SAPIENS IN ARTIFICIAL INTELLIGENCE
Vol.2 No.2 (2025): Journal Scientific ISSN: 3073-1402
https://sapiensjournal.ec/index.php/sai/index

ID del documento: SAI-Vol.2.N.2.001.2025

Tipo de artículo: Investigación

Sandbox virtual con herramientas open source para pentesting: Una propuesta tecnológica aplicada a la seguridad cibernética de las pymes

Analysis of the foundations, ethics and social impact of AI in a general elementary school

Autores:
Hernando Alexander Cachaya Moreno[1], Hildebrando Castañeda Rincón[2], Luis Edilson Torres Roncancio[3], Johemir Jesús Pérez Pertuz[4]

[1]Escuela de Tecnologías de la Información y las Comunicaciones (ESTIC), Bogotá, Colombia, gerencias348@hotmail.com, https://orcid.org/0009-0005-2935-9417

[2]Escuela de Tecnologías de la Información y las Comunicaciones (ESTIC), Bogotá, Colombia, hildebrando.castaneda1024@correo.policia.gov.co, https://orcid.org/0000-0001-7557-076X

[3]Escuela de Tecnologías de la Información y las Comunicaciones (ESTIC), Bogotá, Colombia, edils.torres@correo.policia.gov.co, https://orcid.org/0009-0007-3973-895X

[4]Escuela de Tecnologías de la Información y las Comunicaciones (ESTIC), Bogotá, Colombia, ppjohemir@gmail.com, https://orcid.org/0000-0002-5094-0530

Corresponding Author: *Hernando Alexander Cachaya Moreno*, nataly.sanchez@unl.edu.ec

Reception: 10-February-2025 **Acceptance:** 18-March-2025 **Publication:** 24-April-2025

Cachaya Moreno, H. A., Castañeda Rincón, H., Torres Roncancio, L. E., & Pérez Pertuz, J. J. (2025). Sandbox virtual con herramientas open source para pentesting: Una propuesta tecnológica aplicada a la seguridad cibernética de las pymes. Sapiens in Artificial Intelligence, 2(2), e-22001. https://doi.org/10.71068/tgqmvg81

Resumen

El artículo presentó los resultados de una investigación tecnológica aplicada al diseño, implementación y evaluación de una arquitectura de sandbox virtual con herramientas de pentesting, enfocada en identificar vulnerabilidades en aplicaciones móviles y sitios web de pequeñas y medianas empresas (PYMEs). Ante el aumento de ciberataques y la limitada capacidad de estas organizaciones para adoptar soluciones de seguridad avanzadas, se desarrolló un entorno controlado que integró herramientas open source como REMnux, OpenVAS, OWASP ZAP y MobSF. El estudio adoptó un enfoque cualitativo descriptivo y exploratorio, complementado con técnicas cuantitativas mediante encuestas estructuradas a 17 empresas y entrevistas a expertos. La metodología se dividió en tres fases: selección y evaluación de herramientas, pruebas de concepto en entornos virtuales y elaboración de una guía operativa. Los resultados demostraron que el entorno sandbox fue efectivo en la detección de malware y vulnerabilidades, permitiendo el análisis estático y dinámico de amenazas y fortaleciendo la resiliencia digital de las PYMEs. Se identificaron beneficios como la reducción de riesgos, mayor conciencia sobre seguridad informática y la aplicación de soluciones viables sin grandes inversiones. Se concluyó que la propuesta tecnológica fue funcional, replicable y adaptable, representando una alternativa eficaz para mejorar la seguridad cibernética en empresas con recursos limitados. Finalmente, se establecieron recomendaciones técnicas y líneas de investigación futuras en detección automatizada y seguridad en entornos IoT y cloud.

Palabras clave: Sandbox virtual, prueba de pentesting, ciberseguridad, análisis de malware, PYMEs.

