Microsentinel: plataforma de análisis y monitoreo en ciberseguridad para agencias del sector de telecomunicaciones en Colombia

Mario Alexis Chaparro Gómez

Asesora

Maritza Farley Mondragon Guzmán

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería (ECBTI)

Ingeniería de Telecomunicaciones

2026

Agradecimientos

En primer lugar, agradezco a Dios por darme la fortaleza y la determinación necesarias para superar los desafíos y completar este proyecto de grado. Su guía ha sido mi mayor fuente de inspiración durante este recorrido.

Agradezco profundamente a la Universidad Nacional Abierta y a Distancia (UNAD) por brindarme la oportunidad de formarme en un entorno flexible y accesible, que me ha permitido combinar mis responsabilidades profesionales y personales con el desarrollo académico. Gracias a su modelo educativo, es posible alcanzar metas que parecían inalcanzables.

Un agradecimiento especial a la Ingeniera Maritza Farley Mondragon Guzman, por su valioso acompañamiento como asesora y directora de este proyecto. Su experiencia y orientación han sido fundamentales para mi crecimiento profesional y para la culminación exitosa de este trabajo. Su apoyo constante ha hecho de este proceso una experiencia enriquecedora.

Dedicatoria

A Dios por escogerme como uno de sus hijos favoritos y darme la fuerza necesaria para cumplir esta meta. A mi esposa por su apoyo incondicional, por su sabiduría, por su perseverancia, por su tesón, por ser el mejor ejemplo para seguir. A mi hijo por ser el motor que mueve mi día a día. A la ingeniera Maritza Farley Mondragon Guzmán por todo su acompañamiento para lograr finalizar este proyecto.

Resumen

Microsentinel es una solución tecnológica desarrollada con el propósito de fortalecer la ciberseguridad de las pequeñas y medianas empresas del sector telecomunicaciones en Colombia, las cuales presentan altos niveles de vulnerabilidad frente a las crecientes amenazas digitales. Este proyecto de aplicación se enfoca en el diseño e implementación de una herramienta de análisis automatizado que permite identificar vulnerabilidades comunes en infraestructuras expuestas, especialmente en entornos web, mediante el uso de tecnologías open-source como Nmap, Nikto, WPScan, WhatWeb y sqlmap.

Adicionalmente, Microsentinel incorpora un enfoque formativo mediante la integración de un módulo educativo contextual, el cual vincula los resultados del análisis con recomendaciones prácticas y contenido explicativo, contribuyendo al fortalecimiento de la cultura de ciberseguridad dentro de las organizaciones. Asimismo, el sistema incluye un protocolo de uso ético y legal que garantiza la ejecución responsable de las pruebas de seguridad, solicitando la validación previa del usuario antes de realizar cualquier análisis.

***Palabras clave*:** ciberseguridad, pymes, telecomunicaciones, vulnerabilidades, análisis

Abstract

Microsentinel is a technological solution designed to strengthen cybersecurity in small and medium-sized enterprises (SMEs) within the telecommunications sector in Colombia, which face increasing exposure to cyber threats and often lack adequate protection mechanisms. This applied project focuses on the design and implementation of an automated analysis tool aimed at identifying common vulnerabilities in exposed infrastructures, particularly in web environments, through the integration of open-source technologies such as Nmap, Nikto, WPScan, WhatWeb, and sqlmap.

Additionally, Microsentinel integrates a contextual educational module that links technical findings with practical recommendations and explanatory content, contributing to the development of cybersecurity awareness within organizations. The system also includes an ethical and legal usage protocol, requiring user confirmation prior to executing any analysis, ensuring responsible and authorized use of security testing tools.

Keywords**:** cybersecurity, smes, telecommunications, vulnerabilities, automated

Tabla de contenido

Lista de figuras

Glosario

Ciberseguridad: Práctica de proteger sistemas, redes y programas de ataques digitales.

PYMEs: Abreviatura de Pequeñas y Medianas Empresas, que suelen tener recursos limitados en comparación con grandes corporaciones.

Amenazas Cibernéticas: Cualquier posible peligro que puede dañar o robar datos e interrumpir las operaciones digitales.

Evaluación de Riesgos: Proceso de identificar, analizar y evaluar riesgos potenciales para la seguridad de una organización.

NIST: Instituto Nacional de Estándares y Tecnología, que proporciona un marco de seguridad reconocido internacionalmente.

Medidas de Seguridad: Acciones y protocolos implementados para proteger sistemas y datos contra ciberataques.

Capacitación: Proceso de educar y entrenar al personal en prácticas de seguridad cibernética.

Resiliencia Digital: Capacidad de una organización para recuperarse rápidamente de incidentes cibernéticos y continuar operando eficazmente.

Máquinas Virtuales: Entornos computacionales creados mediante software que permiten ejecutar sistemas operativos y aplicaciones de forma aislada en una única máquina física.

OWASP: Open Web Application Security Project, organización mundial sin fines de lucro enfocada en mejorar la seguridad del software y las aplicaciones web.

Hacking Ético: Práctica de probar sistemas y redes en busca de vulnerabilidades, utilizando los mismos métodos que los hackers malintencionados, pero con el objetivo de mejorar la seguridad.

Phishing: Técnica de ingeniería social utilizada para obtener información confidencial mediante la suplantación de identidad.

Malware: Software malicioso diseñado para dañar, interrumpir o acceder de manera no autorizada a sistemas informáticos.

Ransomware: Tipo de malware que cifra los datos de una víctima y exige un rescate para devolver el acceso a los datos.

Firewall: Dispositivo de seguridad de red que monitorea y controla el tráfico de red entrante y saliente.

Intrusión: Acceso no autorizado a un sistema informático con la intención de causar daño o robo de información.

Cifrado: Proceso de convertir datos en un código para evitar el acceso no autorizado.

Autenticación: Proceso de verificar la identidad de un usuario o dispositivo antes de permitir el acceso a recursos del sistema.

Gestión de Incidentes: Conjunto de procedimientos y acciones para identificar, analizar y corregir problemas de seguridad en un sistema.

Redes de Telecomunicaciones: Infraestructura de comunicación que permite la transmisión de datos a través de grandes distancias.

Ingeniería Social: Técnica de manipulación psicológica utilizada para influir en las personas para que divulguen información confidencial.

Sistema de Detección de Intrusiones (IDS): Software o hardware diseñado para detectar actividades sospechosas en una red.

Amenazas Internas: Riesgos de seguridad que provienen de dentro de una organización, a menudo de empleados o exempleados.

Política de Seguridad: Conjunto de reglas y prácticas que regulan cómo se protege la información y los recursos en una organización.

Control de Acceso: Medidas implementadas para restringir el acceso a recursos y datos a usuarios autorizados únicamente.

Sistemas de Información: Conjunto de componentes interrelacionados que recolectan, procesan, almacenan y distribuyen información.

Vulnerabilidad: Debilidad en un sistema de información que puede ser explotada por una amenaza para obtener acceso no autorizado.

Pruebas de Penetración (Pen Testing): Simulaciones controladas de ataques cibernéticos para identificar y corregir vulnerabilidades en los sistemas.

Seguridad de la Información: Práctica de proteger la información contra accesos no autorizados, uso indebido, divulgación, interrupción, modificación o destrucción.

Copia de Seguridad (Backup): Proceso de crear una copia de los datos para restaurarlos en caso de pérdida o daño.

Recuperación de Desastres: Estrategias y procedimientos para recuperar sistemas y datos críticos después de un incidente catastrófico.

Autenticación de Dos Factores (2FA): Método de seguridad que requiere dos formas distintas de verificación de identidad antes de conceder acceso.

SOC (Security Operations Center): Centro de Operaciones de Seguridad, que monitorea y responde a incidentes de seguridad en una organización.

SIEM (Security Information and Event Management): Gestión de Información y Eventos de Seguridad, que proporciona análisis en tiempo real de alertas de seguridad generadas por hardware y aplicaciones de red.

BIA (Business Impact Analysis): Análisis de Impacto en el Negocio, proceso de determinar los efectos de una interrupción en las operaciones de negocio.

CORTAFUEGOS: (firewall) es la parte de un sistema o una red informáticos que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. Los cortafuegos. pueden ser implementados en hardware o software, o en una combinación de ambos

Denegación de Servicios (DoS): Tipo de ataque cibernético cuyo objetivo es hacer que un sistema, servicio o red sea inaccesible para los usuarios legítimos. Esto se logra sobrecargando los recursos del sistema objetivo, como el ancho de banda o la capacidad de procesamiento, mediante una gran cantidad de solicitudes falsas.

CIS (Center for Internet Security): Organización sin fines de lucro que se dedica a mejorar la seguridad cibernética de organizaciones y usuarios en todo el mundo. Proporciona un conjunto de controles de seguridad conocidos como los "Controles CIS," que son prácticas recomendadas para la defensa contra ciberamenazas. Estos controles abarcan áreas clave como la gestión de activos, el control de acceso y la defensa contra el malware.

VPN (Virtual Private Network): Tecnología que permite crear una conexión segura y encriptada sobre una red menos segura, como Internet. Las VPNs se utilizan para proteger la

privacidad en línea, ocultar la dirección IP del usuario, y permitir el acceso seguro a redes privadas desde ubicaciones remotas.

