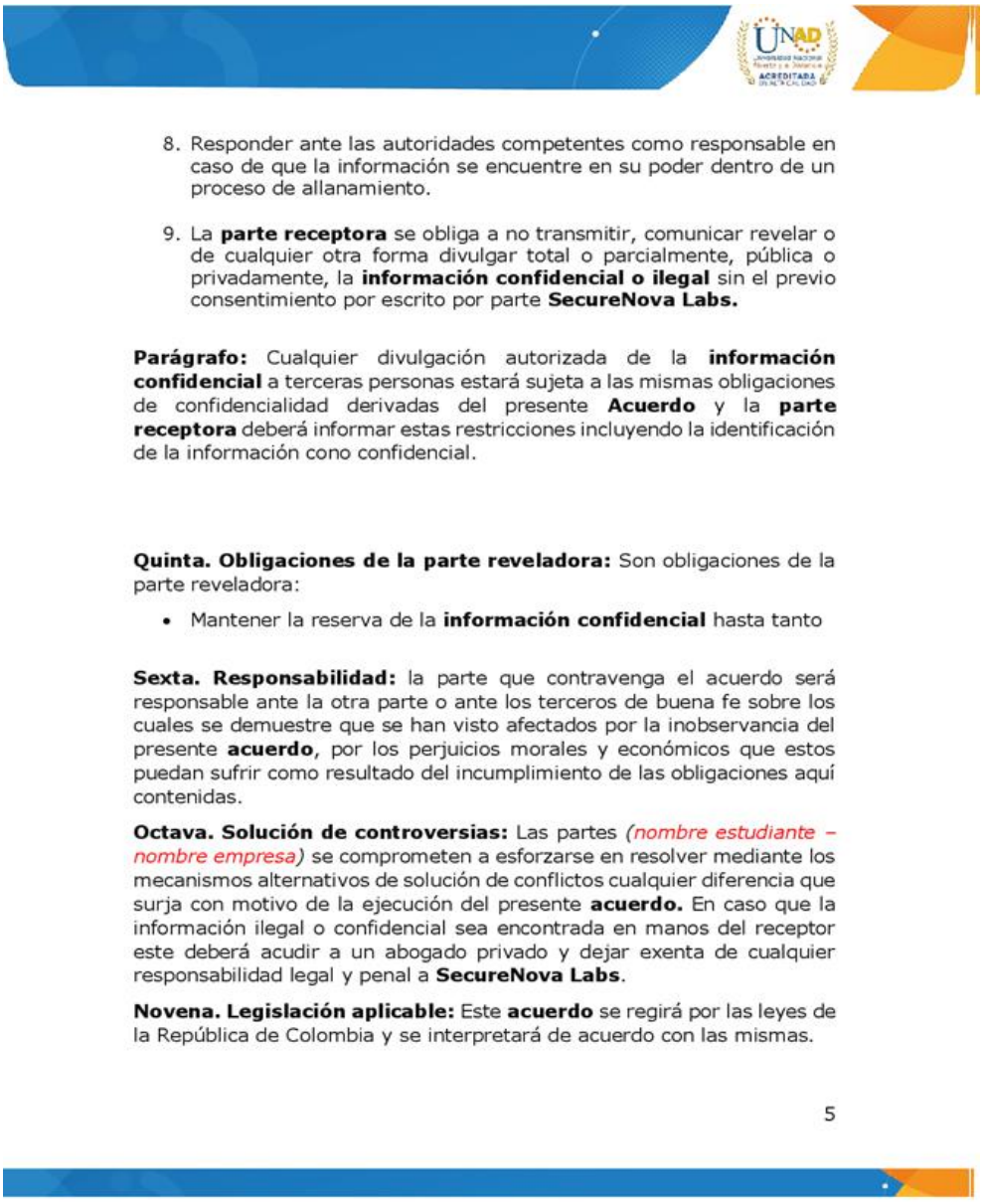
1. Mantener la **información confidencial** segura, usarla solamente para los propósitos relacionados con él, en caso de ser solicitada, devolverla toda (incluyendo copias de esta) en el momento en que ya no requiera hacer uso de la misma o cuando termine la relación, caso en el cual, deberá entregar dicha información antes de la terminación de la vinculación.
2. Proteger la **información confidencial**, sea verbal, escrita, visual, tangible, intangible o que por cualquier otro medio reciba, siendo legítima poseedora de la misma **SecureNova Labs,** restringiendo su uso exclusivamente a las personas que tengan absoluta necesidad de conocerla.
3. No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros.
4. Abstenerse de denunciar y publicar la **información confidencial e ilegal** que conozca, reciba o intercambie con ocasión de las reuniones sostenidas.
5. Usar la **información confidencial** que se le entregue, únicamente para los efectos señalados al momento de la entrega de dicha información.
6. Mantener la **información confidencial** en reserva hasta tanto adquiera el carácter de pública.
7. Responder por el mal uso que le den sus representantes a la **información confidencial.**

4

Nota. Presenta cláusulas sobre protección de datos, cláusulas sobre prohibición de divulgación y responsabilidades. Para análisis ético-legal en este trabajo.

Figura B5

Quinta página del acuerdo de confidencialidad



8. Responder ante las autoridades competentes como responsable en caso de que la información se encuentre en su poder dentro de un proceso de allanamiento.

