Revista Iberoamericana para la Investigación y el Desarrollo Educativo
ISSN 2007 - 7467

https://doi.org/10.23913/ride.v15i29.2052

Artículos científicos

EthkLab: laboratorio de bajo costo para aprendizaje práctico en temas de ciberseguridad

EthkLab: Low-cost laboratory for hands-on learning in cybersecurity issues

EthkLab: laboratório de baixo custo para aprendizagem prática em temas de segurança cibernética

Holzen Atocha Martínez-García
Tecnológico Nacional de México, Instituto Tecnológico Superior Progreso, México
holzen.mg@progreso.tecnm.mx
https://orcid.org/0000-0003-0591-0049

Enrique Camacho-Pérez
Universidad Autónoma de Yucatán, México
enrique.camacho@correo.uady.mx
https://orcid.org/0000-0002-2581-1921

Ligia Beatriz Chuc-Us
Tecnológico Nacional de México, Instituto Tecnológico Superior Progreso, México
ligia.cu@progreso.tecnm.mx
https://orcid.org/0000-0002-6433-630X

Resumen

En este artículo se presenta EthkLab, un laboratorio portátil y de bajo costo para el aprendizaje en ciberseguridad y *hacking* ético. El objetivo fue desarrollar un entorno de aprendizaje para estudiantes del Tecnológico Nacional de México, campus Progreso, los cuales carecen de un laboratorio especializado en ciberseguridad. Para eso, en primer lugar, se evalúa la viabilidad de la construcción de dicho laboratorio y, posteriormente, se diseña la arquitectura específica de *hardware* y se desarrolla el prototipo. Para validar el laboratorio se efectuaron diversas pruebas con estudiantes voluntarios, las cuales arrojaron resultados satisfactorios que respaldan la hipótesis de que puede ser empleado en beneficio de los estudiantes y potenciar el desarrollo de sus habilidades mediante pruebas prácticas realistas. Sin embargo, como en todo desarrollo preliminar, se identificaron áreas de oportunidad que

deberán ser evaluadas y mejoradas en futuros trabajos sobre esta arquitectura propuesta, la cual es escalable tanto vertical como horizontalmente debido a la naturaleza de su diseño.

Palabras clave: aprendizaje práctico, ciberseguridad, entorno de aprendizaje, laboratorio portátil.

Abstract

EthkLab, a low-cost portable laboratory for learning cybersecurity and ethical hacking, is presented. The objective was to develop a learning environment for students at the Tecnológico Nacional de México campus Progreso, who lack a specialized laboratory about cybersecurity. First, it is defined whether it is possible and feasible to build such a laboratory. Then the specific hardware architecture is designed and the prototype is developed. Various tests are applied to volunteer students for validation of the lab, revealing satisfactory results that support the hypothesis that it can be used to benefit students and improve their skills with realistic hands-on testing.

As in any preliminary development, areas of opportunity were found to be evaluated and corrected in future work on this proposed architecture, which is vertically and horizontally scalable due to the nature of its design.

Keywords: Learning environment, Cybersecurity, Hands-on learning, Portable lab.

Resumo

Este artigo apresenta o EthkLab, um laboratório portátil e de baixo custo para aprendizagem em segurança cibernética e hacking ético. O objetivo foi desenvolver um ambiente de aprendizagem para alunos do Tecnológico Nacional de México, campus Progreso, que carecem de um laboratório especializado em segurança cibernética. Para isso, primeiro avalia-se a viabilidade de construção do referido laboratório e, posteriormente, projeta-se a arquitetura de hardware específica e desenvolve-se o protótipo. Para validar o laboratório, foram realizados diversos testes com alunos voluntários, que produziram resultados satisfatórios que sustentam a hipótese de que o mesmo pode ser utilizado em benefício dos alunos e potenciar o desenvolvimento das suas competências através de testes práticos realistas. No entanto, como em todo o desenvolvimento preliminar, foram identificadas áreas de oportunidade que devem ser avaliadas e melhoradas em trabalhos futuros nesta

arquitectura proposta, que é escalável tanto vertical como horizontalmente devido à natureza do seu design.

Palavras-chave: aprendizagem prática, segurança cibernética, ambiente de aprendizagem, laboratório portátil.

Fecha Recepción: Febrero 2024 **Fecha Aceptación:** Agosto 2024

Introducción

El persistente déficit de personal capacitado en el ámbito de la ciberseguridad, evidenciado por los 1.8 millones de vacantes a nivel mundial en 2021 y los 35 000 puestos sin cubrir en México en áreas como *hacking* ético y cómputo forense, se ha convertido en un desafío crítico (Salazar-Mata *et al.*, 2021), panorama que se agrava por el continuo aumento de dispositivos electrónicos y servicios digitales, que brindan a los ciberdelincuentes una mayor amplitud de acción (Torres-Knight y Méndez-Morales, 2023). La alarmante realidad se refleja en los 187 000 millones de intentos de ciberataques registrados en México durante 2022, lo que representa un incremento del 20 % en comparación con el año anterior, según FortiGuard Labs (Fuentes-Penna *et al*., 2023).