Introducción

En la actualidad, la transformación digital ha impulsado a las empresas a depender cada vez más de las tecnologías de la información y las comunicaciones para el desarrollo de sus operaciones. En este contexto, la ciberseguridad se ha convertido en un componente fundamental para garantizar la protección de la información, la continuidad de los servicios y la confianza de los usuarios. Sin embargo, las pequeñas y medianas empresas (pymes), especialmente en el sector telecomunicaciones, enfrentan importantes desafíos para implementar medidas de seguridad adecuadas, debido a limitaciones de recursos, conocimiento técnico y cultura organizacional en torno a la gestión de riesgos digitales.

En Colombia, el panorama de amenazas cibernéticas ha crecido de manera significativa en los últimos años, afectando de forma directa a las pymes, las cuales constituyen una gran parte del tejido empresarial del país. Estas organizaciones suelen ser objetivos frecuentes de ataques como phishing, ransomware y explotación de vulnerabilidades, debido a la falta de controles de seguridad robustos y a la baja capacitación del personal. Esta situación no solo genera pérdidas económicas, sino también impactos negativos en la reputación y continuidad operativa de las empresas.

Frente a esta problemática, surge la necesidad de desarrollar soluciones tecnológicas accesibles que permitan a las empresas identificar vulnerabilidades en sus sistemas, comprender los riesgos asociados y tomar acciones correctivas de manera oportuna. En este sentido, el presente proyecto propone el desarrollo de Microsentinel, una herramienta de ciberseguridad orientada a la detección automatizada de vulnerabilidades en infraestructuras expuestas, haciendo uso de herramientas open-source ampliamente reconocidas en el ámbito del análisis de seguridad.

Microsentinel se caracteriza por integrar en una sola solución múltiples funcionalidades que facilitan su adopción en entornos empresariales con bajo nivel de madurez tecnológica. Entre estas se destacan una interfaz gráfica amigable, la generación de informes automatizados en español con priorización de riesgos, la incorporación de un módulo educativo contextual que permite al usuario comprender y prevenir vulnerabilidades, y la implementación de un protocolo de uso ético que garantiza la ejecución responsable de las pruebas de seguridad.

El desarrollo de esta solución se fundamenta en un enfoque de investigación aplicada, apoyado en principios de la ingeniería de telecomunicaciones, la seguridad en redes y marcos de referencia como el NIST, lo que permite estructurar un sistema orientado a la identificación, análisis y mitigación de riesgos de manera sistemática. De esta forma, el proyecto no solo aporta una herramienta funcional, sino que también contribuye al fortalecimiento de la cultura de ciberseguridad en las empresas.

El presente documento se estructura en varios capítulos. En primer lugar, se presenta el planteamiento del problema y la justificación del proyecto. Posteriormente, se definen los objetivos y el marco teórico que sustenta la investigación. A continuación, se describe la metodología utilizada para el desarrollo de la solución, seguido del diseño e implementación de Microsentinel, los resultados obtenidos y su respectivo análisis. Finalmente, se presentan las conclusiones y recomendaciones derivadas del proyecto.

Descripción del Problema

Las pequeñas y medianas empresas del sector de telecomunicaciones en Colombia enfrentan crecientes riesgos cibernéticos que amenazan la continuidad de sus operaciones y la seguridad de la información que gestionan. Estas empresas, responsables de ofrecer servicios esenciales de conectividad y transmisión de datos, operan en entornos altamente expuestos debido a la naturaleza de sus infraestructuras, lo que incrementa significativamente su superficie de ataque. Sin embargo, en muchos casos, no cuentan con los recursos financieros, tecnológicos ni con personal especializado necesario para implementar y mantener sistemas de ciberseguridad robustos y actualizados.

Esta situación de vulnerabilidad las expone a una amplia variedad de amenazas, entre las que se destacan los accesos no autorizados, ataques de inyección SQL, explotación de vulnerabilidades en gestores de contenido (CMS), escaneo de puertos abiertos y otras técnicas de intrusión utilizadas por actores maliciosos. Estos ataques pueden derivar en pérdidas económicas significativas, interrupciones en la prestación de servicios, afectaciones a la reputación corporativa e incluso sanciones legales derivadas del incumplimiento de normativas relacionadas con la protección de datos y la seguridad de la información.

Adicionalmente, el factor humano juega un papel determinante en la materialización de estos riesgos, ya que la falta de capacitación en ciberseguridad y la ausencia de protocolos claros de gestión incrementan la probabilidad de incidentes. La baja cultura de seguridad dentro de las organizaciones limita la capacidad de prevención y respuesta ante amenazas, manteniendo un enfoque reactivo en lugar de preventivo.

A pesar de la existencia de diversas herramientas especializadas para la detección y mitigación de vulnerabilidades, la mayoría de estas soluciones presentan barreras importantes

para su adopción en pequeñas y medianas empresas. En muchos casos, requieren conocimientos técnicos avanzados para su configuración e interpretación de resultados, o implican costos elevados que resultan difíciles de asumir. Como consecuencia, se genera un vacío en la protección digital del sector, dejando a estas organizaciones expuestas a riesgos que podrían ser identificados y mitigados de manera oportuna con herramientas adecuadas.

Asimismo, cuando se realizan análisis de seguridad, los resultados suelen presentarse en formatos técnicos complejos y en idioma inglés, lo que dificulta su comprensión por parte de usuarios no especializados y limita la toma de decisiones efectivas. La falta de priorización de los riesgos y de orientación práctica para su mitigación reduce el impacto real de estos análisis, impidiendo que las empresas implementen mejoras concretas en su postura de seguridad.

En este contexto, se evidencia la necesidad de desarrollar una solución tecnológica accesible, integrada y fácil de usar que permita a las pequeñas y medianas empresas del sector telecomunicaciones identificar, monitorear y mitigar sus riesgos cibernéticos de manera eficiente. Dicha solución debe no solo automatizar el análisis de vulnerabilidades, sino también presentar los resultados de forma clara, priorizar las acciones de remediación, incorporar componentes formativos que fortalezcan la cultura de ciberseguridad y garantizar el uso ético de las herramientas empleadas.

Por tanto, el desarrollo de una herramienta como Microsentinel responde a la necesidad de mejorar la resiliencia digital de estas empresas, facilitando la identificación temprana de vulnerabilidades, promoviendo la toma de decisiones informadas y contribuyendo a la estabilidad y competitividad del sector en el entorno digital actual.

Objetivos

Objetivo General.

Desarrollar una solución tecnológica denominada Microsentinel para la identificación de vulnerabilidades en infraestructuras expuestas de empresas del sector telecomunicaciones, mediante análisis automatizado que facilite la detección de riesgos y la generación de recomendaciones técnicas.

Objetivos Específicos.

Diseñar la arquitectura funcional de la aplicación Microsentinel, definiendo sus módulos, flujo de operación y estructura general del sistema.

Desarrollar el módulo de análisis automatizado que permita identificar puertos abiertos, servicios expuestos y posibles vulnerabilidades en sistemas accesibles desde la red.

Implementar la generación de informes automatizados en español, organizados según el nivel de riesgo y acompañados de recomendaciones técnicas.

Evaluar el funcionamiento de la herramienta mediante pruebas controladas, verificando la detección de vulnerabilidades y la utilidad de los reportes generados.

Justificación

En un entorno donde las pequeñas y medianas empresas del sector telecomunicaciones enfrentan riesgos cibernéticos crecientes y carecen de soluciones accesibles y adaptadas a su realidad operativa, surge la necesidad de herramientas tecnológicas concretas que fortalezcan su seguridad digital. Estas organizaciones, al operar con infraestructuras expuestas y gestionar información sensible, se convierten en objetivos frecuentes de ataques informáticos, sin contar en muchos casos con los recursos necesarios para implementar medidas de protección adecuadas.

Microsentinel se propone como una plataforma diseñada para suplir esta carencia, combinando en una sola solución el diagnóstico automatizado de vulnerabilidades, la generación de recomendaciones prácticas y la incorporación de un componente formativo en ciberseguridad, todo ello a través de una interfaz gráfica amigable y de fácil uso. Este enfoque integral permite no solo identificar riesgos, sino también facilitar su comprensión y promover acciones concretas para su mitigación, incluso en entornos donde no se dispone de personal altamente especializado.

El desarrollo de este proyecto se justifica en la medida en que contribuye directamente a la protección de los activos digitales de las empresas del sector telecomunicaciones, mediante una solución aplicable, económica y funcional. Al utilizar herramientas open-source y automatizar procesos de análisis, Microsentinel reduce las barreras de acceso a la ciberseguridad, permitiendo que organizaciones con bajo nivel de madurez tecnológica puedan mejorar su postura de seguridad sin incurrir en altos costos.

Adicionalmente, el proyecto incorpora un enfoque orientado a la toma de decisiones, mediante la generación de informes estructurados y priorizados según el nivel de riesgo, lo que facilita la identificación de vulnerabilidades críticas y la implementación de medidas correctivas de manera oportuna. La integración de un módulo educativo contextual refuerza la cultura

organizacional en ciberseguridad, abordando uno de los principales factores de riesgo: el error humano.

Desde una perspectiva social y económica, fortalecer la ciberseguridad de las pequeñas y medianas empresas contribuye a la continuidad de sus operaciones, la protección de la información de sus clientes y la estabilidad del sector telecomunicaciones. Esto, a su vez, impacta positivamente en la confianza digital y en el desarrollo del entorno empresarial.