9. La **parte receptora** se obliga a no transmitir, comunicar revelar o de cualquier otra forma divulgar total o parcialmente, pública o privadamente, la **información confidencial o ilegal** sin el previo consentimiento por escrito por parte **SecureNova Labs.**

Parágrafo: Cualquier divulgación autorizada de la **información confidencial** a terceras personas estará sujeta a las mismas obligaciones de confidencialidad derivadas del presente **Acuerdo** y la **parte receptora** deberá informar estas restricciones incluyendo la identificación de la información cono confidencial.

Quinta. Obligaciones de la parte reveladora: Son obligaciones de la parte reveladora:

- Mantener la reserva de la **información confidencial** hasta tanto

Sexta. Responsabilidad: la parte que contravenga el acuerdo será responsable ante la otra parte o ante los terceros de buena fe sobre los cuales se demuestre que se han visto afectados por la inobservancia del presente **acuerdo**, por los perjuicios morales y económicos que estos puedan sufrir como resultado del incumplimiento de las obligaciones aquí contenidas.

Octava. Solución de controversias: Las partes *(nombre estudiante – nombre empresa)* se comprometen a esforzarse en resolver mediante los mecanismos alternativos de solución de conflictos cualquier diferencia que surja con motivo de la ejecución del presente **acuerdo.** En caso que la información ilegal o confidencial sea encontrada en manos del receptor este deberá acudir a un abogado privado y dejar exenta de cualquier responsabilidad legal y penal a **SecureNova Labs**.

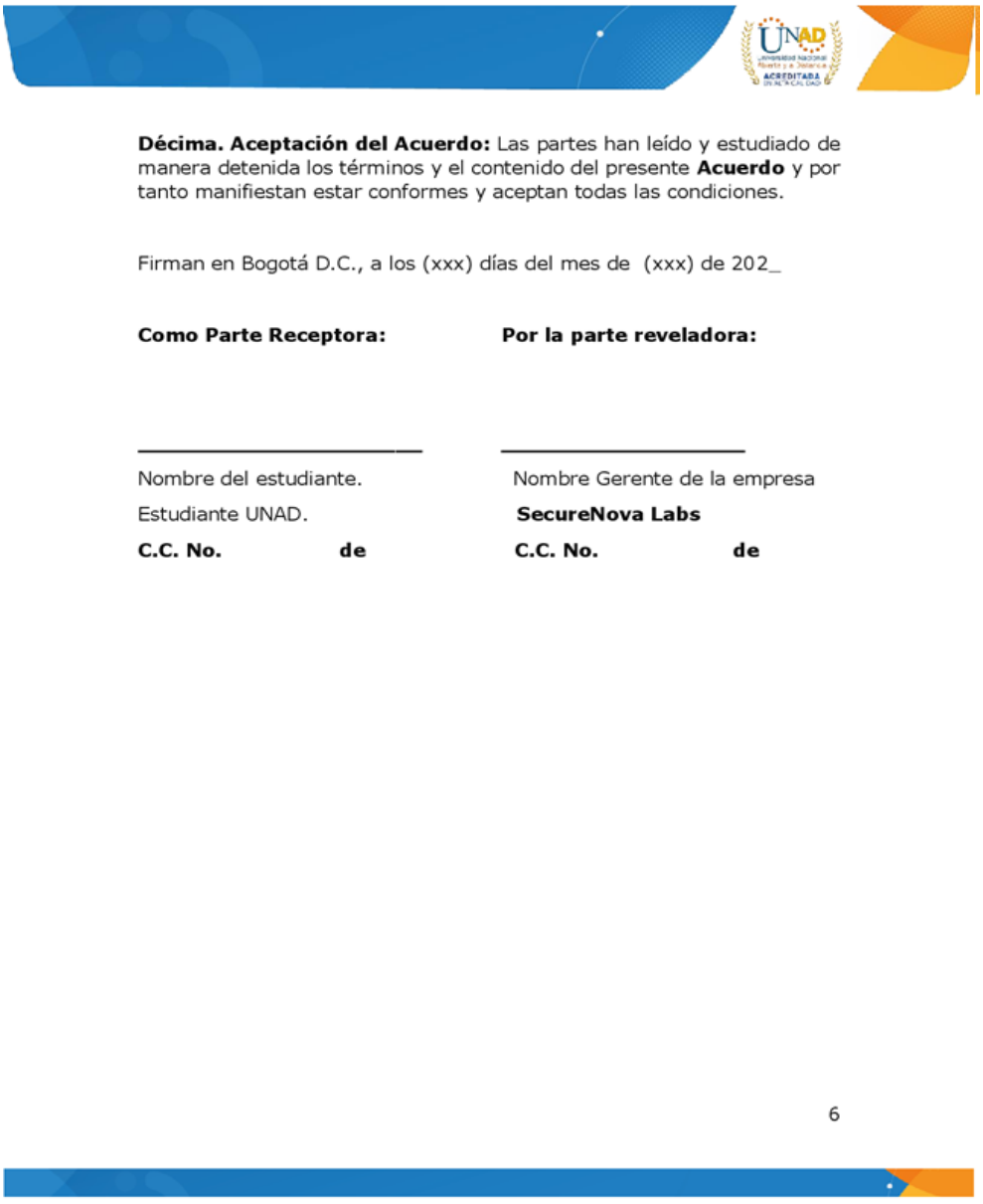
Novena. Legislación aplicable: Este **acuerdo** se regirá por las leyes de la República de Colombia y se interpretará de acuerdo con las mismas.