Ante este escenario, la estrategia propuesta de crear centros educativos especializados en ciberseguridad, sugerida por Arreola-García (2019), resulta de gran interés, pues su enseñanza desde la academia no solo abordaría la urgente necesidad de personal cualificado, sino que también sería un pilar esencial para fortalecer la capacidad de empresas y gobiernos, lo que les permitiría desempeñar sus funciones en el ciberespacio de manera segura, innovadora y eficaz.

Aunque la expansión masiva de centros educativos especializados en ciberseguridad es un desafío, existe un creciente interés en abordar los problemas actuales. Universidades e institutos de educación superior ya ofrecen programas especializados, desde pregrado hasta posgrado, en áreas como *hacking* ético y gestión de riesgos. Este enfoque integral no solo busca satisfacer la demanda de expertos en ciberseguridad, sino también formar líderes capaces de enfrentar los retos digitales en constante evolución. Además, algunas instituciones entrenan a su personal mediante laboratorios prácticos.

Una de las mejores maneras de aprender sobre ciberseguridad es a través de los laboratorios de *hacking* ético (Pearson *et al.*, 2020), es decir, es un espacio donde se simula un ambiente real pero controlado para permitir que los estudiantes aprendan cómo funcionan los sistemas de seguridad, cómo detectar vulnerabilidades y las técnicas para explotarlas, de

modo que comprendan de manera integral cómo protegerse adecuadamente contra este tipo de ataques.

Sin embargo, aunque es fundamental que las instituciones de educación superior proporcionen la infraestructura tecnológica adecuada para apoyar el desarrollo integral del estudiante universitario (Muñoz-Martínez, 2020), la realidad suele ser diferente, especialmente en la educación universitaria pública, donde no se ha alcanzado la competitividad deseada en comparación con otros países. A pesar de que la educación pública universitaria es obligatoria según el artículo 3 de la Constitución Mexicana, en la práctica, las instituciones no cuentan con la infraestructura adecuada. Esto se debe en gran parte al contexto económico del país, por lo que el decreto mencionado puede considerarse efectivo en términos de cobertura, pero no en cuanto a mejoramiento (Velasco-Arellanes *et al.*, 2020).

En el caso específico del Tecnológico Nacional de México, campus Progreso, se observa una deficiencia en la carrera de Ingeniería en Sistemas Computacionales debido a la actualización de la especialidad del programa educativo, que en su última versión se enfoca en ciberseguridad, pero que no cuenta con un laboratorio especializado en esa disciplina para apoyar el desempeño de los estudiantes.

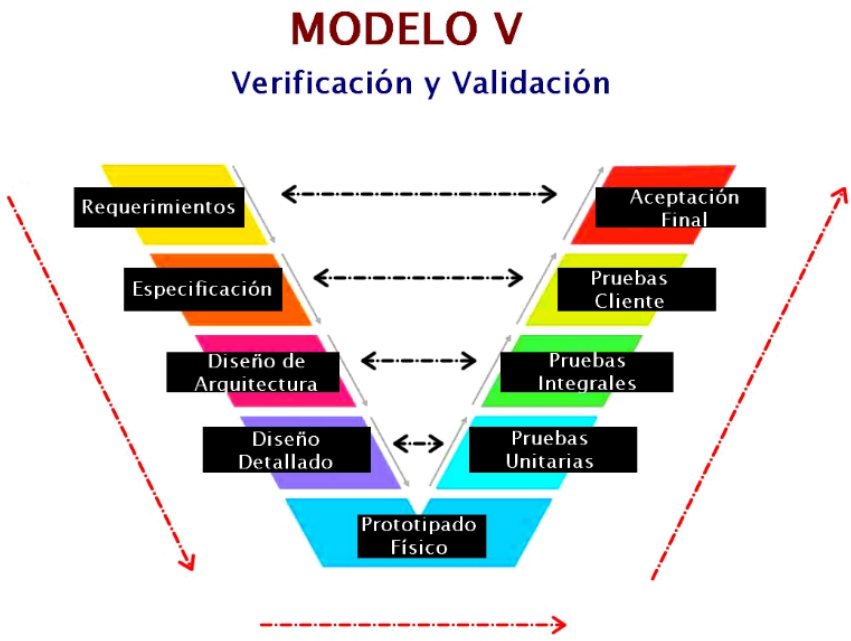
Por ello, el presente trabajo se enfoca en el diseño y desarrollo de un prototipo funcional de un laboratorio de ciberseguridad que se caracterice por ser de bajo costo, contar con entornos realistas y contribuir al desarrollo integral de los estudiantes en cuanto a habilidades prácticas en *pentesting* y *hacking* ético. La propuesta ofrecida constituye un estudio preliminar para determinar la viabilidad de utilizar tecnología de bajo costo en el desarrollo de una arquitectura de *hardware* que funcione como laboratorio de *hacking* ético, con el objetivo de minimizar costos y espacios para la implementación de un entorno físico de entrenamiento en ciberseguridad. El segundo aspecto a evaluar es la adaptabilidad y pertinencia de los estudiantes del Tecnológico Nacional de México para utilizar esta arquitectura.