Abstract

The article presented the results of an applied technological research focused on the design, implementation, and evaluation of a virtual sandbox architecture with pentesting tools, aimed at identifying vulnerabilities in mobile applications and websites of small and medium-sized enterprises (SMEs). Given the increasing risk of cyberattacks and the limited capacity of these organizations to adopt advanced security solutions, a controlled testing environment was developed, integrating open-source tools such as REMnux, OpenVAS, OWASP ZAP, and MobSF. The study adopted a qualitative descriptive and exploratory approach, complemented by quantitative techniques through structured surveys conducted with 17 companies and semi-structured interviews with experts. The methodology was divided into three phases: selection and evaluation of tools, proof-of-concept testing in virtual environments, and development of an operational guide. The results demonstrated that the sandbox environment was effective in detecting malware and vulnerabilities, allowing for both static and dynamic threat analysis and strengthening the digital resilience of SMEs. Key benefits identified included risk reduction, increased awareness of cybersecurity, and the implementation of viable and scalable solutions without requiring significant investments. It was concluded that the proposed technology was functional, replicable, and adaptable, representing an effective alternative to enhancing cybersecurity in resource-constrained business contexts. Finally, technical recommendations and future research directions were established, focusing on automated threat detection and security in IoT and cloud environments.

Keywords: Virtual sandbox, pentesting, cybersecurity, malware analysis, SMEs.

1. INTRODUCCIÓN

En la actualidad frente a la transformación digital acelerada, las pequeñas y medianas empresas (PYMEs) enfrentan crecientes desafíos en materia de ciberseguridad. La expansión de servicios en línea, el uso masivo de aplicaciones móviles y el almacenamiento de datos sensibles en entornos digitales han incrementado la exposición a amenazas cibernéticas, muchas de las cuales pueden comprometer seriamente la estabilidad operativa, la confianza del cliente y la sostenibilidad del negocio. Tal como plantean Ospina y Sanabria (2020), a medida que las tecnologías digitales se consolidan como pilares fundamentales de la competitividad empresarial, garantizar la protección de los sistemas de información deja de ser una opción para convertirse en una necesidad prioritaria.

Así pues, la falta de implementación de mecanismos proactivos de defensa, como las pruebas de penetración (pentesting), representa una brecha crítica en las estrategias de seguridad de muchas PYMEs. De esta forma, el pentesting permite identificar vulnerabilidades en sitios web y aplicaciones móviles antes de que sean explotadas por agentes maliciosos, facilitando así la corrección temprana de fallos y fortaleciendo la resiliencia digital de las organizaciones. La mencionada práctica, además de contribuir al cumplimiento de normativas de seguridad cada vez más rigurosas, refuerza la confianza del cliente y demuestra un compromiso real con la protección de la información.

Del mismo modo, siguiendo los planteamientos de Díaz et al. (2023) es importante señalar que la adopción de herramientas especializadas de ciberseguridad aún presenta barreras para muchas empresas de menor escala, entre ellas los altos costos de licenciamiento, la complejidad técnica de las plataformas comerciales y la escasa formación del talento humano. En el mencionado contexto, surge la necesidad de desarrollar soluciones asequibles, funcionales y adaptadas a las capacidades operativas de las PYMEs. Una de estas soluciones es el uso de entornos de prueba seguros, como los sandbox virtuales, los cuales permiten ejecutar pruebas de seguridad de manera controlada, sin poner en riesgo los sistemas reales.

De esta forma, el sandboxing representa una estrategia de probada eficacia para evaluar el comportamiento de aplicaciones en ejecución y detectar vulnerabilidades potenciales, al tiempo que aísla los procesos del entorno de producción. Es por esto, que al integrar herramientas de pentesting dentro de estos entornos se ofrece a las empresas la posibilidad de realizar auditorías técnicas en tiempo real, con bajo impacto operativo y sin requerir infraestructuras complejas. Como lo señalan Fernández y Martínez (2018), es fundamental comprender las debilidades del sistema para anticipar fallos de seguridad y establecer un entorno digital confiable tanto para aplicaciones móviles como para sitios web.

Asimismo, en el ámbito de la seguridad informática, se reconoce ampliamente que la protección debe fundamentarse en tres pilares esenciales: la confidencialidad, la integridad y la disponibilidad de la información (Vanegas, 2019). Estos principios orientan por una parte el diseño de arquitecturas de seguridad y del mismo modo contribuyen a la selección de herramientas y a la definición de políticas que garanticen una defensa robusta ante las amenazas emergentes.

En este sentido, el presente artículo presenta el diseño de una arquitectura de sandbox virtual equipada con herramientas de pentesting, orientada específicamente a su implementación en pequeñas y medianas empresas. Esta propuesta tiene como finalidad dotar a las PYMEs de una plataforma funcional para identificar y corregir vulnerabilidades en sus entornos digitales, sin necesidad de recurrir a soluciones costosas o altamente especializadas. Asimismo, se pretende demostrar que la aplicación de este modelo contribuye a una mejora significativa en la gestión de riesgos cibernéticos, fortaleciendo la capacidad de las empresas para operar en un entorno cada vez más digitalizado y competitivo.