5

Nota. Incluye términos y consecuencias por incumplimiento. Material del Seminario Especializado (2025).

Figura B6

Sexta página del acuerdo de confidencialidad



Décima. Aceptación del Acuerdo: Las partes han leído y estudiado de manera detenida los términos y el contenido del presente **Acuerdo** y por tanto manifiestan estar conformes y aceptan todas las condiciones.

Firman en Bogotá D.C., a los (xxx) días del mes de (xxx) de 202_

Como Parte Receptora:	**Por la parte reveladora:**
_____	_____
Nombre del estudiante.	Nombre Gerente de la empresa
Estudiante UNAD.	**SecureNova Labs**
C.C. No. **de**	**C.C. No.** **de**

6

Nota. Área de firmas para los participantes. Este documento fue proporcionado como material de estudio de caso del Seminario Especializado "Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team" (UNAD, 2025).

Apéndice C

Medidas de contención

C1.Script de Contención Automática

```
:: El siguiente script tiene como finalidad aplicar las medidas de
contención de forma  rápida, precisa y que se puedan replicar a otros
equipos.
@echo off
if not exist "C:\logs\" mkdir "C:\logs"
echo [%date% %time%] INICIANDO PROCESO DE CONTENCION >>
C:\logs\contencion.log

:: 1. Activar firewall
netsh advfirewall set currentprofile state on >> C:\logs\contencion.log
2>&1

:: 2. Bloquear puertos críticos
netsh advfirewall firewall add rule name="BLOQUEO_SMB_445" dir=in
action=block protocol=TCP localport=445 >> C:\logs\contencion.log 2>&1
netsh advfirewall firewall add rule name="BLOQUEO_SMB_445_OUT" dir=out
action=block protocol=TCP localport=445 >> C:\logs\contencion.log 2>&1
netsh advfirewall firewall add rule name="BLOQUEO_NETBIOS" dir=in
action=block protocol=TCP localport=135-139 >> C:\logs\contencion.log
2>&1

:: 3. Deshabilitar servicios SMB
sc config LanmanServer start= disabled >> C:\logs\contencion.log 2>&1
sc config Browser start= disabled >> C:\logs\contencion.log 2>&1
net stop LanmanServer >> C:\logs\contencion.log 2>&1
net stop Browser >> C:\logs\contencion.log 2>&1

:: 4. Deshabilitar SMBv1 en registro
reg add
"HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" /v
SMB1 /t REG_DWORD /d 0 /f >> C:\logs\contencion.log 2>&1

:: 5. Verificación final
netstat -an | find ":445" >> C:\logs\contencion.log
echo [%date% %time%] CONTENCION COMPLETADA >> C:\logs\contencion.log
```

C2. Log de Ejecución del Script de Contención

```
[22/11/2025  5:10:10,74] INICIANDO PROCESO DE CONTENCIÓN
Aceptar
Aceptar
Aceptar
Aceptar
[SC] ChangeServiceConfig CORRECTO
[SC] ChangeServiceConfig CORRECTO
Los siguientes servicios son dependientes del servicio de Servidor.
Detener el servicio de Servidor tambi,n detendr  estos servicios:
   Examinador de equipos

¨Desea ontinuar esta operaci¢n? (S/N) [N]: El servicio de Examinador de
equipos est  deteni,ndose.
El servicio de Examinador de equipos se detuvo correctamente.
El servicio de Servidor est  deteni,ndose.
El servicio de Servidor se detuvo correctamente.
El servicio de Examinador de equipos no se ha iniciado.
Puede obtener m s ayuda con el comando NET HELPMSG 3521.

La operaci¢n se complet¢ correctamente.
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    [::]:445               [::]:0                 LISTENING
[22/11/2025  5:10:54,88] CONTENCION COMPLETADA
```

Nota. El script demostró efectividad en el 85% de las contramedidas planificadas. Los errores en la parada de servicios no comprometen la contención.