Materiales y métodos

Para determinar la viabilidad de crear un laboratorio de ciberseguridad y *hacking* ético con tecnología de bajo costo, como primer paso se realizó una revisión del estado del arte y de la técnica con el objetivo de identificar prototipos similares documentados y evaluar su éxito en la implementación o pruebas. La búsqueda se llevó a cabo en la base de datos de Google Académico, utilizando términos como "cyber range low cost", "laboratorio de bajo costo", "cybersecurity lab ARM" y "SoC lab". De los resultados obtenidos, se seleccionaron 36 artículos relevantes basados en su título y resumen, y tras una lectura completa, se eligieron siete que presentaban prototipos funcionales con dispositivos de arquitectura ARM. Entre estos, destacaron los trabajos de Oh *et al.* (2020) y de Legg *et al.* (2023), quienes coincidieron en el uso de Raspberry Pi, una tarjeta de desarrollo con características de computadora personal de bolsillo.

Luego, en la segunda fase, se desarrolló la arquitectura del laboratorio propuesto, utilizando una metodología de validación y verificación (figura 1).

Figura 1. Modelo utilizado para el desarrollo de la arquitectura del laboratorio



Fuente: Elaboración propia

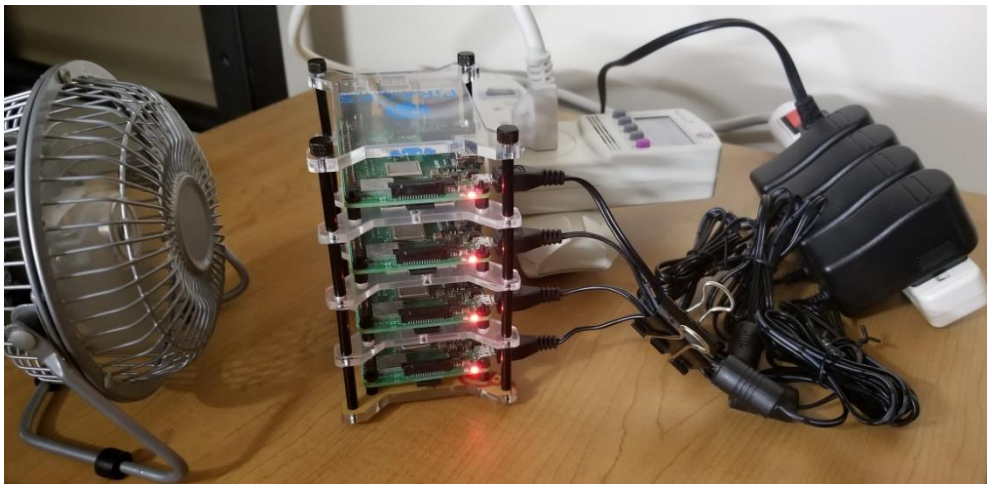
En la fase de validación, se configuraron escenarios vulnerables que fueron puestos a prueba por un grupo de 12 estudiantes voluntarios del séptimo semestre de la carrera de Ingeniería en Sistemas Computacionales del Instituto. Para ello, se diseñó una encuesta con el fin de evaluar la percepción de los alumnos sobre la utilización y desempeño del laboratorio. Este grupo fue seleccionado porque sus integrantes están comenzando a cursar asignaturas de la especialidad en ciberseguridad.

Primera fase

Como se mencionó, se seleccionaron siete publicaciones con prototipos experimentales que indicaban la posibilidad de generar laboratorios de ciberseguridad para la enseñanza universitaria. Entre ellos, se destacaron los estudios titulados *Teaching Web-Attacks on a Raspberry Pi Cyber Range* (Oh *et al*., 2020) y *Teaching Offensive and Defensive Cyber Security in Schools using a Raspberry Pi Cyber Range* (Legg *et al*., 2023).