Desde una perspectiva investigativa, se parte de la formulación de un problema vigente en el campo de la ciberseguridad para las PYMEs, a partir del cual se plantea un marco técnico-metodológico orientado a la construcción de un entorno seguro, flexible y replicable. En consecuencia, el diseño e implementación del sandbox virtual con herramientas de pentesting por una parte representa una solución tecnológica concreta, del mismo modo se constituye como una estrategia de fortalecimiento institucional frente a los retos de la era digital.

La creciente digitalización de los procesos empresariales ha traído consigo una expansión en las superficies de ataque que pueden ser explotadas por actores maliciosos. Este fenómeno ha intensificado la necesidad de que las organizaciones, en especial las pequeñas y medianas empresas (PYMEs), adopten estrategias de ciberseguridad eficaces y adaptables a sus limitaciones técnicas y presupuestales. Uno de los enfoques más relevantes en este contexto es la realización de pruebas de penetración (pentesting), las cuales permiten simular ataques controlados con el fin de identificar vulnerabilidades antes de que sean aprovechadas con fines maliciosos.

Sandbox (Entorno de Pruebas Aislado)

Un sandbox puede definirse como un entorno virtual controlado y aislado del sistema operativo principal, diseñado para ejecutar, observar y analizar el comportamiento de aplicaciones, archivos o código sin que ello represente un riesgo para el sistema anfitrión. Su propósito principal es permitir la ejecución segura de procesos potencialmente maliciosos o no confiables, facilitando la detección de vulnerabilidades, análisis forense y pruebas de seguridad como el pentesting, sin afectar la integridad del entorno de producción. En ciberseguridad, los sandboxes son fundamentales para el análisis dinámico, ya que permiten

simular condiciones reales de ejecución mientras se monitorean los efectos del código en evaluación (Wright et al., 2006).

El paradigma BYOD en Entornos Empresariales

Uno de los factores que ha ampliado las posibilidades de ataque en los sistemas corporativos es la política de "Traiga Su Propio Dispositivo" (BYOD, por sus siglas en inglés). Esta práctica permite a los empleados utilizar sus dispositivos personales (como smartphones y portátiles) para acceder a redes corporativas y ejecutar funciones laborales. Si bien esta estrategia mejora la movilidad y la productividad, también introduce nuevos vectores de riesgo si no se acompaña de protocolos de seguridad adecuados (Smith y Forman, 2014). En este sentido, la presencia de múltiples dispositivos no gestionados debilita el perímetro de seguridad tradicional y exige mecanismos de defensa más dinámicos.

Pentesting: Definición y Relevancia

El pentesting, o prueba de penetración, es una metodología de evaluación de seguridad informática que simula ataques reales para identificar vulnerabilidades en sistemas, aplicaciones o redes. Esta práctica tiene como propósito detectar fallos antes de que puedan ser explotados por ciberatacantes, aportando información clave para fortalecer la infraestructura tecnológica de la organización (Weidman, 2014). A diferencia de otros métodos de evaluación pasiva, el pentesting adopta un enfoque ofensivo, lo cual lo convierte en una herramienta preventiva altamente eficaz.

Metodología del Pentesting

El proceso de pentesting se estructura en diversas fases que incluyen reconocimiento, análisis de vulnerabilidades, explotación, y generación de reportes. Este enfoque ordenado permite sistematizar la identificación de errores y evaluar el impacto potencial de cada vulnerabilidad en la organización (Rueda, 2017). El origen de las pruebas puede ser interno, cuando se ejecutan desde dentro de la red organizacional, o externo, cuando se realizan desde fuera, como en el caso de un sitio web o una tienda virtual (Gaitán, 2019).

En función del nivel de conocimiento que se tiene del sistema a evaluar, se distinguen tres tipos de pruebas: caja negra, donde no se tiene información previa sobre el sistema; caja gris, que ofrece un conocimiento parcial; y caja blanca, que proporciona un acceso total al funcionamiento interno de la infraestructura. Estos enfoques permiten simular distintos escenarios de ataque y adaptar la profundidad del análisis a los objetivos de seguridad de la empresa. Como lo sostienen Ovallos et al. (2020), estas pruebas también permiten verificar la capacidad de reacción de los responsables de seguridad ante posibles intrusiones.