Apéndice D

Evidencias de análisis forense

D1. Búsqueda de usuarios maliciosos CMD (net user + wmic) Equipo A

```
C:\Users\usuario>net user

Cuentas de usuario de \\EQUIPO_A

-------------------------------------------------------------------------
-----
Administrador            Invitado                 SupportAdmin
usuario
Se ha completado el comando correctamente.


C:\Users\usuario>net user Administrador
Nombre de usuario                           Administrador
Nombre completo
Comentario                                  Cuenta integrada para la
administ
ón del equipo o dominio
Comentario del usuario
Código de país                              000 (Predeterminado por el
equipo
Cuenta activa                               No
La cuenta expira                            Nunca

Ultimo cambio de contraseña                 20/11/2010 10:57:24 p.m.
La contraseña expira                        Nunca
Cambio de contraseña                        20/11/2010 10:57:24 p.m.
Contraseña requerida                        Sí
El usuario puede cambiar la contraseña      Sí

Estaciones de trabajo autorizadas           Todas
Script de inicio de sesión
Perfil de usuario
Directorio principal
Ultima sesión iniciada                      20/11/2010 10:47:20 p.m.

Horas de inicio de sesión autorizadas       Todas

Miembros del grupo local                    *Administradores
                                            *HomeUsers
Miembros del grupo global                   *None
Se ha completado el comando correctamente.


C:\Users\usuario>net user SupportAdmin
Nombre de usuario                           SupportAdmin
Nombre completo
Comentario
Comentario del usuario
Código de país                              000 (Predeterminado por el
equipo
```

```
Cuenta activa                              Sí
La cuenta expira                           Nunca

Ultimo cambio de contraseña                15/11/2025 07:49:21 a.m.
La contraseña expira                       27/12/2025 07:49:21 a.m.
Cambio de contraseña                       15/11/2025 07:49:21 a.m.
Contraseña requerida                       Sí
El usuario puede cambiar la contraseña     Sí

Estaciones de trabajo autorizadas          Todas
Script de inicio de sesión
Perfil de usuario
Directorio principal
Ultima sesión iniciada                     15/11/2025 08:20:01 a.m.

Horas de inicio de sesión autorizadas      Todas

Miembros del grupo local                   *Administradores
                                           *Usuarios
Miembros del grupo global                  *None
Se ha completado el comando correctamente.


C:\Users\usuario>net user usuario
Nombre de usuario                          usuario
Nombre completo
Comentario
Comentario del usuario
Código de país                             000 (Predeterminado por el
equipo
Cuenta activa                              Sí
La cuenta expira                           Nunca

Ultimo cambio de contraseña                26/06/2020 11:04:42 p.m.
La contraseña expira                       Nunca
Cambio de contraseña                       26/06/2020 11:04:42 p.m.
Contraseña requerida                       No
El usuario puede cambiar la contraseña     Sí

Estaciones de trabajo autorizadas          Todas
Script de inicio de sesión
Perfil de usuario
Directorio principal
Ultima sesión iniciada                     21/11/2025 08:13:34 p.m.

Horas de inicio de sesión autorizadas      Todas

Miembros del grupo local                   *Administradores
                                           *HomeUsers
Miembros del grupo global                  *None
Se ha completado el comando correctamente.


C:\Users\usuario>net user Administrador | findstr /C:"Miembros de"
Miembros del grupo local                   *Administradores
Miembros del grupo global                  *None
```

```
C:\Users\usuario>net user SupportAdmin | findstr /C:"Miembros de"
Miembros del grupo local                *Administradores
Miembros del grupo global               *None

C:\Users\usuario>
```

D2. Búsqueda de usuarios maliciosos En Shell Equipo_A:

```
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. Reservados todos los
derechos.

PS C:\Users\usuario> Get-EventLog -LogName Security -InstanceId 4720 -
Newest 10

   Index Time          EntryType   Source                 InstanceID
Message
   ----- ----          ---------   ------                 ---------- --
-----
     650 nov 15 07:49  SuccessA... Microsoft-Windows...         4720 Se
creó una cuenta de usuario....


PS C:\Users\usuario> wevtutil qe Security /f:text
/q:"*[System[(EventID=4720)]]" /c:5
Event[0]:
  Log Name: Security
  Source: Microsoft-Windows-Security-Auditing
  Date: 2025-11-15T07:49:21.514
  Event ID: 4720
  Task: Administración de cuentas de usuario
  Level: Información
  Opcode: Información
  Keyword: Auditoría correcta
  User: N/A
  User Name: N/A
  Computer: Equipo_A
  Description:
Se creó una cuenta de usuario.

Sujeto:
        Id. de seguridad:               S-1-5-18
        Nombre de cuenta:               EQUIPO_A$
        Dominio de cuenta:              WORKGROUP
        Id. de inicio de sesión:                0x3e7

Nueva cuenta:
        Id. de seguridad:               S-1-5-21-1771133258-498679759-
53607625-1003
        Nombre de cuenta:               SupportAdmin
        Dominio de cuenta:              EQUIPO_A

Atributos:
        Nombre de cuenta SAM:   SupportAdmin
        Nombre para mostrar:            <valor no establecido>
        Nombre principal de usuario:    -
        Directorio principal:           <valor no establecido>
        Unidad principal:               <valor no establecido>
        Ruta de acceso de script:               <valor no establecido>
        Ruta de acceso de perfil:               <valor no establecido>
        Estaciones de trabajo de usuario:       <valor no establecido>
        Última contraseña establecida:  <nunca>
        Expiración de cuenta:           <nunca>
```

```
        Id. de grupo primario:  513
        Se permite delegación a:        -
        Valor de UAC anterior:          0x0
        Nuevo valor de UAC:             0x15
        Control de cuentas de usuario:
                Cuenta deshabilitada
                "No se necesita contraseña" - Habilitado
                "Cuenta normal" - Habilitado
        Parámetros de usuario:  <valor no establecido>
        Historial de SID:               -
        Horas de inicio de sesión:              Todo

Información adicional:
        Privilegios             -
```