En el ámbito disciplinar, este proyecto representa la aplicación práctica de los conocimientos adquiridos en ingeniería de telecomunicaciones, especialmente en áreas como seguridad en redes, análisis de vulnerabilidades y gestión de riesgos tecnológicos. Asimismo, se apoya en buenas prácticas y marcos de referencia reconocidos, lo que le otorga validez técnica y académica.

Finalmente, Microsentinel responde a una necesidad real del sector, aportando una solución viable que integra diagnóstico, formación y responsabilidad en el uso de herramientas de ciberseguridad, contribuyendo así al fortalecimiento de la resiliencia digital en las empresas del sector telecomunicaciones.

Marco Teórico

Conceptos Básicos

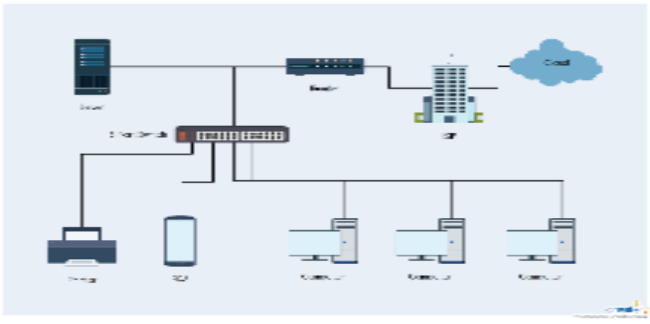
Redes de Telecomunicaciones

Las redes de telecomunicaciones constituyen la infraestructura fundamental que permite la transmisión de datos, voz e imagen entre diferentes sistemas. Estas redes están compuestas por dispositivos como servidores, routers, switches y enlaces de comunicación que garantizan la interconectividad de los servicios digitales.

En el sector telecomunicaciones, estas infraestructuras soportan servicios críticos, por lo que su correcta configuración y seguridad son esenciales para garantizar la continuidad operativa. Sin embargo, una configuración inadecuada puede generar exposición de servicios, puertos abiertos y accesos no controlados.

Desde la perspectiva de Microsentinel, las redes de telecomunicaciones representan el principal objeto de análisis, ya que la herramienta se enfoca en identificar vulnerabilidades asociadas a la exposición de servicios en estas infraestructuras. A través del escaneo de puertos y la detección de tecnologías, es posible evaluar el nivel de seguridad de la red y determinar posibles puntos de entrada para ataques.

Figura 1 *Esquema general de una red de telecomunicaciones*



Nota. La imagen representa la interconexión entre dispositivos, servidores, usuarios y servicios de red que conforman un entorno típico de comunicaciones digitales sobre el cual pueden existir superficies de exposición. Adaptado de Tanenbaum y Wetherall (2021).

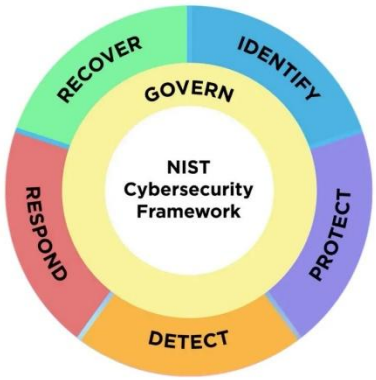
Seguridad Cibernética

La seguridad cibernética se refiere al conjunto de prácticas, tecnologías y procesos diseñados para proteger sistemas, redes y datos frente a accesos no autorizados, ataques o daños. Su objetivo principal es garantizar la confidencialidad, integridad y disponibilidad de la información.

En el contexto de las pequeñas y medianas empresas del sector telecomunicaciones, la ciberseguridad presenta desafíos significativos debido a la limitada implementación de controles de seguridad y a la exposición constante de sus sistemas a internet.

Microsentinel se enmarca dentro de este contexto como una herramienta orientada a la identificación de vulnerabilidades en sistemas expuestos, permitiendo detectar riesgos asociados a configuraciones inseguras, servicios vulnerables y aplicaciones desactualizadas. De esta manera, contribuye al fortalecimiento de la seguridad cibernética mediante el análisis técnico y la generación de información útil para la mitigación de riesgos.

Figura 2 *Funciones del NIST Cybersecurity Framework aplicables a la gestión del riesgo digital.*



Nota. Se observan las funciones de gobernanza, identificación, protección, detección, respuesta y recuperación propuestas por el marco NIST para la administración integral de riesgos de ciberseguridad. National Institute of Standards and Technology (2024).

Principales Amenazas Cibernéticas

Phishing, Vishing y Smishing

En el contexto de Microsentinel, estas amenazas son relevantes porque pueden facilitar accesos indebidos a sistemas que posteriormente son explotados mediante vulnerabilidades técnicas. Por esta razón, la identificación de servicios expuestos y configuraciones inseguras permite reducir el impacto de accesos no autorizados derivados de este tipo de ataques.

Phishing. Ataques que utilizan correos electrónicos fraudulentos para engañar a los usuarios y obtener información confidencial, como contraseñas y números de tarjetas de crédito. Estos correos electrónicos a menudo parecen legítimos y pueden imitar a instituciones de confianza.

Figura 3 *Ejemplo de un ataque de phishing por correo electrónico.*

Nota. La imagen ilustra un escenario de engaño digital donde se replica visualmente una plataforma legítima con el fin de capturar credenciales o información sensible del usuario. Adaptado de OWASP Foundation (2021).

Vishing (Voice Phishing.). Variante del phishing que utiliza llamadas telefónicas para obtener información confidencial. Los atacantes se hacen pasar por entidades legítimas y solicitan datos personales o financieros.

Smishing (SMS Phishing). Similar al phishing, pero utiliza mensajes de texto SMS para engañar a los usuarios y obtener información confidencial.

Web Spoofing El web spoofing es una técnica de ataque que consiste en la creación de sitios web falsos que imitan plataformas legítimas con el objetivo de capturar credenciales o información sensible de los usuarios. Este tipo de ataque suele estar asociado a campañas de phishing y representa un riesgo significativo para empresas que operan servicios web.

Este tipo de amenaza puede verse favorecida por configuraciones inseguras, uso de protocolos no cifrados o vulnerabilidades en aplicaciones web. Microsentinel contribuye a la mitigación de este riesgo mediante la identificación de tecnologías web utilizadas y la detección

de servicios que no implementan mecanismos adecuados de seguridad, como el uso de HTTPS o versiones actualizadas de software.

Accesos no autorizados y ataques automatizados los accesos no autorizados constituyen una de las amenazas más críticas en los sistemas de información, ya que permiten a actores maliciosos ingresar a infraestructuras sin contar con permisos legítimos. Estos accesos pueden lograrse mediante ataques de fuerza bruta, explotación de vulnerabilidades en aplicaciones web o inyecciones SQL.

Los ataques automatizados permiten escanear múltiples sistemas en busca de debilidades, identificando puertos abiertos, servicios vulnerables y configuraciones inseguras. Este tipo de ataques es especialmente efectivo en entornos donde no existen mecanismos de monitoreo o control adecuados.

Microsentinel está diseñado específicamente para identificar este tipo de riesgos, mediante la automatización de herramientas como Nmap, Nikto, WPScan y sqlmap. A través de estos análisis, se detectan puntos de acceso potenciales y vulnerabilidades explotables, permitiendo a las empresas tomar medidas correctivas antes de que estos sean aprovechados por atacantes

Metodologías de Protección

Cifrado de Información

El cifrado de la información es una metodología fundamental en la protección de datos, ya que permite garantizar la confidencialidad de la información durante su transmisión y almacenamiento. Este proceso se basa en el uso de algoritmos criptográficos que transforman los datos en formatos ilegibles para usuarios no autorizados.

En entornos de telecomunicaciones, el uso de protocolos seguros como HTTPS y TLS es esencial para proteger la información que circula por la red. La ausencia de estos mecanismos puede facilitar la interceptación de datos mediante ataques como el “man-in-the-middle”.

Microsentinel permite identificar servicios que no implementan cifrado adecuado, detectando aplicaciones que operan bajo protocolos inseguros. A partir de estos hallazgos, se generan recomendaciones orientadas a la implementación de mecanismos de protección como certificados digitales y comunicaciones seguras.

Configuración de Perímetros Seguros

La configuración de perímetros seguros es una estrategia clave en la protección de redes, ya que permite controlar el acceso a los sistemas mediante el uso de firewalls, listas de control de acceso y segmentación de redes.

El objetivo principal es reducir la superficie de ataque, permitiendo únicamente el tráfico necesario y bloqueando accesos no autorizados. Una mala configuración del perímetro puede dejar expuestos servicios críticos, facilitando ataques automatizados.

Microsentinel se alinea directamente con esta metodología al identificar puertos abiertos y servicios expuestos mediante herramientas de escaneo. Esta información permite a las empresas ajustar sus configuraciones de seguridad, cerrando accesos innecesarios y fortaleciendo el control perimetral.

El marco de referencia del NIST establece un modelo estructurado para la gestión de la ciberseguridad basado en cinco funciones: identificar, proteger, detectar, responder y recuperar.

Microsentinel se integra principalmente en las funciones de identificación y detección, mediante el análisis automatizado de vulnerabilidades en sistemas expuestos. Adicionalmente,

contribuye a la función de protección al generar recomendaciones técnicas orientadas a mitigar los riesgos identificados.

Este enfoque permite alinear la solución con estándares internacionales, fortaleciendo su validez técnica y su aplicabilidad en entornos reales.