Tipos de Pentesting Aplicables a PYMEs

La elección del tipo de prueba depende del contexto y de los objetivos específicos del análisis. En este estudio, se prioriza el enfoque de caja blanca, ya que permite evaluar en profundidad el código fuente y la lógica interna de aplicaciones móviles y sitios web, facilitando así la identificación precisa de fallos estructurales y su posterior corrección. Además, se recurre a registros de vulnerabilidades como el Common Vulnerabilities and Exposures (CVE), los cuales catalogan amenazas conocidas y permiten comparar los hallazgos con estándares internacionales (CVE-Mitre, 2025).

Metodologías de Pentesting Reconocidas

Según plantea Gordón y Pacheco (2018), diversas organizaciones han desarrollado metodologías formales para guiar la ejecución de pruebas de penetración bajo estándares de calidad. Entre las más relevantes se encuentra:

- OSSTMM (Open-Source Security Testing Methodology Manual): Evalúa la seguridad de sistemas mediante "dimensiones de seguridad" como autenticación, confidencialidad, integridad y visibilidad.

- ISSAF (Information Systems Security Assessment Framework): Organiza los procesos de evaluación en dominios y criterios de prueba, estructurando así auditorías más completas.

- OWASP (Open Web Application Security Project): Promueve la identificación y mitigación de vulnerabilidades específicas en aplicaciones web, como inyecciones SQL, fallos en autenticación, y configuraciones inseguras.

Adicionalmente, herramientas como Zed Attack Proxy (ZAP), desarrollada por OWASP, permiten realizar análisis dinámicos y estáticos sobre aplicaciones web. Su código abierto, interfaz amigable y capacidad de interceptación del tráfico HTTP/HTTPS la convierten en una herramienta ampliamente adoptada para escaneos automatizados y generación de reportes detallados.

Herramientas de Pentesting Móvil

Con el auge de las aplicaciones móviles como canal principal de interacción digital, el análisis de seguridad sobre estas plataformas se ha vuelto crucial. Las herramientas de pentesting para móviles se dividen en dos categorías: análisis estático, enfocado en el examen del código fuente sin ejecutar la aplicación, y análisis dinámico, basado en la ejecución del software en un entorno controlado para observar su comportamiento (Fortra, 2025).

Entre las herramientas más destacadas para sistemas Android e iOS se encuentran:

- Drozer: Permite análisis completo sobre dispositivos Android, incluyendo exploración de servicios y evaluación forense.

- JAADAS y DroidBox: Se centran en la detección de vulnerabilidades mediante simulación dinámica y trazado de datos.

- Introspy-iOS e iDB: Orientadas al análisis de aplicaciones en iOS, facilitando la inspección de interacciones con el sistema operativo.

- Hooker y Jsunpack-n: Especializadas en desempaquetado de código y análisis de ejecución de scripts.

- Magento-Malware-scanner: Enfocada en la detección de amenazas en sitios desarrollados con Magento (Fortra, 2023).

El uso combinado de estas herramientas en un entorno sandbox permite realizar auditorías profundas de seguridad en aplicaciones móviles, garantizando un entorno seguro y replicable para pruebas sin poner en riesgo los sistemas reales.

3. METODOLOGÍA

La presente investigación adopta un enfoque cualitativo, centrado en la interpretación contextual y técnica del fenómeno objeto de estudio: la necesidad de diseñar una arquitectura de sandbox virtual con herramientas de pentesting para identificar vulnerabilidades en aplicaciones móviles y sitios web, orientada a pequeñas y medianas empresas (PYMEs). De acuerdo con Hernández et al. (2014), el enfoque cualitativo permite analizar en profundidad documentos, registros y anotaciones mediante una aproximación interpretativa del fenómeno. Esta investigación tecnológica aplicada sigue una lógica de diseño sistemático, abordando de forma estructurada las etapas del análisis, desarrollo y validación de la solución tecnológica.

El estudio se sitúa en un nivel descriptivo y exploratorio, ya que no solo busca comprender las necesidades de seguridad digital en las PYMEs, sino también proponer una solución tecnológica adaptada a sus características y contextos. El método se basa en fases periódicas de análisis y pruebas piloto, orientadas a construir una arquitectura funcional, eficiente y replicable para el análisis de vulnerabilidades y malware.