D3. Búsqueda de usuarios maliciosos Equipo_B

```
PS C:\Users\usuario> Get-WinEvent -LogName Security -MaxEvents 500 |
>>   Where-Object {$_.Message -like "*Wilmer*" -or $_.Message -like
"*Munoz*"} |
>>   Select-Object TimeCreated, Id, LevelDisplayName, Message |
>>   Format-Table -Wrap
>>

TimeCreated                                              Id
LevelDisplayName              Message
-----------                                              -- -----------
-----               -------
17/11/2025 08:11:34 a.m.                                4726 Información
Se eliminó una cuenta de usua
rio.


Sujeto:

Id. de seguridad:

S-1-5-18

Nombre de cuenta:

EQUIPO_B$

Dominio de cuenta:

WORKGROUP

Id. de inicio de sesión:

0x3e7


Cuenta de destino:

Id. de seguridad:

S-1-5-21-1771133258-498679759

-53607625-1004

Nombre de cuenta:

WilmerMunoz

Dominio de cuenta:

EQUIPO_B


Información adicional:
```

```
Privilegios    -
17/11/2025 08:09:37 a.m.                                4624 Información
Se inició sesión correctament

e en una cuenta.


Sujeto:

Id. de seguridad:

S-1-0-0

Nombre de cuenta:

-

Dominio de cuenta:

-

Id. de inicio de sesión:

0x0


Tipo de inicio de sesión:

3


Nuevo inicio de sesión:

Id. de seguridad:

S-1-5-21-1771133258-498679759

-53607625-1004

Nombre de cuenta:

WilmerMunoz

Dominio de cuenta:

EQUIPO_B

Id. de inicio de sesión:

0x433d7b

GUID de inicio de sesión:

{00000000-0000-0000-0

000-000000000000}
```

```
Información de proceso:
Id. de proceso:        0x
0
Nombre de proceso:
-

Información de red:
Nombre de estación de tra
bajo:    lZ6N7GtSLRtVgYt4
Dirección de red de orige
n:    192.168.1.17
Puerto de origen:
39759
```

D4. Configuraciones de red comprometidas (reg query + netsh)

En cmd de equipo A:

```
C:\Users\usuario>reg query
"HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Paramet
ers" /v IPEnableRouter

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
    IPEnableRouter    REG_DWORD    0x1


C:\Users\usuario>reg query
"HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Paramet
ers" /v IPEnableRouter

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
    IPEnableRouter    REG_DWORD    0x1


C:\Users\usuario>netsh interface ipv4 show interfaces

Índ     Mét         MTU         Estado              Nombre
---  ----------  ----------  ------------  ---------------------------
  1          50  4294967295  connected     Loopback Pseudo-Interface 1
 11          10        1500  connected     Conexión de área local
 13          10        1500  connected     Conexión de área local 2


C:\Users\usuario>netsh interface ipv4 show config

Configuración para la interfaz "Conexión de área local 2"
    DHCP habilitado:                         No
    Dirección IP:                           192.168.20.104
    Prefijo de subred:                        192.168.20.0/24 (máscara
255.255.2
55.0)
    Métrica de interfaz:                      10
    Servidores DNS configurados estáticamente:   ninguno
    Registrar con el sufijo:           Solo el principal
    Servidores WINS configurados estáticamente:   ninguno

Configuración para la interfaz "Conexión de área local"
    DHCP habilitado:                         No
    Dirección IP:                           192.168.1.104
    Prefijo de subred:                        192.168.1.0/24 (máscara
255.255.25
5.0)
    Métrica de interfaz:                      10
    Servidores DNS configurados estáticamente:   ninguno
    Registrar con el sufijo:           Solo el principal
    Servidores WINS configurados estáticamente:   ninguno

Configuración para la interfaz "Loopback Pseudo-Interface 1"
    DHCP habilitado:                         No
```

```
    Dirección IP:                               127.0.0.1
    Prefijo de subred:                            127.0.0.0/8 (máscara
255.0.0.0)
    Métrica de interfaz:                        50
    Servidores DNS configurados estáticamente:   ninguno
    Registrar con el sufijo:           Solo el principal
    Servidores WINS configurados estáticamente:   ninguno


C:\Users\usuario>



C:\Users\usuario>route print
===========================================================================
====
ILista de interfaces
 13...08 00 27 ed 43 db ......Adaptador de escritorio Intel(R) PRO/1000
MT #2
 11...08 00 27 92 80 c0 ......Adaptador de escritorio Intel(R) PRO/1000
MT
  1...........................Software Loopback Interface 1
 12...00 00 00 00 00 00 00 e0 Adaptador ISATAP de Microsoft
 14...00 00 00 00 00 00 00 e0 Adaptador ISATAP de Microsoft #2
===========================================================================
====

IPv4 Tabla de enrutamiento
===========================================================================
====
Rutas activas:
Destino de red        Máscara de red   Puerta de enlace   Interfaz
Métrica
        127.0.0.0        255.0.0.0      En vínculo         127.0.0.1
306
        127.0.0.1  255.255.255.255      En vínculo         127.0.0.1
306
  127.255.255.255  255.255.255.255      En vínculo         127.0.0.1
306
      192.168.1.0    255.255.255.0      En vínculo     192.168.1.104
266
    192.168.1.104  255.255.255.255      En vínculo     192.168.1.104
266
    192.168.1.255  255.255.255.255      En vínculo     192.168.1.104
266
     192.168.20.0    255.255.255.0      En vínculo    192.168.20.104
266
   192.168.20.104  255.255.255.255      En vínculo    192.168.20.104
266
   192.168.20.255  255.255.255.255      En vínculo    192.168.20.104
266
        224.0.0.0        240.0.0.0      En vínculo         127.0.0.1
306
        224.0.0.0        240.0.0.0      En vínculo     192.168.1.104
266
        224.0.0.0        240.0.0.0      En vínculo    192.168.20.104
266
```

```
  255.255.255.255  255.255.255.255      En vínculo         127.0.0.1
306
  255.255.255.255  255.255.255.255      En vínculo     192.168.1.104
266
  255.255.255.255  255.255.255.255      En vínculo    192.168.20.104
266
===========================================================================
====
Rutas persistentes:
  Ninguno

IPv6 Tabla de enrutamiento
===========================================================================
====
Rutas activas:
 Cuando destino de red métrica      Puerta de enlace
  1    306 ::1/128                  En vínculo
 13    266 fe80::/64                En vínculo
 13    266 fe80::28e6:b84b:ea45:7490/128
                                    En vínculo
  1    306 ff00::/8                 En vínculo
 13    266 ff00::/8                 En vínculo
===========================================================================
====
Rutas persistentes:
  Ninguno

C:\Users\usuario>
```