En la propuesta de Oh *et al*. (2020) se implementa un laboratorio de ciberseguridad enfocado en ataques web, desplegando un servidor web vulnerable basado en tecnología Docker y cuatro nodos Raspberry Pi (figura 2). El análisis concluye que el costo fue inferior a 250 dólares y el consumo de energía menor a 25 watts (tabla 1). Entre las conclusiones, se sugiere que los laboratorios construidos con clústeres de Raspberry Pi pueden reducir los costos y mejorar la educación en ciberseguridad.

Figura 2. Clúster de laboratorio con Raspberry Pi 3b+



Fuente: Oh *et al*. (2020)

Tabla 1. Desglose de gastos y consumo de energía del clúster de laboratorio Raspberry Pi Cyber Range

Descripción	Cantidad	Costo unitario en dólares (US)	Total en dólares (US)	Consumo Máximo Unitario (Watts)
Raspberry Pi Modelo 3B+	4	35.00	140.00	4.9
Tarjetas microSD 8 GB	4	4.99	19.96	
Caja de acrílico PiRacks Clúster	1	29.95	29.95	
Fuente de poder	4	8.99	32.94	
Ventilador	1	10.99	10.99	5
Gran Total			233.84	24.6

Fuente: Elaboración propia con base en Oh *et al*. (2020)

Aunque el Raspberry Pi Cyber Range puede parecer visualmente poco elegante, los autores destacan que cumple eficientemente con el propósito original. Una de las características destacables de este proyecto es su bajo consumo de energía y el costo del *hardware*, que está por debajo del de un equipo de cómputo común, aunque ofrece prestaciones suficientes para ejecutar los entornos de práctica.

En cuanto al trabajo propuesto por Legg *et al*. (2023), se ofrece una variación en la metodología, ya que no utiliza un clúster como servidor objetivo. En su lugar, los dispositivos se emplean como terminales independientes que interactúan con un objetivo común. Para esto, se utiliza un modelo de Raspberry Pi con características diferentes, la Raspberry Pi 400, que ya incluye el teclado como parte del dispositivo y tiene el circuito embebido dentro de él (figura 3).

A la Raspberry Pi 400 se le añade un monitor portátil y un ratón para funcionar como terminal independiente, y se incluye una Raspberry Pi 4 como punto de acceso. El prototipo con cuatro terminales y un punto de acceso, denominado “UWE Cyber Pi Lab portable setup” por los autores, se muestra en la figura 4. Esta propuesta destaca una característica adicional de los laboratorios desarrollados con dispositivos de bajo costo: la portabilidad.

Figura 3. Raspberry Pi 400 por dentro y por fuera

Fuente: Raspberry Pi Ltd (s. f.)

Figura 4. UWE Cyber Pi Lab portable setup

Fuente: Legg *et al*. (2023)

Segunda fase

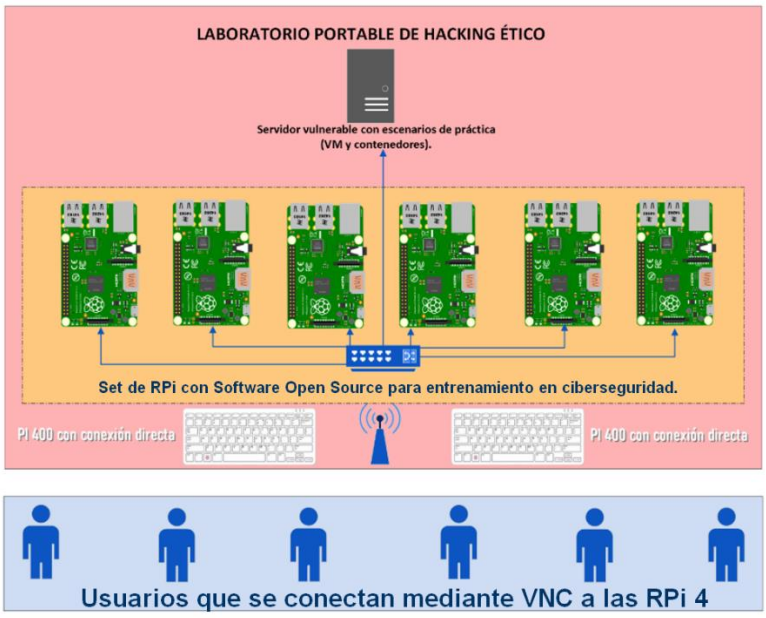
Según los estudios y resultados examinados, es factible responder a las preguntas iniciales sobre la posibilidad de establecer un laboratorio de *hacking* ético para la instrucción en ciberseguridad mediante el uso de tecnologías de bajo costo. La respuesta afirmativa se basa en varios estudios revisados que sugieren el uso de tecnologías asequibles con capacidades suficientes para la creación de laboratorios de ciberseguridad y *hacking* ético. Además, se observó que es viable aprovechar las dimensiones de la arquitectura para lograr un laboratorio fácilmente transportable.