Unidades de análisis

La población objeto del estudio está conformada por dos unidades de análisis principales: Se seleccionaron en primera instancia pequeñas y medianas empresas (PYMEs) en Colombia, definidas por contar con un rango de entre 10 y 250 empleados y desarrollar actividades económicas en diversos sectores. Estas organizaciones constituyen un sector estratégico de la economía nacional y presentan una creciente preocupación por la seguridad digital. A través de un proceso de muestreo intencional, se seleccionaron 16 PYMEs dispuestas a

participar activamente en la prueba e implementación del entorno sandbox, cumpliendo los siguientes criterios: Tener aplicaciones móviles sitios web o infraestructuras de información susceptibles a amenazas; carecer de soluciones avanzadas de pentesting; estar dispuestas a participar en pruebas piloto y brindar retroalimentación técnica.

Por otra parte, se seleccionaron profesionales en ingeniería de sistemas, especializados en ciberseguridad, con al menos un año de experiencia en evaluación de vulnerabilidades y manejo de herramientas de código abierto. Se seleccionaron 5 ingenieros, cuyos perfiles se alinean con roles como analistas de seguridad, consultores e investigadores. Este proceso se realizó entre enero y marzo de 2024, y se garantizó el consentimiento informado de las empresas participantes, así como la confidencialidad de la información proporcionada, siguiendo principios éticos de investigación tecnológica.

Técnicas e instrumentos de recolección de información

La investigación utilizó una combinación de entrevista semiestructurada y encuesta estructurada como técnicas principales para la recolección de datos.

La entrevista semiestructurada permitió establecer un diálogo técnico y contextualizado con los profesionales expertos, facilitando una comprensión profunda sobre el uso y evaluación de herramientas de pentesting. Según plantea Arias (2012), esta técnica facilita una interacción directa y flexible entre entrevistador y entrevistado, permitiendo abordar temas predefinidos y emergentes.

La encuesta estructurada fue aplicada a las 16 PYMEs participantes, abordando variables como: Nivel de conocimiento previo sobre ciberseguridad, herramientas de pentesting utilizadas actualmente, percepciones sobre la necesidad de fortalecer su infraestructura digital, interés en adoptar soluciones como REMnux, VirtualBox y otras herramientas de sandboxing, preocupaciones relacionadas con costos, operatividad y capacitación.

Ambas técnicas permitieron obtener una caracterización precisa de las necesidades de seguridad digital de las PYMEs y la viabilidad de implementar la solución tecnológica propuesta.

Procesamiento y análisis de la información

El análisis de la información recabada se desarrolló a través de dos dimensiones: En primer lugar se empleó el análisis cualitativo de los datos obtenidos en las entrevistas, con codificación temática y categorización de respuestas para identificar patrones de necesidades, niveles de preparación técnica y percepción del riesgo en seguridad digital. Del mismo modo, se llevó a cabo el análisis descriptivo aplicado a los datos de la encuesta, con la finalidad de interpretar tendencias relacionadas con el uso y percepción de herramientas de pentesting.

De forma posterior al análisis de los datos, se llevaron a cabo tres etapas que permitieron desarrollar y validar una arquitectura funcional de sandbox virtual con herramientas de pentesting orientada a PYMEs. En la primera fase, se llevó a cabo la identificación y selección de herramientas open source especializadas en análisis de vulnerabilidades, análisis de malware y pruebas de seguridad para aplicaciones móviles y sitios web. La elección se fundamentó en criterios como robustez técnica, facilidad de integración, documentación disponible, compatibilidad con sistemas operativos y pertinencia para entornos empresariales de escala media. Entre las herramientas seleccionadas se destacan REMnux, VirtualBox, OWASP ZAP, OpenVAS, MobSF y Kali Linux.

Asimismo, durante la segunda fase se realizaron pruebas de concepto (PoC) en entornos virtuales, simulando escenarios reales de ataques cibernéticos. Estas pruebas permitieron verificar la funcionalidad y efectividad de las herramientas seleccionadas, así como su capacidad para operar de forma integrada dentro del sandbox. También se evaluaron aspectos como la facilidad de uso, la interoperabilidad entre plataformas y la pertinencia de los resultados obtenidos para contextos organizacionales diversos.

De forma posterior, en la tercera fase se elaboró una guía operativa detallada que documenta paso a paso el proceso de instalación, configuración, integración y uso del entorno sandbox. Esta guía incluye lineamientos técnicos para la ejecución de pruebas, interpretación de resultados y generación de reportes, y fue validada por expertos en ciberseguridad, así como por los representantes de las empresas participantes en las pruebas piloto, asegurando su aplicabilidad práctica y su facilidad de adopción por parte de las PYMEs.