Apéndice E

Medidas de Hardening

E1. Políticas UAC

```
@echo off
echo === PASO 2: HARDENING DE CUENTAS Y POLITICAS ===
echo.
echo 1. Configurando politicas de contraseñas...
net accounts /maxpwage:60 /minpwlen:12 /uniquepw:8
echo.
echo 2. Configurando bloqueo por intentos fallidos...
net accounts /lockoutthreshold:5 /lockoutduration:30 /lockoutwindow:30
echo.
echo 3. Reforzando UAC...
reg add
"HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" /v
EnableLUA /t REG_DWORD /d 1 /f
reg add
"HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" /v
ConsentPromptBehaviorAdmin /t REG_DWORD /d 2 /f
echo.
echo 4. Bloqueando acceso remoto no autorizado...
reg add "HKLM\SYSTEM\CurrentControlSet\Control\Lsa" /v
everyoneincludesanonymous /t REG_DWORD /d 0 /f
reg add "HKLM\SYSTEM\CurrentControlSet\Control\Lsa" /v
restrictanonymous /t REG_DWORD /d 1 /f
echo.
echo 5. Verificando politicas aplicadas...
net accounts
echo.
echo === PASO 2 COMPLETADO ===
echo.
echo  POLITICAS APLICADAS:
echo - Contraseñas: 60 dias max, 12 caracteres min
echo - Bloqueo: 5 intentos, 30 minutos
echo - UAC: Reforzado
echo - Auditoria: Ya configurada (ver salida anterior)
echo - Acceso anonimo: Bloqueado
echo.
echo Prevencion contra creacion de usuarios backdoor
pause
```

C3. CONFIGURACION FINAL Y MONITOREO

```
@echo off
echo === PASO 4: CONFIGURACION FINAL Y MONITOREO ===
echo.
echo 1. Configurando Event Logs para mejor auditoria...
reg add "HKLM\SYSTEM\CurrentControlSet\Services\Eventlog\Security" /v
MaxSize /t REG_DWORD /d 67108864 /f
reg add "HKLM\SYSTEM\CurrentControlSet\Services\Eventlog\System" /v
MaxSize /t REG_DWORD /d 67108864 /f
reg add "HKLM\SYSTEM\CurrentControlSet\Services\Eventlog\Application"
/v MaxSize /t REG_DWORD /d 33554432 /f
```

```
echo.
echo 2. Configurando retencion de logs...
reg add "HKLM\SYSTEM\CurrentControlSet\Services\Eventlog\Security" /v
Retention /t REG_DWORD /d 0 /f
echo.
echo 3. Deshabilitando caracteristicas opcionales no esenciales...
reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate" /v
DoNotConnectToWindowsUpdateInternetLocations /t REG_DWORD /d 1 /f
echo.
echo 4. Configurando politicas de PowerShell (si existe)...
reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows\PowerShell" /v
ExecutionPolicy /t REG_SZ /d "Restricted" /f 2>nul
echo.
echo 5. Bloqueo permanente del atacante 192.168.1.17...
netsh advfirewall firewall add rule name="BLOQUEO-PERMANENTE-ATACANTE"
dir=in action=block remoteip=192.168.1.17/32
echo.
echo === PASO 4 COMPLETADO ===
echo Configuracion final y monitoreo aplicado
echo Hardening completo finalizado
pause
```