Por lo tanto, se consideró plausible avanzar con el proyecto de implementación de un laboratorio de *hacking* ético y ciberseguridad para el Tecnológico Nacional de México,

campus Progreso, tomando como base los estudios previos y la necesidad local. En consecuencia, se optó por utilizar un dispositivo de bajo costo denominado Raspberry Pi, el cual es portátil, con un tamaño aproximado de una tarjeta de crédito y con una altura de unos pocos centímetros. Incluye componentes como un microprocesador, memoria, tarjeta de red, tarjeta wifi, Bluetooth, entrada de sonido, puertos USB, puerto HDMI y entrada de alimentación. Además, cuenta con pines GPIO que pueden interactuar con otros circuitos eléctricos o electrónicos y se pueden programar utilizando el lenguaje Python a través de su sistema operativo, lo que lo convierte en un dispositivo versátil y multifuncional (Martínez-Luengo, 2021).

Un primer diseño consideró la interconexión de un servidor de máquinas virtuales vulnerables con dispositivos Raspberry Pi 4 como terminales, los cuales contienen el *software* necesario para atacar escenarios vulnerables de práctica. Para acceder a los terminales, que carecen de pantallas, se debe conectar un equipo de cómputo a la red interna del laboratorio y controlar de forma remota una Raspberry Pi 4 mediante VNC (Virtual Network Computing). VNC utiliza un protocolo propio llamado RFB (Remote Framebuffer Protocol), que permite la transmisión de información gráfica entre el servidor VNC (en la máquina que se controla) y el cliente VNC (en la máquina que realiza el control remoto). Aunque se contempló la opción de conexión directa a la red con equipos Raspberry Pi 400, esta se descartó posteriormente. La figura 5 muestra un esquema básico de la idea original.

Figura 5. Diseño preliminar de la arquitectura del laboratorio propuesto



Fuente: Elaboración propia

Después de realizar algunos cambios en la arquitectura de acuerdo con los requisitos especificados, la lista de elementos utilizados final quedó de la siguiente manera (se lista lo más relevante):

Tabla 2. Lista de elementos utilizados para el desarrollo de la arquitectura

CANTIDAD	DESCRIPCIÓN	FUNCIÓN
8	Raspberry Pi 4 B 8GB Ram ARM cortex 1.5 Ghz	Terminales con toda la instalación y configuración de *software* para escanear y vulnerar los escenarios de prueba.
1	MiniPC Intel NUC 10 performance NUC10i7FNKN intel core i7 12 GB Ram 1TB NVMe SSD	Equipo servidor/objetivo que contiene los escenarios vulnerables en máquinas virtuales.
1	Monitor Qian QM2151F 21.5” puerto HDMI	Pantalla para monitoreo del servidor de escenarios.
1	Router TP-Link Dual Band AX Archer AX10 WIFI6	Enrutador principal de la arquitectura
2	Switch Linksys SE3008 8 puertos 10/100/1000	Interconexión entre los RPi y el servidor de escenarios.
1	Hadulcet - Estación de computadora móvil con ruedas, color negro.	Parte de la estructura del laboratorio móvil.
1	Gabinete de pared profesional para servidores de red 6U Enson	Contenedor de la conexión eléctrica y de red cableada.
1	Kit teclado/ratón inalámbrico Logitech	Accesorios para manipular el servidor de escenarios.