4. RESULTADOS

En la presente sección se exponen los principales hallazgos obtenidos a partir de la aplicación de encuestas, entrevistas y pruebas técnicas realizadas durante el desarrollo del proyecto. Los resultados permiten evaluar tanto la percepción y preparación de las PYMEs frente a la ciberseguridad, como la eficacia del diseño e implementación del sandbox virtual con herramientas de pentesting para identificar vulnerabilidades en aplicaciones móviles y sitios web.

Herramientas de Pentesting y Percepción Empresarial sobre la Seguridad Cibernética

A partir de la aplicación de una encuesta estructurada a 17 pequeñas y medianas empresas (PYMEs), se obtuvo una caracterización inicial del contexto de seguridad digital de las organizaciones participantes. En cuanto al tamaño de las empresas, el 76.5% corresponde a medianas y el 23.5% a pequeñas empresas, lo que refleja una mayor participación del segmento mediano, posiblemente por su estructura organizativa más abierta a intervenciones tecnológicas.

Respecto al conocimiento previo sobre ciberseguridad, el 82.4% de los encuestados manifestó tener nociones en el área, frente a un 11.8% que no posee conocimiento y un 5.9% que no está seguro. Sin embargo, a pesar de esa familiaridad general con la temática, el 100% de las empresas reportó no implementar actualmente herramientas de pentesting, lo cual evidencia una brecha entre el reconocimiento del problema y la acción técnica concreta.

En esa misma línea, el 82.4% de los participantes consideró urgente mejorar la seguridad cibernética de su empresa, mientras que el 17.6% indicó que esto dependería del contexto específico. Las vulnerabilidades en aplicaciones fueron percibidas como el principal riesgo (82.4%), muy por encima de amenazas como malware, phishing o ingeniería social.

Asimismo, el 64.7% de las empresas identificó como principal utilidad del uso de herramientas como REMnux o un sandbox virtual la identificación y corrección de vulnerabilidades, mientras que un 23.5% valoró su uso para fomentar la cultura de la seguridad, y el 11.8% señaló el cumplimiento normativo.

Sin embargo, se evidencian barreras importantes para su adopción: el costo de implementación fue la principal preocupación (82.4%), seguido por la complejidad técnica (11.8%) y la seguridad de los datos (5.9%). En relación con la herramienta REMnux, la mayor inquietud fue precisamente la complejidad de uso (29.4%). Estos datos muestran una disposición favorable al uso de herramientas avanzadas, pero condicionada por limitaciones presupuestarias y técnicas.

De igual manera, un 70.6% de los participantes indicó que su empresa tiene un nivel de conocimientos intermedio sobre pentesting y ciberseguridad, mientras que el 29.4% se dividió entre bajo o nulo conocimiento. Esto refuerza la necesidad de capacitación previa como requisito para la implementación efectiva de entornos seguros.

Diseño e Implementación de la Arquitectura del Sandbox Virtual

En esta categoría se describe la construcción y puesta en marcha del sandbox virtual que integró múltiples herramientas open source para el análisis de malware y el pentesting de sitios web y aplicaciones móviles.

Se diseñó una infraestructura basada en VirtualBox que incluyó cinco máquinas virtuales con sistemas operativos Windows, Ubuntu y Kali Linux, configuradas en red privada para garantizar el aislamiento del entorno. Las herramientas integradas fueron REMnux, OpenVAS, OWASP ZAP y MobSF, entre otras, seleccionadas por su capacidad técnica y disponibilidad gratuita.

Durante las simulaciones, se llevaron a cabo escenarios de prueba enfocados en tres áreas:

- Análisis de malware con REMnux: Mediante la inyección y ejecución controlada del ransomware TeslaCrypt en una máquina virtual con Windows 11. Se utilizaron herramientas como Wireshark y Process Monitor para capturar el comportamiento malicioso en tiempo real, así como Radare2, Ghidra y Binwalk para realizar análisis estático. El sandbox permitió ejecutar estas pruebas sin comprometer la infraestructura real, validando así su eficacia como entorno seguro.

- Evaluación de vulnerabilidades en sitios web: Mediante OpenVAS y OWASP ZAP. Se realizaron escaneos sobre servidores simulados (IP 193.168.1.65), detectando debilidades como inyecciones SQL, configuraciones inseguras y encabezados HTTP vulnerables. Las pruebas confirmaron la capacidad de estas herramientas para identificar amenazas críticas y emitir recomendaciones precisas.