Marco Legal y Normativo

El desarrollo e implementación de soluciones tecnológicas orientadas a la ciberseguridad requiere no solo fundamentos técnicos, sino también un respaldo jurídico y normativo que garantice su uso responsable, ético y alineado con la legislación vigente. En el caso de Microsentinel, al tratarse de una herramienta destinada a la identificación automatizada de vulnerabilidades en sistemas accesibles desde la red, resulta indispensable considerar el marco legal aplicable en materia de protección de datos, delitos informáticos, seguridad digital y buenas prácticas internacionales.

En Colombia, la transformación digital y el aumento de incidentes de seguridad han impulsado la consolidación de un conjunto de disposiciones legales que buscan proteger la información, sancionar el acceso no autorizado a sistemas y promover una cultura de gestión segura de los activos digitales. De igual manera, a nivel internacional existen estándares y marcos de referencia que orientan el análisis, tratamiento y mitigación de vulnerabilidades en entornos tecnológicos.

En este sentido, el presente capítulo expone las principales normas y lineamientos que sustentan el desarrollo del proyecto Microsentinel y delimitan el contexto legal dentro del cual debe ser utilizada esta solución tecnológica.

Legislación Colombiana Sobre Protección de Datos Personales

En Colombia, la protección de la información constituye un elemento central dentro del ecosistema digital, especialmente cuando las organizaciones almacenan, procesan o transmiten datos a través de sistemas conectados. La Ley 1581 de 2012 establece el régimen general de

protección de datos personales y reconoce el derecho de todas las personas a conocer, actualizar, rectificar y controlar la información que repose en bases de datos públicas o privadas.

Esta normativa impone a las organizaciones la obligación de adoptar medidas técnicas, humanas y administrativas que permitan evitar el acceso no autorizado, la pérdida o alteración de la información. En consecuencia, cualquier herramienta de ciberseguridad orientada a analizar activos digitales debe considerar que los resultados obtenidos pueden involucrar información sensible sobre configuraciones, servicios y estructuras tecnológicas, razón por la cual su tratamiento debe realizarse bajo principios de confidencialidad y uso restringido.

Dentro del contexto de Microsentinel, esta ley respalda la necesidad de implementar controles de uso responsable y generación segura de reportes, evitando la divulgación inadecuada de información derivada de los análisis realizados.

Delitos Informáticos y Acceso No Autorizado a Sistemas

Uno de los principales referentes legales aplicables al proyecto es la Ley 1273 de 2009, por medio de la cual se incorporó al Código Penal colombiano el bien jurídico de la protección de la información y de los datos, tipificando conductas como el acceso abusivo a un sistema informático, la interceptación de datos, el daño informático y el uso de software malicioso.

Esta disposición resulta especialmente relevante debido a que Microsentinel integra herramientas de análisis de vulnerabilidades que, si bien están orientadas a pruebas de seguridad, pueden generar implicaciones legales cuando son utilizadas sobre objetivos sin autorización previa. Por esta razón, el proyecto contempla la validación de consentimiento antes de ejecutar cualquier escaneo, estableciendo un control funcional que promueve el uso ético de la herramienta y se alinea con la prevención de conductas tipificadas por la legislación nacional.

De esta manera, Microsentinel no se concibe como una herramienta de explotación ofensiva, sino como una solución de diagnóstico preventivo orientada a entornos autorizados y controlados.

Política Nacional de Seguridad Digital y Confianza Tecnológica

El Estado colombiano ha fortalecido en los últimos años su marco de gobernanza en seguridad digital a través del CONPES 3995 de 2020, documento que define la Política Nacional de Confianza y Seguridad Digital, cuyo objetivo es establecer medidas para mejorar la seguridad digital, fortalecer capacidades institucionales y aumentar la confianza en el entorno tecnológico.

Complementariamente, el Decreto 338 de 2022 consolida lineamientos generales para la gobernanza de la seguridad digital, promoviendo modelos de gestión de riesgos, prevención de incidentes y fortalecimiento de capacidades de respuesta.

Estos lineamientos nacionales sustentan la pertinencia de desarrollar herramientas como Microsentinel, ya que responden a la necesidad de que las organizaciones adopten mecanismos preventivos para identificar debilidades de seguridad antes de que se conviertan en incidentes reales. En este sentido, la plataforma se articula con la visión estatal de promover entornos digitales más seguros, resilientes y confiables.

Estándares Internacionales Aplicables a la Gestión de Vulnerabilidades

A nivel internacional, la gestión de riesgos y vulnerabilidades en ciberseguridad se encuentra respaldada por marcos de referencia ampliamente reconocidos. Uno de los más relevantes es el marco de trabajo propuesto por la National Institute of Standards and Technology, el cual plantea cinco funciones esenciales: identificar, proteger, detectar, responder

y recuperar. Dichas funciones permiten estructurar procesos de seguridad orientados a la prevención y tratamiento de incidentes.

Microsentinel se relaciona especialmente con las funciones de identificar y detectar, ya que automatiza el reconocimiento de puertos abiertos, servicios expuestos y posibles fallas de seguridad presentes en sistemas conectados.

De igual manera, la OWASP Foundation establece lineamientos internacionales para la identificación de riesgos comunes en aplicaciones web, destacando vulnerabilidades como configuraciones inseguras, exposición de componentes vulnerables e inyecciones. Estos lineamientos constituyen una referencia fundamental para el análisis automatizado realizado por Microsentinel sobre servicios y aplicaciones accesibles desde internet.

La adopción conceptual de estos estándares internacionales aporta validez técnica al proyecto y garantiza que la solución se encuentre alineada con prácticas reconocidas en el ámbito de la ciberseguridad.

Consideraciones Éticas y Legales en el Uso de Microsentinel

Toda herramienta de análisis de vulnerabilidades implica una responsabilidad ética asociada a su ejecución. La capacidad de identificar servicios, configuraciones y debilidades tecnológicas puede convertirse en un riesgo si no se establecen límites claros de uso y autorización.

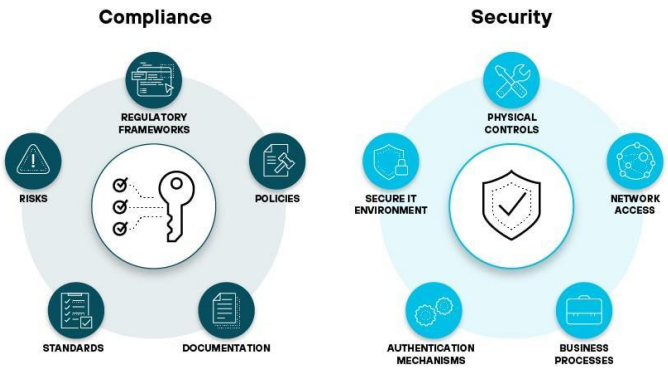
Por esta razón, Microsentinel incorpora un mecanismo de confirmación previa mediante el cual el usuario debe manifestar que cuenta con autorización para realizar el análisis sobre el objetivo definido. Este control no solo constituye una medida funcional dentro del sistema, sino

que representa una salvaguarda frente a posibles usos contrarios a la normativa nacional en materia de acceso abusivo a sistemas informáticos.

Asimismo, los reportes generados están orientados exclusivamente a fines de diagnóstico y mitigación, evitando cualquier enfoque ofensivo o de explotación. Esto permite que la herramienta mantenga coherencia con los principios de hacking ético, auditoría responsable y fortalecimiento preventivo de la seguridad digital.

En consecuencia, el marco legal y normativo analizado no solo avala la pertinencia del proyecto, sino que también delimita las condiciones bajo las cuales Microsentinel debe ser utilizada como una solución tecnológica de apoyo a la gestión segura de vulnerabilidades.

Figura 4 *Relación entre protección de datos, seguridad digital y cumplimiento normativo.*



Nota. La figura muestra la interacción entre los componentes legales y técnicos que intervienen en la gestión responsable de la información y en el uso de herramientas de análisis de seguridad. Adaptado de Congreso de Colombia (2009), Congreso de Colombia (2012) y NIST (2024)

Metodología Del Proyecto

La metodología empleada para el desarrollo del proyecto Microsentinel se estructuró bajo un enfoque de aplicación tecnológica orientado a la construcción progresiva de una solución funcional. Este tipo de metodología permite organizar el proyecto en fases secuenciales de trabajo, donde cada etapa responde a un objetivo específico previamente definido y conduce a la obtención de un resultado verificable dentro del sistema desarrollado.

A diferencia de una investigación exclusivamente descriptiva, el presente proyecto se fundamenta en una metodología de desarrollo aplicada, debido a que no solo analiza una problemática existente en materia de ciberseguridad, sino que propone, construye, implementa y valida una herramienta tecnológica concreta para contribuir a su mitigación.

En este sentido, la metodología se diseñó en cuatro fases principales, alineadas directamente con los cuatro objetivos específicos del proyecto, permitiendo una trazabilidad clara entre la planificación, las actividades ejecutadas y los resultados alcanzados durante el desarrollo de Microsentinel.

Tipo de Metodología

El proyecto Microsentinel se desarrolló bajo una metodología de tipo aplicada con enfoque de desarrollo tecnológico incremental. Se considera aplicada porque parte de una problemática real identificada en pequeñas y medianas empresas del sector telecomunicaciones relacionada con la detección limitada de vulnerabilidades y la ausencia de soluciones accesibles para el análisis preventivo de riesgos digitales.