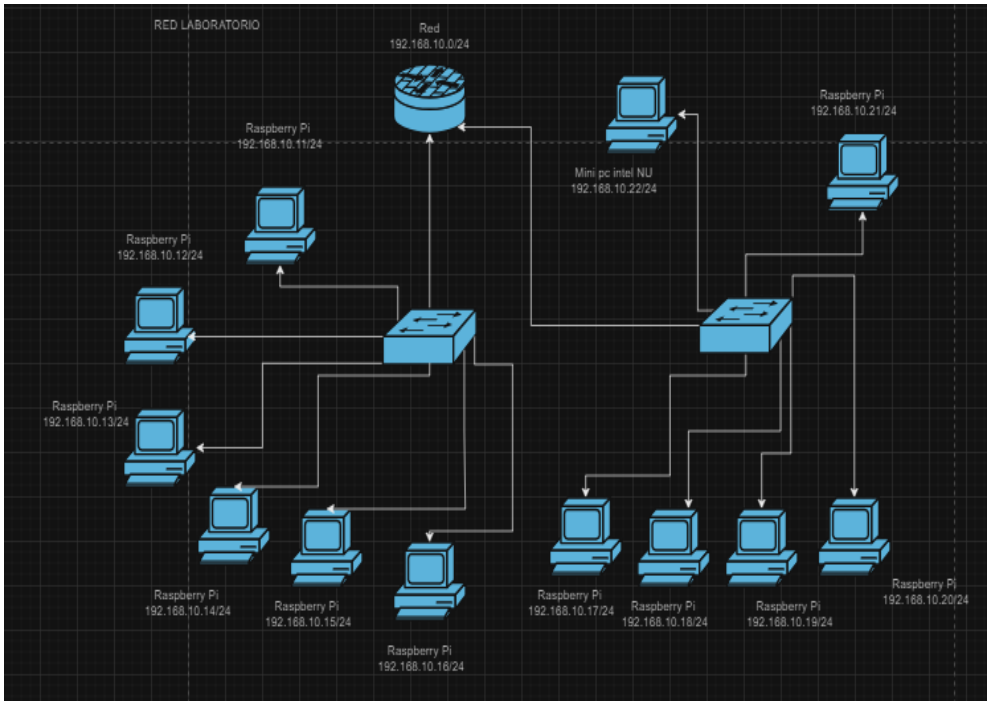
Fuente: Elaboración propia

Es importante recalcar que también se obtuvieron otros aditamentos para el correcto funcionamiento y mantenimiento de la propuesta, tales como cablería eléctrica, cableado de red, disco de respaldo periódico, tarjetas de memoria SD, entre otros materiales.

Resultados

Entre los resultados obtenidos en el análisis de la arquitectura de *hardware* deseada, se desarrolló el esquema de red descrito en la figura 6. Se diseñó la red utilizando una topología de estrella con dos *switches* y un *router*. Se implementaron dos métodos de asignación de direcciones IP: se asignaron direcciones IP estáticas a los dispositivos terminales RPi 4 y al servidor de escenarios, mientras que se habilitó el servicio dinámico para los clientes conectados a través de red inalámbrica mediante DHCP (Protocolo de Configuración Dinámica de Host).

Figura 6. Diseño lógico de la red en el laboratorio



Fuente: Elaboración propia

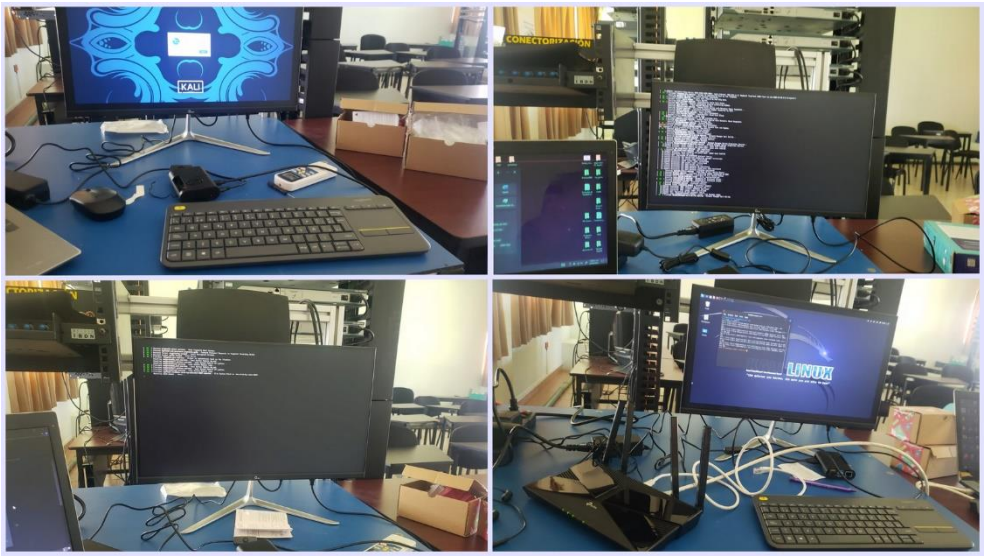
Seguidamente, se obtuvo el prototipado físico de la red (figura 7) y se iniciaron las pruebas unitarias (figura 8) para verificar el funcionamiento adecuado de cada uno de los dispositivos involucrados, realizando pruebas de manera individual. En el caso de las terminales, las pruebas se centraron en el encendido y la comunicación exitosa en red. Los dispositivos intermedios (*switch* y *router*) fueron evaluados simultáneamente, tomando como

parámetros de éxito la comunicación entre los dispositivos del laboratorio y el equipo que se conecta de forma remota. La tabla 3 presenta los resultados obtenidos en esta etapa.