- Pentesting en aplicaciones móviles: Con MobSF, utilizando emuladores Android e iOS para instalar y analizar APKs. Se configuraron los permisos mínimos necesarios y se integró el análisis tanto estático como dinámico, detectando estructuras inseguras y funciones de riesgo.

La arquitectura fue validada por expertos, siguiendo guías operativas que definieron claramente las fases de pentesting (reconocimiento, análisis, explotación, pos-explotación y reporte), asegurando la reproducibilidad del procedimiento.

Evaluación del Producto Tecnológico y Validación de la Hipótesis

La evaluación integral del sandbox virtual confirmó la hipótesis central del estudio: es posible diseñar e implementar una arquitectura funcional que permita a las PYMEs analizar y mitigar vulnerabilidades críticas en sus sistemas mediante herramientas open source.

El uso de REMnux permitió realizar análisis estáticos y dinámicos de malware en condiciones controladas, identificando técnicas de cifrado, comportamiento en red y persistencia. La capacidad de aislar el malware en el entorno virtual aseguró la integridad de la infraestructura real, lo que representa una ventaja crucial para las PYMEs con recursos limitados.

Por su parte, OpenVAS y OWASP ZAP evidenciaron su eficacia para detectar fallos en sitios web, tales como ejecución remota, inyecciones, fallos de autenticación y configuración insegura. MobSF facilitó un análisis técnico detallado de aplicaciones móviles, revelando errores comunes de desarrollo y potenciales vectores de ataque.

A la luz de lo antes planteado, es posible afirmar que los resultados reflejan que la arquitectura propuesta ofrece una solución robusta, flexible y escalable, que permite a las PYMEs ejecutar pruebas de seguridad avanzadas sin depender de

costosos entornos comerciales. Además, la validación práctica mediante escenarios reales de prueba respalda la viabilidad operativa del producto tecnológico diseñado.

5. CONCLUSIONES

La presente investigación permitió diseñar, implementar y evaluar una arquitectura de sandbox virtual con herramientas de pentesting de tipo open source, orientada a mejorar la detección de vulnerabilidades en aplicaciones móviles y sitios web, especialmente en el contexto de las pequeñas y medianas empresas (PYMEs). De esta forma, los resultados obtenidos reflejan la efectividad de esta solución tecnológica aplicada, tanto en el plano técnico como en el fortalecimiento de la cultura de seguridad cibernética en las organizaciones participantes.

En primera instancia, se concluye que la arquitectura propuesta demostró una alta eficacia en la detección de malware y vulnerabilidades, validando la hipótesis de que es posible identificar riesgos críticos mediante un entorno de pruebas aislado y controlado. Así, el uso de herramientas como REMnux, OpenVAS, OWASP ZAP y MobSF permitió por na parte detectar de forma precisa amenazas como ransomware, inyecciones SQL y configuraciones inseguras, asimismo fue posible generar reportes detallados para su análisis técnico y mitigación.

Asimismo, se constató que esta implementación contribuye significativamente a la reducción de riesgos cibernéticos, al permitir una evaluación previa de las debilidades antes de que puedan ser explotadas por actores maliciosos. La mencionada capacidad preventiva fortalece la resiliencia digital de las empresas y protege activos sensibles frente a amenazas en línea cada vez más sofisticadas.

Por otra parte, durante la ejecución del proyecto también se identificaron áreas de mejora relacionadas con la complejidad técnica de ciertas herramientas y la necesidad de contar con hardware robusto para ejecutar múltiples entornos virtualizados. En ese sentido, se evidenció la importancia de contar con personal técnico capacitado y la necesidad de ajustar configuraciones de red, permisos y recursos del sistema para lograr un funcionamiento óptimo del sandbox virtual.

Otro hallazgo relevante obtenido, fue el impacto positivo que tuvo el proyecto en la cultura de seguridad organizacional. Así, a través de las entrevistas y encuestas aplicadas, se observó un creciente interés por parte de las empresas en fortalecer su postura de seguridad, así como una mayor conciencia sobre la importancia del pentesting como práctica regular. Este proceso de concienciación, aunque incipiente, constituye una base sólida para futuras acciones de formación y fortalecimiento institucional.