Asimismo, presenta un enfoque de desarrollo tecnológico debido a que el resultado principal del proyecto es la construcción de una herramienta funcional de software orientada a la automatización de procesos de análisis de seguridad informática.

El carácter incremental de la metodología radica en que la solución fue construida por etapas sucesivas, donde cada fase permitió incorporar nuevos componentes funcionales, validar avances y consolidar progresivamente el sistema final.

Figura 5 *Metodología del Proyecto*

Fases Metodológicas del Desarrollo del Proyecto

Para garantizar el cumplimiento de los objetivos planteados, la metodología se dividió en cuatro fases de trabajo secuenciales, cada una asociada directamente a uno de los objetivos específicos del proyecto. En cada fase se definieron actividades concretas, productos obtenidos y resultados esperados, permitiendo estructurar de manera ordenada el proceso de diseño, construcción y validación de la herramienta Microsentinel.

Fase 1. Diseño de la Arquitectura Funcional

Objetivo asociado: Diseñar la arquitectura funcional de la aplicación Microsentinel, definiendo sus módulos, flujo de operación y estructura general del sistema.

Durante esta fase se realizó la planeación estructural de la herramienta, estableciendo la organización interna del sistema, los componentes principales de la interfaz gráfica, el flujo de interacción del usuario y la secuencia lógica de ejecución de las herramientas de análisis integradas.

Fase 2. Desarrollo del Módulo de Análisis Automatizado

Objetivo asociado: Desarrollar el módulo de análisis automatizado que permita identificar puertos abiertos, servicios expuestos y posibles vulnerabilidades en sistemas accesibles desde la red.

En esta fase se llevó a cabo la integración de herramientas open-source especializadas en análisis de seguridad, tales como Nmap, WhatWeb, Nikto, WPScan y SQLMap, las cuales fueron articuladas mediante scripts de automatización que permiten su ejecución secuencial desde una misma interfaz.

Las actividades desarrolladas comprendieron la configuración de comandos, la parametrización de ejecución, la captura automática de resultados y la sincronización de las salidas generadas por cada herramienta dentro del flujo central del sistema.

El resultado esperado de esta fase fue la construcción del motor de análisis automatizado de Microsentinel, encargado de realizar el reconocimiento técnico del objetivo evaluado y recopilar la información necesaria para el diagnóstico de vulnerabilidades.

Fase 3. Implementación del Sistema de Reportes Automatizados

Objetivo asociado: Implementar la generación de informes automatizados en español, organizados según el nivel de riesgo y acompañados de recomendaciones técnicas.

Durante esta fase se desarrolló el componente encargado de procesar la información obtenida por las herramientas de análisis, organizar los hallazgos detectados y transformarlos en un reporte legible para el usuario final.

Las actividades incluyeron la clasificación de resultados según criticidad, la redacción automatizada de observaciones en español, la incorporación de recomendaciones básicas de mitigación y la exportación de la información a un archivo PDF estructurado.

Como producto de esta fase se obtuvo un sistema de generación de informes automatizados capaz de presentar de manera comprensible los hallazgos del análisis, facilitando la interpretación de vulnerabilidades y la toma de decisiones técnicas.

Fase 4. Evaluación y Validación Funcional

Objetivo asociado: Evaluar el funcionamiento de la herramienta mediante pruebas controladas, verificando la detección de vulnerabilidades y la utilidad de los reportes generados.

En la fase final se realizaron pruebas controladas de funcionamiento con el propósito de validar la estabilidad del sistema, verificar la correcta ejecución del flujo de análisis y evaluar la coherencia de los reportes producidos.

Las actividades ejecutadas contemplaron la realización de escaneos sobre objetivos de prueba, la observación directa del comportamiento del sistema, la verificación de la información detectada y el análisis de la utilidad de los reportes generados frente a los hallazgos encontrados.

Como resultado se obtuvo la validación funcional de Microsentinel, evidenciando que la herramienta cumple con las capacidades definidas en los objetivos y responde adecuadamente al propósito del proyecto.

Técnicas e Instrumentos de Evaluación

Para la validación del proyecto se utilizaron técnicas de observación directa, pruebas funcionales controladas y análisis comparativo de resultados. Estas técnicas permitieron evaluar el comportamiento general del sistema, la estabilidad de la ejecución automatizada y la calidad de la información entregada por la herramienta.

Como instrumentos de evaluación se emplearon registros de ejecución, revisión manual de hallazgos, análisis de coherencia de reportes y comprobación del flujo completo del sistema desde el ingreso del objetivo hasta la generación del informe final.

La aplicación de estos instrumentos permitió verificar que Microsentinel mantiene consistencia operativa, identifica información relevante del objetivo analizado y presenta resultados útiles para el usuario final.

Desarrollo de la Solución

Una vez definida la metodología de trabajo y establecidas las fases de desarrollo del proyecto, se procedió a la construcción técnica de la solución Microsentinel, orientada a automatizar procesos de análisis de vulnerabilidades en sistemas accesibles desde la red.

El presente capítulo describe de manera detallada la estructura funcional de la herramienta, las tecnologías utilizadas, el enfoque de análisis implementado y la integración de los diferentes componentes que permiten el funcionamiento del sistema. Asimismo, se exponen los mecanismos desarrollados para la captura de resultados, generación de reportes y control de uso, consolidando así la materialización práctica de la propuesta tecnológica planteada.

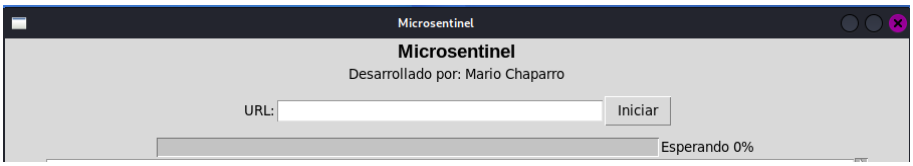
Diseño de la Solución

El diseño de Microsentinel fue concebido como una arquitectura funcional centralizada, en la cual una única interfaz gráfica permite al usuario ejecutar múltiples procesos de análisis de seguridad sin necesidad de interactuar directamente con cada herramienta especializada.

La solución fue estructurada bajo un esquema de entrada–proceso–salida. Como entrada, el sistema recibe el dominio o dirección objetivo suministrado por el usuario. Posteriormente, el módulo de proceso activa de manera secuencial las herramientas integradas de reconocimiento y análisis de vulnerabilidades. Finalmente, como salida, el sistema consolida toda la información recolectada en una consola visual y en un reporte automatizado en formato PDF.

Este diseño permite simplificar la complejidad técnica propia de las pruebas de ciberseguridad, reduciendo la necesidad de ejecutar comandos manuales y facilitando la interpretación de los hallazgos obtenidos.

Figura 6 *Interfaz gráfica principal de la aplicación Microsentinel.*



Nota. En la imagen se observa la ventana inicial del sistema, desde la cual el usuario ingresa el dominio objetivo y activa el proceso automatizado de análisis. Elaboración propia.

Herramientas Utilizadas

Para el funcionamiento de Microsentinel se seleccionaron herramientas open-source ampliamente utilizadas en el ámbito de la ciberseguridad ofensiva y defensiva, debido a su capacidad de reconocimiento técnico, análisis de servicios y detección de vulnerabilidades comunes en entornos web.

La integración de estas herramientas permite que el sistema cubra distintas capas del análisis, desde la identificación de puertos hasta la detección de posibles configuraciones inseguras.

Exploración Pasiva

Dentro de la fase inicial de reconocimiento se emplean técnicas de exploración pasiva, entendidas como aquellas que permiten obtener información básica del objetivo sin realizar interacciones agresivas sobre el sistema analizado.

En Microsentinel, esta etapa se apoya principalmente en WhatWeb, herramienta encargada de identificar tecnologías web, servidores utilizados, frameworks y componentes visibles desde la respuesta HTTP del objetivo.

La exploración pasiva constituye un punto de partida esencial, ya que permite construir un contexto preliminar del entorno evaluado antes de iniciar pruebas más profundas.

Exploración Semi-Pasiva

La exploración semi-pasiva corresponde a un nivel intermedio de interacción, en el cual se ejecutan consultas controladas para identificar puertos abiertos, servicios activos y versiones expuestas sin llegar aún a pruebas de explotación.

Para esta etapa Microsentinel integra Nmap, el cual permite reconocer servicios accesibles, puertos TCP abiertos y versiones detectables de software, proporcionando un mapa técnico del sistema objetivo.

La información recolectada en esta fase resulta fundamental para orientar el análisis posterior y establecer posibles superficies de exposición.

Exploración Activa

En la fase activa del análisis se ejecutan herramientas orientadas a detectar configuraciones inseguras, componentes vulnerables o posibles fallas explotables dentro del sistema objetivo.

Para ello Microsentinel articula Nikto, WPScan y SQLMap. Nikto permite identificar vulnerabilidades conocidas en servidores web, WPScan realiza comprobaciones sobre instalaciones WordPress cuando son detectadas, y SQLMap evalúa la posible existencia de vectores asociados a inyección SQL.

Esta etapa representa el núcleo del análisis de seguridad, debido a que permite pasar del reconocimiento a la identificación de debilidades concretas.

en el sistema.

Enfoque de Análisis Aplicado en Microsentinel

El enfoque de análisis implementado por Microsentinel se basa en un modelo automatizado secuencial, en el cual las herramientas no se ejecutan de manera aislada, sino dentro de una cadena lógica de reconocimiento y diagnóstico.