Figura 7. Prototipo físico de la arquitectura de red

Fuente: Elaboración propia

Figura 8. Pruebas unitarias en los dispositivos



Fuente: Elaboración propia

Tabla 3. Resultados de las pruebas unitarias

Dispositivo	Pruebas exitosas	Pruebas fallidas	Comentarios
Raspberry Pi 1 (192.168.0.11)	6	0	Sin incidencias
Raspberry Pi 2 (192.168.0.12)	4	2	En la tercera y cuarta prueba se congeló por momentos en el escritorio del sistema, no dejando trabajar fluidamente. Se notó un problema de memoria SD corrupta, procediendo al reemplazo.
Raspberry Pi 3 (192.168.0.13)	6	0	Sin incidencias
Raspberry Pi 4 (192.168.0.14)	6	0	Sin incidencias
Raspberry Pi 5 (192.168.0.15)	6	0	Sin incidencias
Raspberry Pi 6 (192.168.0.16)	6	0	Sin incidencias
Raspberry Pi 7 (192.168.0.17)	6	0	Sin incidencias
Raspberry Pi 8 (192.168.0.18)	6	0	Sin incidencias
Switch LinkSys 1	24	0	Permitió conectividad y comunicación con la mitad de los dispositivos durante las seis pruebas realizadas.
Switch LinkSys 2	24	0	Permitió conectividad y comunicación con la mitad de los dispositivos durante las seis pruebas realizadas.

Router TP-Link	45	3	En las pruebas tres, ocho y 12 Se encontraron incidencias para asignación de dirección IP mediante DHCP a la laptop cliente. Se realizaron cambios a las configuraciones del servicio hasta lograr un óptimo desempeño.

Fuente: Elaboración propia

Para realizar las pruebas integrales y de cliente se completó la integración de los elementos en el laboratorio propuesto, como se puede observar en la figura 9. Posteriormente, se convocó al grupo de séptimo semestre de Ingeniería en Sistemas Computacionales del Tecnológico Nacional de México, campus Progreso, para realizar prácticas en el laboratorio (figura 10).

Figura 9. EthkLab: laboratorio ya integrado (vistas perspectiva derecha y frontal)

Fuente: Elaboración propia

Figura 10. Estudiantes conectados al laboratorio mediante VNC realizando prácticas de *hacking* ético

Fuente: Elaboración propia

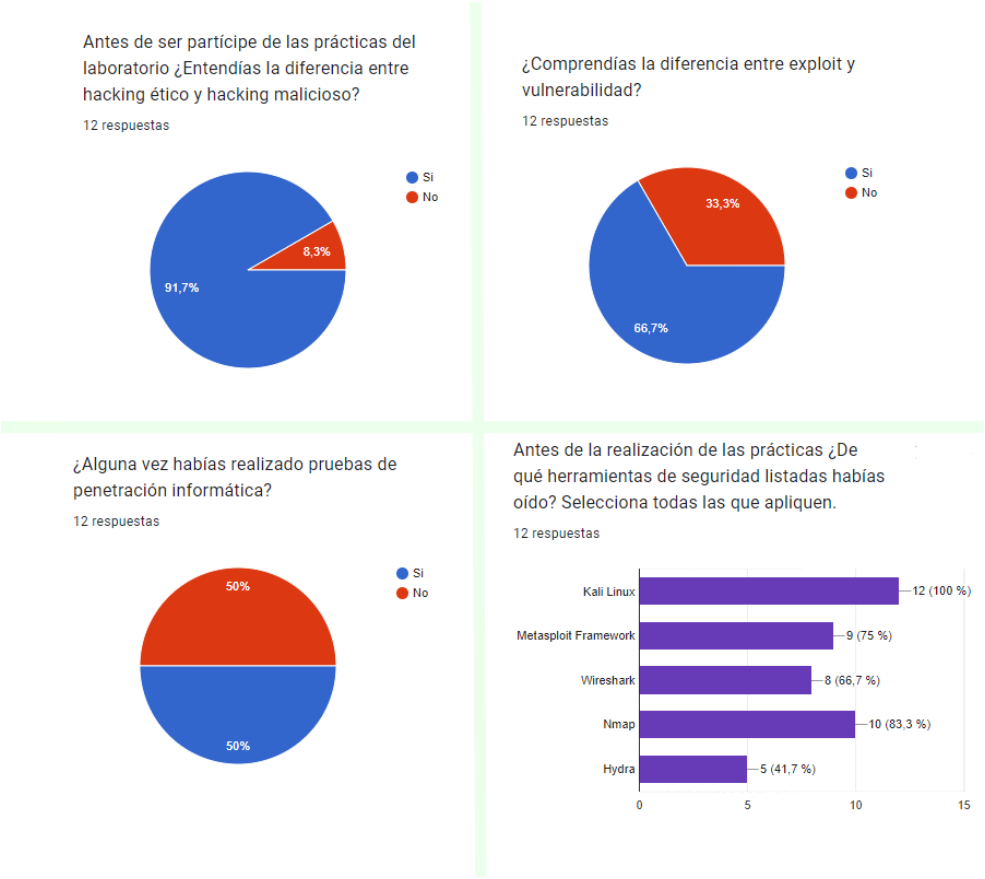
Tabla 4. Prácticas realizadas por los estudiantes

Número de práctica	Título	Objetivo
1	Escaneo de redes	Identificar dispositivos en una red y sus servicios activos.
2	Análisis de vulnerabilidades	Identificar posibles vulnerabilidades en los servicios y sistemas detectados.
3	Explotación de vulnerabilidades conocidas	Ganar acceso no autorizado a sistemas para entender las implicaciones de las vulnerabilidades.
4	(In)seguridad web	Realizar una prueba de penetración a un servidor web, utilizando como puerta de entrada un sitio alojado en el mismo.
5	Pentesting (no guiado)	Realizar una prueba de penetración integrando los conceptos y técnicas previamente estudiadas.