Del mismo modo, en cuanto a las consideraciones económicas, si bien el costo de implementación fue identificado como una barrera importante, se concluye que el uso de herramientas de código abierto representa una alternativa accesible y escalable para las PYMEs. Los beneficios obtenidos en términos de detección temprana de vulnerabilidades y protección de activos superan los costos iniciales, especialmente si se considera la posibilidad de implementar el producto tecnológico por fases.

Así pues, la investigación confirma la importancia de adoptar medidas proactivas para prevenir incidentes de seguridad, mediante entornos de prueba que permitan realizar evaluaciones constantes. Del mismo modo, se resalta la necesidad de mantener un proceso continuo de actualización, monitoreo y mejora de las capacidades de defensa cibernética, apoyado en soluciones accesibles y eficientes como las desarrolladas en este estudio.

De esta forma, se establece que la colaboración con expertos, la inversión en capacitación y la integración de estas herramientas en procesos institucionales estables, son aspectos clave para garantizar una protección efectiva en el actual entorno digital. Así, el producto tecnológico diseñado y validado en esta investigación constituye así una propuesta aplicable, replicable y de alto valor para las PYMEs, al ofrecerles una solución integral para mejorar su seguridad informática frente a amenazas emergentes.

REFERENCIAS BIBLIOGRÁFICAS

Arias, F. G. (2012). El proyecto de investigación. Introducción a la metodología científica. 6ta. Fidias G. Arias Odón. https://acortar.link/YdzwnY

CVE-Mitre. (2025). CVE - Lucha Contra el Extremismo Viral. https://cve.mitre.org/

Díaz, C., Ariza, E., & Ruiz, M. (2023). La Ciberseguridad en las PYMES [Tesis de Especialización, Escuela de Administración de Negocios]. https://scholar.google.es/scholar?hl=es&as_sdt=0%2C5&q=ciberseguridad+pymes&btnG=

Fernández, D., & Martínez, G. (2018). Ciberseguridad, Ciberespacio y Ciberdelincuencia (pp. 1-236). Thomson Reuters Aranzadi. https://udimundus.udima.es/handle/20.500.12226/84

Fortra. (2025). Fortra | Soluciones de software de Ciberseguridad. https://www.fortra.com/es

Gaitán, S. (2019). Riesgos del uso de dispositivos móviles en seguridad de la información de las PYMES. Universidad Piloto de Colombia. http://repository.unipiloto.edu.co/handle/20.500.12277/6472

Gordón, D., & Pacheco, R. (2018). Análisis de Estrategias de Gestión de Seguridad Informática con Base en la Metodología Open Source Security Testing Methodology Manual (OSSTMM) para la Intranet de una Institución de Educación Superior.

ReCIBE. Revista electrónica de Computación, Informática, Biomédica y Electrónica, 7(1), 1-21.

Hernández, R., Fernández, C., & Baptista, P. (2014). Metodología de la Investigación. McGraw Hill Education.

Ospina, M., & Sanabria, P. (2020). Desafíos nacionales frente a la ciberseguridad en el escenario global: Un análisis para Colombia. Revista Criminalidad, 62(2), 199-217.

Ovallos, J., Rico, D., & Medina, Y. (2020). Guía práctica para el análisis de vulnerabilidades de un entorno cliente-servidor GNU/Linux mediante una metodología de pentesting. Revista Ibérica de Sistemas e Tecnologias de Informação, 335-350.

Rueda, A. (2017, mayo 16). Diseño de un Pentesting para una Aplicación Web Basado en la Metodología OWASP V.4. Gestiopolis. https://www.gestiopolis.com/diseno-pentesting-una-aplicacion-web-basado-la-metodologia-owasp-v-4/

Smith, K., & Forman, S. (2014). Bring your own device: Challenges and solutions for the mobile workplace. Employment Relations Today, 67-73.

Vanegas, A. (2019). Pentesting, ¿porque es importante para las empresas? Universidad Piloto de Colombia. http://repository.unipiloto.edu.co/handle/20.500.12277/6286

Weidman, G. (2014). Penetration Testing: A Hands-On Introduction to Hacking. No Starch Press.

Wright, W., Schroh, D., Proulx, P., Skaburskis, A., & Cort, B. (2006). The Sandbox for analysis: Concepts and methods. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 801-810. https://doi.org/10.1145/1124772.1124890

Conflicto de Intereses: Los autores afirman que no existen conflictos de intereses en este estudio y que se han seguido éticamente los procesos establecidos por esta revista. Además, aseguran que este trabajo no ha sido publicado parcial ni totalmente en ninguna otra revista.