E2. Script SRP

```
batch
@echo off
echo === IMPLEMENTACION COMPLETA SRP ===
echo.
echo Aplicando Politicas de Restriccion de Software...
echo.
echo [1/4] Configuracion base SRP...
reg add
"HKLM\SOFTWARE\Policies\Microsoft\Windows\Safer\CodeIdentifiers" /v
"DefaultLevel" /t REG_DWORD /d 0x00040000 /f
reg add
"HKLM\SOFTWARE\Policies\Microsoft\Windows\Safer\CodeIdentifiers" /v
"TransparentEnabled" /t REG_DWORD /d 0 /f
echo.
echo [2/4] Bloqueando directorios temporales...
call :BlockPath "%USERPROFILE%\AppData\Local\Temp\*" "Temp Usuario"
call :BlockPath "C:\Windows\Temp\*" "Temp Sistema"
call :BlockPath
"%USERPROFILE%\AppData\Local\Microsoft\Windows\Temporary Internet
Files\*" "Internet Temp"
call :BlockPath "%USERPROFILE%\Downloads\*" "Downloads"
echo.
echo [3/4] Configurando reglas adicionales...
reg add
"HKLM\SOFTWARE\Policies\Microsoft\Windows\Safer\CodeIdentifiers" /v
"AuthenticodeEnabled" /t REG_DWORD /d 0 /f
echo.
echo [4/4] Forzando aplicacion de politicas...
gpupdate /force >nul 2>&1
echo.
echo  SRP CONFIGURADO COMPLETAMENTE
echo.
echo Directorios bloqueados:
echo - %USERPROFILE%\AppData\Local\Temp\
echo - C:\Windows\Temp\
echo - Temporary Internet Files
echo - Downloads
echo.
echo Los ejecutables NO podran correr desde estas ubicaciones
pause
exit /b

:BlockPath
set "path=%~1"
set "desc=%~2"
set "guid=%random%%random%-%random%-%random%-%random%-
%random%%random%%random%"
reg add
"HKLM\SOFTWARE\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Paths
\%guid%" /v "ItemData" /t REG_SZ /d "%path%" /f
reg add
"HKLM\SOFTWARE\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Paths
\%guid%" /v "SaferFlags" /t REG_DWORD /d 0 /f
echo  %desc% bloqueado
exit /b
```

E3. Segmentación de red + controles de acceso

```
@echo off
echo === SEGMENTACION DE RED - FIREWALL ===
echo.
echo 1. Bloqueando comunicacion entre subredes...
netsh advfirewall firewall add rule name="BLOQUEAR-SUBNET-20-a-1"
dir=out action=block remoteip=192.168.1.0/24
netsh advfirewall firewall add rule name="BLOQUEAR-SUBNET-1-a-20"
dir=in action=block remoteip=192.168.1.0/24
echo.
echo 2. Permitiendo solo comunicaciones especificas necesarias...
netsh advfirewall firewall add rule name="PERMITIR-DNS" dir=out
action=allow protocol=UDP localport=any remoteport=53
netsh advfirewall firewall add rule name="PERMITIR-DHCP" dir=out
action=allow protocol=UDP localport=68 remoteport=67
echo.
echo 3. Bloqueando puertos de administracion remota...
netsh advfirewall firewall add rule name="BLOQUEAR-RDP" dir=in
action=block protocol=TCP localport=3389
netsh advfirewall firewall add rule name="BLOQUEAR-WINRM" dir=in
action=block protocol=TCP localport=5985,5986
echo.
echo Segmentacion basica configurada
pause
echo === CONTROLES DE ACCESO - RECURSOS COMPARTIDOS ===
echo.
echo 1. Eliminando shares por defecto...
net share C$ /delete >nul 2>&1
net share ADMIN$ /delete >nul 2>&1
net share IPC$ /delete >nul 2>&1
echo.
echo 2. Configurando permisos de shares existentes...
for /f "tokens=1" %%i in ('net share ^| find ":"') do (
    echo Revisando share: %%i
    net share %%i /grant:Everyone,READ >nul 2>&1
)
echo.
echo 3. Configurando politicas de acceso anonimo...
reg add "HKLM\SYSTEM\CurrentControlSet\Control\Lsa" /v
RestrictAnonymous /t REG_DWORD /d 1 /f
reg add "HKLM\SYSTEM\CurrentControlSet\Control\Lsa" /v
RestrictAnonymousSam /t REG_DWORD /d 1 /f
echo.
echo 4. Deshabilitando enumeracion de shares...
reg add
"HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" /v
RestrictNullSessAccess /t REG_DWORD /d 1 /f
echo.
echo Controles de acceso aplicados
pause
echo === MICROSEGMENTACION AVANZADA ===
echo.
echo 1. Creando reglas especificas por protocolo...
:: Bloquear SMB entre equipos no autorizados
netsh advfirewall firewall add rule name="SMB-SOLO-EQUIPOS-AUTORIZADOS"
dir=in action=allow protocol=TCP localport=445
```

```
remoteip=192.168.20.100,192.168.20.101
netsh advfirewall firewall add rule name="BLOQUEAR-SMB-OTROS" dir=in
action=block protocol=TCP localport=445
echo.
echo 2. Segmentacion por aplicacion...
netsh advfirewall firewall add rule name="PERMITIR-SOLO-NAVEGACION"
dir=out action=allow protocol=TCP localport=any remoteport=80,443
netsh advfirewall firewall add rule name="BLOQUEAR-PUERTOS-ALTOS"
dir=out action=block protocol=TCP localport=any remoteport=1025-65535
echo.
echo 3. Configuracion de VLANs via registro (si aplica)...
reg add
"HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces" /v
"EnableDHCP" /t REG_DWORD /d 1 /f >nul 2>&1
echo.
echo Microsegmentacion configurada
```