El proceso inicia con la identificación básica del objetivo, continúa con el reconocimiento de puertos y servicios, avanza hacia la detección de configuraciones vulnerables y finaliza con la consolidación de hallazgos. Esta secuencia permite optimizar tiempos de análisis y garantizar que cada herramienta opere sobre información previamente recolectada.

El valor agregado del sistema no radica únicamente en ejecutar herramientas de forma conjunta, sino en centralizar sus resultados dentro de una misma interfaz y transformar salidas técnicas dispersas en un diagnóstico más comprensible para el usuario.

Implementación de la Solución

La implementación de Microsentinel se desarrolló mediante programación en Python, utilizando bibliotecas orientadas a la construcción de interfaces gráficas, automatización de procesos del sistema operativo y generación de documentos PDF.

La aplicación fue diseñada para ejecutarse en un entorno Linux, particularmente sobre Kali Linux, debido a la compatibilidad nativa con las herramientas de análisis integradas. A través de scripts internos, el sistema invoca cada comando correspondiente, captura sus resultados en tiempo real y los presenta dentro de una consola visual incorporada en la interfaz.

De manera complementaria, se implementaron mecanismos de control de progreso, validación de consentimiento y exportación automática de resultados, consolidando una experiencia de uso centralizada y funcional.

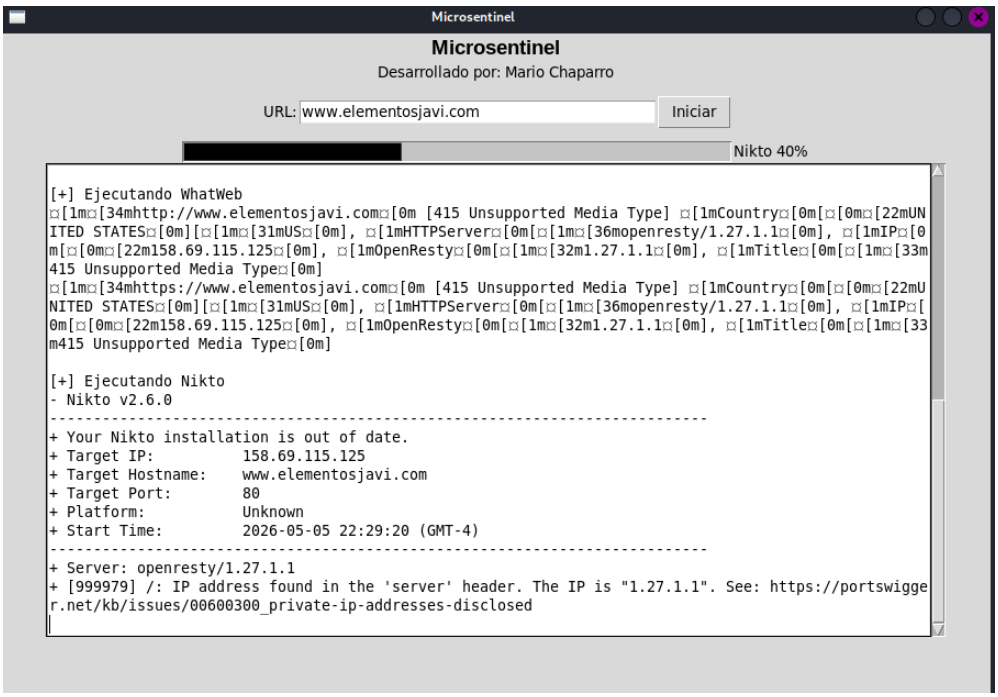
Flujo de Ejecución del Sistema

El flujo operativo de Microsentinel inicia cuando el usuario ingresa el dominio o URL objetivo dentro de la interfaz principal. Posteriormente, el sistema solicita una validación de consentimiento para asegurar que el análisis se realiza sobre un activo autorizado.

Una vez aprobada la ejecución, Microsentinel activa de forma secuencial cada herramienta configurada, mostrando en tiempo real el avance del proceso a través de una barra de progreso y una consola de resultados.

Al finalizar la ejecución, la información recopilada es procesada automáticamente y almacenada para la generación del informe final.

Figura 7 *Ejecución automatizada del análisis de vulnerabilidades en Microsentinel.*



Nota. Se evidencia el avance progresivo del escaneo, la activación secuencial de herramientas integradas y la visualización en tiempo real de resultados técnicos dentro de la consola del sistema. Elaboración propia.

Integración de Herramientas

La integración técnica de herramientas fue realizada mediante el uso de procesos automatizados invocados desde Python, permitiendo ejecutar comandos del sistema operativo y capturar sus salidas estándar.

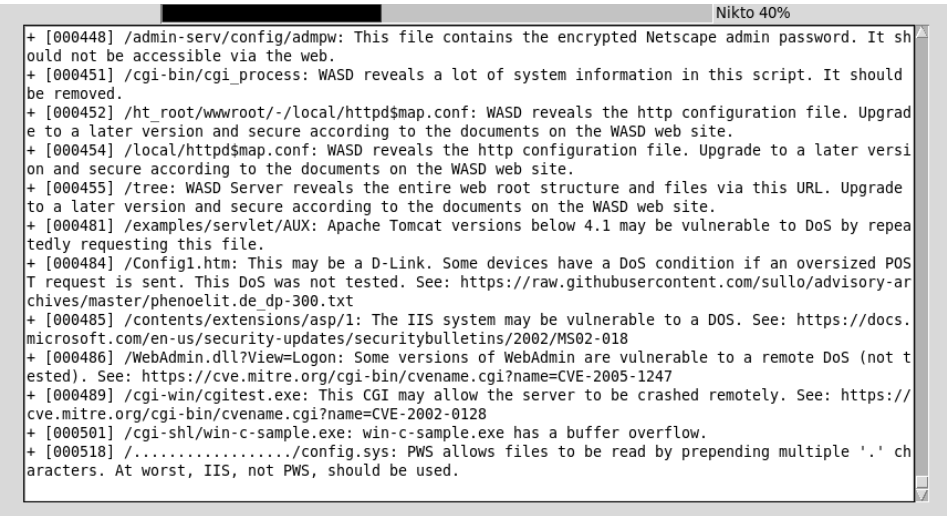
Cada herramienta fue parametrizada según el tipo de análisis requerido, garantizando una ejecución secuencial y controlada. Esta integración evita la necesidad de que el usuario interactúe individualmente con cada software y concentra todo el proceso dentro de un solo entorno de trabajo.

Procesamiento y Organización de Resultados

Una vez obtenidas las salidas de las herramientas, Microsentinel recopila la información generada y la organiza dentro de una variable central de procesamiento. Posteriormente, los hallazgos son estructurados para facilitar su lectura y futura exportación.

Este procesamiento permite unificar información que originalmente es presentada de forma heterogénea por cada herramienta, contribuyendo a la creación de un reporte más homogéneo y comprensible.

Figura 8 *Consola de captura y consolidación de hallazgos técnicos.*



Nota. La figura presenta la información detectada por las herramientas integradas durante el análisis, incluyendo reconocimiento de puertos, servicios expuestos y posibles configuraciones vulnerables. Elaboración propia.

Validación de Uso del Sistema

Como medida de control, la aplicación incorpora una ventana de confirmación previa donde el usuario debe manifestar que cuenta con autorización para realizar el análisis. Esta validación constituye una salvaguarda ética y funcional que limita el uso irresponsable de la herramienta..

Generación de Reportes y Orientación al Usuario

Microsentinel implementa un módulo de generación automática de reportes en formato PDF, en el cual se consolidan los hallazgos obtenidos durante el análisis.

Los reportes incluyen información técnica del objetivo evaluado, descripción de vulnerabilidades detectadas, organización preliminar de hallazgos y recomendaciones orientadas a la mitigación de riesgos. La presentación en idioma español facilita la interpretación de los resultados y amplía la accesibilidad de la herramienta para usuarios no especializados.

Figura 9 *Reporte automatizado generado por Microsentinel.*

REPORTE MICROSENTINEL

Objetivo: www.elementosjavi.com
Fecha: 2026-04-14 00:38:06.728509

Starting Nmap 7.99 (https://nmap.org) at 2026-04-14 00:34 -0400
Stats: 0:01:01 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 92.31% done; ETC: 00:35 (0:00:04 remaining)
Stats: 0:01:11 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 92.31% done; ETC: 00:36 (0:00:05 remaining)
Nmap scan report for www.elementosjavi.com (158.69.115.125)
Host is up (0.048s latency).
rDNS record for 158.69.115.125: ns1.ccomercialmedellin.com
Not shown: 987 filtered tcp ports (no-response)
PORT STATE SERVICE VERSION
21/tcp open ftp Pure-FTPd
22/tcp open ssh OpenSSH 8.0 (protocol 2.0)
25/tcp open smtp?
53/tcp open domain ISC BIND 9.11.36 (RedHat Enterprise Linux 8)
80/tcp open http LiteSpeed
110/tcp open pop3 Dovecot pop3d
143/tcp open imap Dovecot imapd
443/tcp open ssl/https?
465/tcp open ssl/smtp Exim smtpd 4.99.1
587/tcp open smtp Exim smtpd 4.99.1
993/tcp open ssl/imap Dovecot imapd
995/tcp open ssl/pop3 Dovecot pop3d
3306/tcp open mysql MariaDB 5.5.5-10.6.25
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port80-TCP:V=7.99%I=7%D=4/14%Time=69DDC3FF%P=x86_64-pc-linux-gnu%r(GetR
SF:equest,173,"HTTP/1\.0\x20200\x20OK\r\nConnection:\x20close\r\ncontent-t
SF:ype:\x20text/html\r\nlast-modified:\x20Tue,\x2013\x20Jan\x202026\x2017:
SF:15:01\x20GMT\r\naccept-ranges:\x20bytes\r\ncontent-length:\x20163\r\nda
SF:te:\x20Tue,\x2014\x20Apr\x202026\x2004:35:11\x20GMT\r\nserver:\x20LiteS
SF:peed\r\n\r\n<html><head><META\x20HTTP-EQUIV=\"Cache-control\"\x20CONTEN

Nota. Se observa el documento técnico exportado por la herramienta al finalizar el análisis, el cual consolida hallazgos, observaciones y recomendaciones orientativas. Elaboración propia.

Validación de Uso y Control de Acceso

Aunque Microsentinel no implementa un esquema tradicional de autenticación mediante credenciales, sí establece controles básicos de acceso a nivel funcional a través del consentimiento explícito de uso y la ejecución local de la herramienta.

Esto garantiza que los análisis sean realizados en contextos controlados y que la información generada permanezca dentro del entorno del usuario, reduciendo la exposición de resultados sensibles.

Resultados Y Validación

Una vez concluido el proceso de diseño, desarrollo e implementación de la herramienta Microsentinel, se procedió a realizar una serie de pruebas controladas con el propósito de verificar el funcionamiento integral del sistema, la correcta ejecución del módulo automatizado de análisis y la utilidad de los reportes generados.

El presente capítulo expone los resultados obtenidos durante dichas pruebas, analizando el comportamiento de la aplicación frente a diferentes objetivos de análisis, la capacidad de detección de información técnica relevante y la correspondencia entre los resultados alcanzados y los objetivos específicos planteados para el proyecto.

Ejecución de Pruebas

La validación funcional de Microsentinel se realizó mediante pruebas controladas de laboratorio sobre dominios y objetivos accesibles desde red, seleccionados con fines académicos y de comprobación técnica. Estas pruebas permitieron verificar el flujo completo del sistema, desde el ingreso del objetivo por parte del usuario hasta la generación automática del informe final.

Durante cada ejecución se observó el comportamiento de la interfaz gráfica, la respuesta de las herramientas integradas, la actualización de la barra de progreso, la visualización en tiempo real de resultados y la consolidación de la información dentro del reporte PDF.

Las pruebas también permitieron comprobar la correcta interacción entre los distintos módulos internos del sistema, evidenciando estabilidad en la secuencia automatizada de comandos y consistencia en la captura de resultados.

Resultados Obtenidos

Como resultado de las pruebas realizadas, Microsentinel logró identificar información relevante asociada a los objetivos analizados, entre la cual se encontraron puertos abiertos, servicios expuestos, tecnologías web visibles y posibles configuraciones susceptibles de revisión.

La integración de Nmap permitió detectar servicios activos y versiones de software expuestas, mientras que WhatWeb facilitó el reconocimiento de tecnologías de servidor y componentes web. Por su parte, Nikto, WPScan y SQLMap aportaron información complementaria sobre posibles configuraciones inseguras y vectores de vulnerabilidad.

Adicionalmente, el sistema generó de manera satisfactoria reportes automatizados en formato PDF, consolidando toda la información detectada dentro de un documento único, organizado y de fácil interpretación.

Análisis de Resultados

El análisis de los resultados permitió evidenciar que Microsentinel cumple con la finalidad de centralizar múltiples procesos de reconocimiento técnico dentro de una única plataforma de uso simplificado.

Se observó que la automatización reduce significativamente la intervención manual requerida para ejecutar cada herramienta por separado, mejorando la eficiencia del proceso de análisis y disminuyendo la posibilidad de omitir información relevante.

Asimismo, la presentación unificada de resultados en español representa un valor agregado para usuarios con conocimientos técnicos básicos o intermedios, ya que transforma salidas de consola dispersas en una entrega más comprensible y orientada a la toma de decisiones.

En términos funcionales, el sistema mostró coherencia entre la entrada suministrada por el usuario, la ejecución automatizada de comandos y la salida final generada.

Relación Entre Objetivos y Resultados

Con el fin de verificar el cumplimiento del proyecto, se realizó una contrastación entre cada objetivo específico planteado y el resultado evidenciado durante el desarrollo de Microsentinel.

Objetivo Específico 1. Diseñar la Arquitectura Funcional de la Aplicación Microsentinel

Se obtuvo una estructura funcional definida compuesta por interfaz gráfica, módulo de procesamiento, consola de resultados, barra de progreso y sistema de generación documental, permitiendo una interacción centralizada entre usuario y herramienta.

Objetivo Específico 2. Desarrollar el Módulo de Análisis Automatizado

Se integraron satisfactoriamente herramientas de análisis de red y vulnerabilidades dentro de una secuencia automatizada de ejecución, permitiendo detectar puertos abiertos, servicios expuestos y posibles hallazgos técnicos sin intervención manual directa.

Objetivo Específico 3. Implementar la Generación de Informes Automatizados

El sistema logró producir reportes en idioma español en formato PDF, consolidando la información recopilada y proporcionando observaciones y orientación técnica derivada de los hallazgos.

Objetivo Específico 4. Evaluar el Funcionamiento de la Herramienta

Las pruebas controladas demostraron estabilidad operativa, correcta visualización del flujo de análisis y utilidad funcional de los reportes generados como producto final del sistema.

Validación del Sistema

La validación integral de Microsentinel permitió concluir que la herramienta cumple satisfactoriamente con el alcance funcional definido dentro del proyecto. El sistema mostró capacidad para automatizar procesos de análisis, centralizar resultados técnicos y generar informes de salida utilizables dentro de un contexto de diagnóstico preventivo.

Si bien la solución puede continuar fortaleciéndose mediante futuras mejoras de priorización, clasificación avanzada de riesgos o ampliación de herramientas integradas, la versión desarrollada evidencia que es posible construir una plataforma accesible y funcional para apoyar procesos básicos de identificación de vulnerabilidades en entornos de red.

De esta manera, Microsentinel valida su pertinencia como propuesta tecnológica aplicada al fortalecimiento de la ciberseguridad en pequeñas y medianas organizaciones.

Conclusiones

A partir del desarrollo metodológico, técnico y funcional de la herramienta Microsentinel, así como de las pruebas de validación realizadas sobre el sistema, fue posible establecer una serie de conclusiones orientadas a determinar el grado de cumplimiento de los objetivos propuestos, la pertinencia de la solución tecnológica implementada y el aporte generado dentro del campo de la ciberseguridad aplicada. Las conclusiones que se presentan a continuación sintetizan los principales hallazgos del proyecto y permiten evidenciar el valor práctico alcanzado con la construcción de la herramienta.

Cumplimiento del Objetivo General

El objetivo general del proyecto fue cumplido satisfactoriamente, dado que se logró desarrollar una solución tecnológica funcional orientada al análisis automatizado de vulnerabilidades en sistemas accesibles desde la red. Microsentinel demostró capacidad para integrar diferentes procesos de reconocimiento técnico dentro de una única plataforma, permitiendo simplificar tareas de diagnóstico que normalmente requieren la ejecución manual de múltiples herramientas especializadas.

La herramienta construida responde de manera coherente a la problemática identificada inicialmente, relacionada con la necesidad de contar con mecanismos más accesibles para la identificación preventiva de riesgos cibernéticos en entornos tecnológicos.

Generación de Reportes y Orientación al Usuario

La implementación de un módulo de generación de reportes en formato PDF permitió estructurar los resultados del análisis de manera clara y organizada. Asimismo, la inclusión de descripciones y recomendaciones básicas dentro de los reportes aporta un componente de

orientación al usuario, facilitando la comprensión de los hallazgos y promoviendo la adopción de buenas prácticas de seguridad.

Diseño y Consolidación de la Arquitectura Funcional

A través del desarrollo del proyecto se logró estructurar una arquitectura funcional clara para Microsentinel, compuesta por una interfaz gráfica centralizada, un módulo automatizado de ejecución de herramientas, un sistema visual de monitoreo del proceso y un componente de generación documental.

Esta consolidación permitió demostrar que es posible transformar procedimientos técnicos dispersos en una solución unificada y de interacción simplificada, favoreciendo la usabilidad del análisis y reduciendo la dependencia de comandos especializados por parte del usuario.

Desarrollo del Módulo de Análisis Automatizado

La integración de herramientas como Nmap, WhatWeb, Nikto, WPScan y SQLMap dentro de un mismo flujo secuencial permitió construir un motor automatizado capaz de identificar puertos abiertos, servicios expuestos y posibles vulnerabilidades de configuración presentes en objetivos accesibles desde la red.

Este resultado confirma que la automatización de procesos de ciberseguridad representa una alternativa eficiente para centralizar tareas de reconocimiento técnico, mejorar tiempos de análisis y optimizar la recolección de información relevante para la detección temprana de riesgos.

Generación de Reportes Técnicos Automatizados

El proyecto permitió concluir que el desarrollo de herramientas de análisis de vulnerabilidades debe encontrarse necesariamente acompañado por consideraciones éticas y legales que delimiten su utilización sobre activos autorizados.