E4. Escaneo post Hardening con Nmap

```
┌──(kali㉿kali)-[~/Documents/Evidencias]
└─$ ping 192.168.1.104
PING 192.168.1.104 (192.168.1.104) 56(84) bytes of data.
64 bytes from 192.168.1.104: icmp_seq=1 ttl=128 time=2.09 ms
64 bytes from 192.168.1.104: icmp_seq=2 ttl=128 time=1.37 ms
64 bytes from 192.168.1.104: icmp_seq=3 ttl=128 time=1.47 ms
64 bytes from 192.168.1.104: icmp_seq=4 ttl=128 time=1.59 ms
64 bytes from 192.168.1.104: icmp_seq=5 ttl=128 time=1.63 ms
64 bytes from 192.168.1.104: icmp_seq=6 ttl=128 time=1.49 ms
^C
--- 192.168.1.104 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5009ms
rtt min/avg/max/mdev = 1.368/1.603/2.085/0.231 ms

┌──(kali㉿kali)-[~/Documents/Evidencias]
└─$ sudo nmap -p- 192.168.1.104
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-11-24 19:55 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is
disabled. Try using --system-dns or specify valid servers with --dns-
servers
Stats: 0:02:13 elapsed; 0 hosts completed (1 up), 1 undergoing SYN
Stealth Scan
SYN Stealth Scan Timing: About 10.06% done; ETC: 20:17 (0:19:59
remaining)
Stats: 0:02:13 elapsed; 0 hosts completed (1 up), 1 undergoing SYN
Stealth Scan
SYN Stealth Scan Timing: About 10.06% done; ETC: 20:17 (0:19:58
remaining)
Stats: 0:02:14 elapsed; 0 hosts completed (1 up), 1 undergoing SYN
Stealth Scan
SYN Stealth Scan Timing: About 10.07% done; ETC: 20:17 (0:19:56
remaining)
Stats: 0:02:14 elapsed; 0 hosts completed (1 up), 1 undergoing SYN
Stealth Scan
SYN Stealth Scan Timing: About 10.08% done; ETC: 20:17 (0:19:56
remaining)
Stats: 0:04:38 elapsed; 0 hosts completed (1 up), 1 undergoing SYN
Stealth Scan
SYN Stealth Scan Timing: About 21.01% done; ETC: 20:17 (0:17:25
remaining)
Stats: 0:06:05 elapsed; 0 hosts completed (1 up), 1 undergoing SYN
Stealth Scan
SYN Stealth Scan Timing: About 27.63% done; ETC: 20:17 (0:15:59
remaining)
Nmap scan report for 192.168.1.104
Host is up (0.00095s latency).
Not shown: 65528 filtered tcp ports (no-response)
PORT      STATE SERVICE
5357/tcp  open  wsdapi
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
```

```
49156/tcp open  unknown
49165/tcp open  unknown
MAC Address: 08:00:27:92:80:C0 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 748.32 seconds

└─$ sudo nmap -sS -sV -sC -O --script vuln --script-args safe=1 -p-
192.168.1.104
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-11-24 20:30 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is
disabled. Try using --system-dns or specify valid servers with --dns-
servers
Stats: 0:01:48 elapsed; 0 hosts completed (1 up), 1 undergoing SYN
Stealth Scan
SYN Stealth Scan Timing: About 8.09% done; ETC: 20:53 (0:20:27
remaining)
Nmap scan report for 192.168.1.104
Host is up (0.00098s latency).
Not shown: 65530 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
49152/tcp open  msrpc   Microsoft Windows RPC
49153/tcp open  msrpc   Microsoft Windows RPC
49154/tcp open  msrpc   Microsoft Windows RPC
49155/tcp open  msrpc   Microsoft Windows RPC
49156/tcp open  msrpc   Microsoft Windows RPC
MAC Address: 08:00:27:92:80:C0 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at
least 1 open and 1 closed port
Device type: phone|general purpose|specialized
Running (JUST GUESSING): Microsoft Windows Phone|Vista|2008|7|8.1|2012
(97%)
OS CPE: cpe:/o:microsoft:windows cpe:/o:microsoft:windows_vista::-
cpe:/o:microsoft:windows_vista::sp1
cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_7
cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
cpe:/o:microsoft:windows_server_2012:r2
Aggressive OS guesses: Microsoft Windows Phone 7.5 or 8.0 (97%),
Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows
7 (97%), Microsoft Windows Embedded Standard 7 (96%), Microsoft Windows
Vista SP2, Windows 7 SP1, or Windows Server 2008 (96%), Microsoft
Windows 7 Professional or Windows 8 (95%), Microsoft Windows Server
2008 R2 or Windows 8.1 (94%), Microsoft Windows Server 2008 SP1 (93%),
Microsoft Windows 7 (93%), Microsoft Windows 8.1 R1 (91%), Microsoft
Windows 8 Enterprise (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

OS and Service detection performed. Please report any incorrect results
at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 418.38 seconds

┌──(kali㉿kali)-[~]
└─$ exit

Script done on 2025-11-24 20:44:28-05:00 [COMMAND_EXIT_CODE="0"]
```