En este sentido, Microsentinel no solo incorpora componentes técnicos de diagnóstico, sino que también establece controles básicos de consentimiento y promueve una visión preventiva del análisis, orientada al fortalecimiento de la seguridad digital y no a la explotación ofensiva de sistemas.

Esto incrementa la pertinencia del proyecto dentro del contexto actual de transformación tecnológica y necesidad de protección de infraestructuras digitales.

Aporte Disciplinar y Proyección Tecnológica

Desde la perspectiva de la ingeniería en telecomunicaciones, el desarrollo de Microsentinel representa una aplicación práctica de conocimientos asociados a redes, servicios, automatización, seguridad informática y gestión de información.

Adicionalmente, el proyecto deja una base tecnológica susceptible de evolución futura, sobre la cual pueden incorporarse nuevos mecanismos de priorización de vulnerabilidades, monitoreo continuo, inteligencia artificial o ampliación de módulos de análisis, consolidando así una línea de trabajo con proyección de crecimiento y aplicabilidad en escenarios reales.

Recomendaciones

A partir de los resultados obtenidos durante el desarrollo y validación de Microsentinel, se identificaron una serie de oportunidades de mejora orientadas a fortalecer el alcance funcional de la herramienta, ampliar sus capacidades de análisis y optimizar su aplicabilidad en escenarios reales. Las siguientes recomendaciones se plantean como líneas de evolución tecnológica y técnica que permitirían consolidar una versión más robusta del sistema en futuras etapas de desarrollo.

Mejora en la Priorización de Vulnerabilidades

Se recomienda incorporar un mecanismo interno de clasificación avanzada de hallazgos que permita asignar niveles de criticidad de forma más precisa según el tipo de vulnerabilidad detectada, el servicio comprometido y el posible impacto asociado.

Esto permitiría que los reportes no solo presenten resultados descriptivos, sino que establezcan una jerarquización más útil para la toma de decisiones inmediatas.

Evolución de la Interfaz y Experiencia de Usuario

Aunque la interfaz gráfica desarrollada cumple adecuadamente con su función operativa, resulta conveniente proyectar una versión visualmente más robusta e intuitiva, incorporando elementos como paneles organizados, iconografía especializada, historial de análisis ejecutados y visualización resumida de riesgos.

Una interfaz más desarrollada incrementaría la accesibilidad y mejoraría la interacción del usuario con el sistema.

Fortalecimiento de los Mecanismos de Seguridad

Se recomienda integrar mecanismos complementarios de protección interna, tales como autenticación local de usuarios, cifrado de reportes generados y control de almacenamiento seguro de resultados, con el fin de reforzar la confidencialidad de la información analizada.

Estas mejoras permitirían que Microsentinel no solo analice seguridad, sino que también fortalezca la protección de los datos derivados del propio proceso de diagnóstico.

Ampliación de las Capacidades de Análisis

La versión actual integra herramientas orientadas principalmente a reconocimiento de red y vulnerabilidades web básicas; sin embargo, futuras versiones podrían incluir análisis adicionales de certificados SSL, revisión de cabeceras HTTP, detección de configuraciones DNS inseguras y comprobación de reputación de dominios.

Esto ampliaría la cobertura diagnóstica y ofrecería una visión más completa del estado de seguridad del objetivo evaluado

Implementación de Monitoreo Continuo

Como línea de evolución, se recomienda migrar Microsentinel desde un modelo de análisis bajo demanda hacia un esquema de monitoreo programado, donde el sistema pueda ejecutar revisiones periódicas sobre objetivos previamente definidos y generar alertas automáticas ante cambios detectados.

Esta funcionalidad convertiría la herramienta en un mecanismo más proactivo dentro de la gestión continua de riesgos.

.

Integración de Tecnologías Emergentes

En futuras etapas podría contemplarse la incorporación de algoritmos de inteligencia artificial o análisis heurístico para interpretar hallazgos, detectar patrones repetitivos y priorizar vulnerabilidades con base en comportamiento histórico.

La integración de tecnologías emergentes permitiría evolucionar la herramienta desde un sistema automatizado hacia una plataforma con mayores capacidades de asistencia inteligente.

Aplicabilidad en Entornos Reales

Finalmente, se recomienda realizar pruebas de implementación en entornos empresariales reales del sector telecomunicaciones, con el propósito de medir el comportamiento de Microsentinel frente a infraestructuras más complejas y validar su utilidad dentro de procesos de auditoría preventiva o gestión interna de seguridad.

Esta validación en escenarios reales permitiría consolidar el tránsito del proyecto académico hacia una solución con mayor proyección operativa.

Referencias Bibliográficas

Anderson, R. (2020). *Security engineering: A guide to building dependable distributed systems* (3rd ed.). Wiley.

Bejtlich, R. (2013). *The practice of network security monitoring: Understanding incident detection and response*. No Starch Press.

Congreso de Colombia. (2009). *Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado de la protección de la información y de los datos y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones*.

Congreso de Colombia. (2012). *Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales*.

Departamento Nacional de Planeación. (2020). *Documento CONPES 3995. Política nacional de confianza y seguridad digital*.

Goodrich, M. T., & Tamassia, R. (2014). *Introduction to computer security*. Pearson.

Gupta, B. B., Agrawal, D. P., & Yamaguchi, S. (2016). *Handbook of research on modern cryptographic solutions for computer and cyber security*. IGI Global.

Hubbard, D. W. (2014). *How to measure anything: Finding the value of intangibles in business* (3rd ed.). Wiley.

Katz, J., & Lindell, Y. (2020). *Introduction to modern cryptography* (3rd ed.). CRC Press.

Kim, D., & Solomon, M. G. (2016). *Fundamentals of information systems security* (3rd ed.). Jones & Bartlett Learning.

Li, J. (2020). Vulnerabilities mapping based on OWASP-SANS: A survey for static application security testing. *arXiv Preprint*.

Long, J., & Skoudis, E. (2011). *Google hacking for penetration testers* (3rd ed.). Syngress.

Mitnick, K. D., & Simon, W. L. (2017). *The art of invisibility: The world's most famous hacker teaches you how to be safe in the age of big brother and big data*. Little, Brown and Company.

Modesti, P. (2024). Bridging the gap: A survey and classification of research-informed security tools. *Cybersecurity, 4*(3), 1–18.

National Institute of Standards and Technology. (2018). *Framework for improving critical infrastructure cybersecurity, Version 1.1*. U.S. Department of Commerce.

National Institute of Standards and Technology. (2024). *Cybersecurity framework 2.0*. U.S. Department of Commerce.

Nmap Project. (2024). *Nmap reference guide*. Nmap Security Scanner.

Nikto Project. (2024). *Nikto web server scanner documentation*. CIRT.net.

OWASP Foundation. (2021). *OWASP top 10: The ten most critical web application security risks*.

Pfleeger, C. P., & Pfleeger, S. L. (2015). *Security in computing* (5th ed.). Prentice Hall.

Presidencia de la República de Colombia. (2022). *Decreto 338 de 2022 por el cual se establecen lineamientos generales para fortalecer la gobernanza de la seguridad digital*.

Provost, F., & Fawcett, T. (2013). *Data science for business: What you need to know about data mining and data-analytic thinking*. O'Reilly Media.

Singer, P. W., & Friedman, A. (2014). *Cybersecurity and cyberwar: What everyone needs to know*. Oxford University Press.

Skoudis, E., & Liston, T. (2006). *Counter hack reloaded: A step-by-step guide to computer attacks and effective defenses* (2nd ed.). Prentice Hall.

Stallings, W. (2017). *Network security essentials: Applications and standards* (6th ed.). Pearson.

Swetha, B., Susmitha, N. R. K., Thirulogaveni, J., & Sruthi, S. (2024). A comparative analysis of vulnerability management tools: Evaluating Nessus, Acunetix, and Nikto for risk based security solutions. *arXiv Preprint*.

sqlmap Project. (2024). *sqlmap user manual*. sqlmap.org.

Tanenbaum, A. S., & Wetherall, D. J. (2021). *Computer networks* (6th ed.). Pearson.

The Inter-American Development Bank. (2020). *2020 cybersecurity report: Risks, progress, and the way forward in Latin America and the Caribbean*.

WhatWeb Project. (2024). *WhatWeb documentation*. WhatWeb.

Whitman, M. E., & Mattord, H. J. (2021). *Principles of information security* (7th ed.). Cengage Learning.

WPScan Team. (2024). *WPScan user documentation*. WPScan.

Batarseh, F. A. (2022). Cybersecurity law: Legal jurisdiction and authority. *arXiv Preprint*.

Lokare, A., Bankar, S., & Mhaske, P. (2025). Integrating cybersecurity frameworks into IT security: A comprehensive analysis of threat mitigation strategies and adaptive technologies. *arXiv Preprint*.

McGuan, C., Raghavan, A. V., Mandapati, K. M., Yu, C., Ray, B. E., & Jackson, D. K. (2025). Bridging cybersecurity practice and law: A hands-on, scenario-based curriculum using the NICE framework to foster skill development. *arXiv Preprint*.

Gernhardt, D., & Groš, S. (2021). Use of non-peer reviewed sources in cyber-security scientific research. *arXiv Preprint*.

Calder, A. (2018). *NIST cybersecurity framework: A pocket guide*. IT Governance Publishing.

Talabis, M., & Martin, J. (2013). *Information security risk assessment toolkit*. Syngress.

Kosseff, J. (2017). *Cyber security law*. Wiley.