Fuente: Elaboración propia

Al finalizar las prácticas, se aplicó un instrumento a los estudiantes voluntarios. Este instrumento se centró en tres aspectos principales: a) el conocimiento previo del usuario sobre ciberseguridad, b) el desempeño del usuario en las prácticas sobre EthkLab y su percepción propia después de las pruebas, y c) la percepción del usuario sobre EthkLab. A continuación, se presentan los resultados más relevantes.

Figura 11. Conocimiento previo de los usuarios respecto a la temática y herramientas

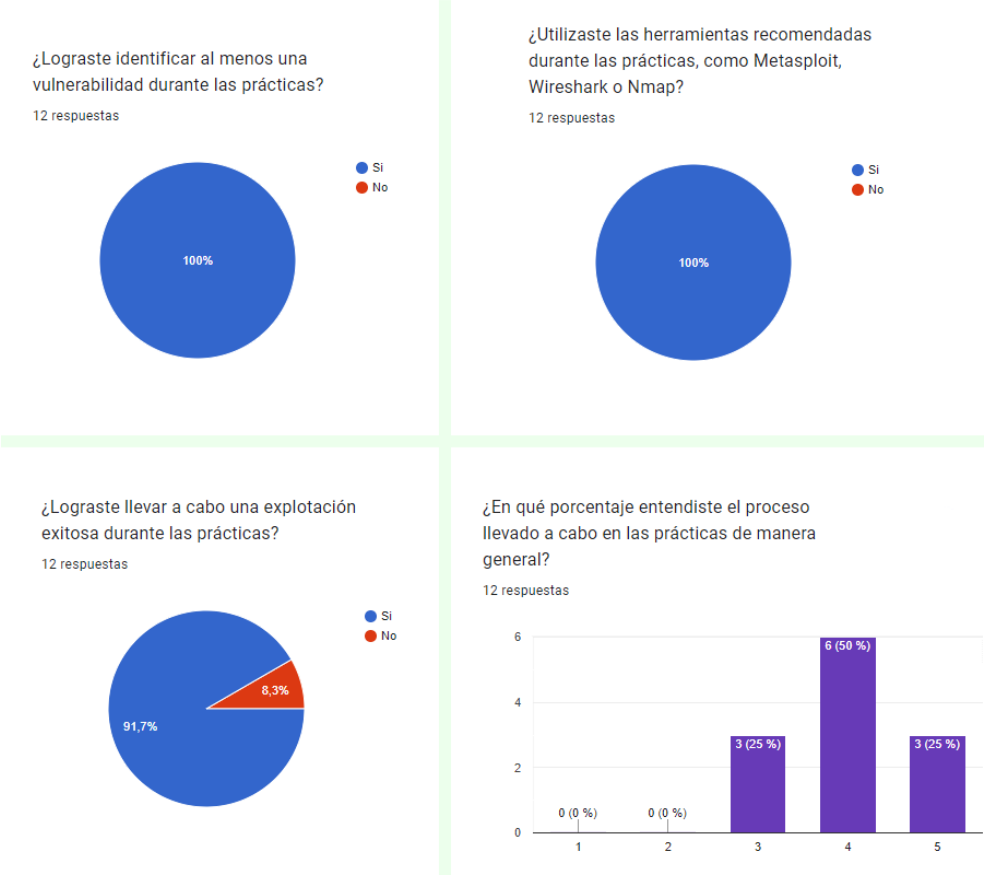


Fuente: Elaboración propia

La figura 11 representa los datos recolectados en la primera sección del instrumento, donde los resultados en general indican una base sólida de conocimientos en ciberseguridad entre los participantes, aunque con algunas variaciones en la familiaridad con herramientas específicas. Por ejemplo, la mayoría de los participantes afirma entender los conceptos básicos de ciberseguridad, y la mitad reporta tener experiencia en pruebas de penetración informática, lo que sugiere un interés o exposición previa en el campo de la seguridad cibernética. En cuanto a las herramientas, Kali Linux es ampliamente reconocido, así como Metasploit Framework, Wireshark y Nmap; sin embargo, Hydra parece ser menos familiar para algunos participantes.

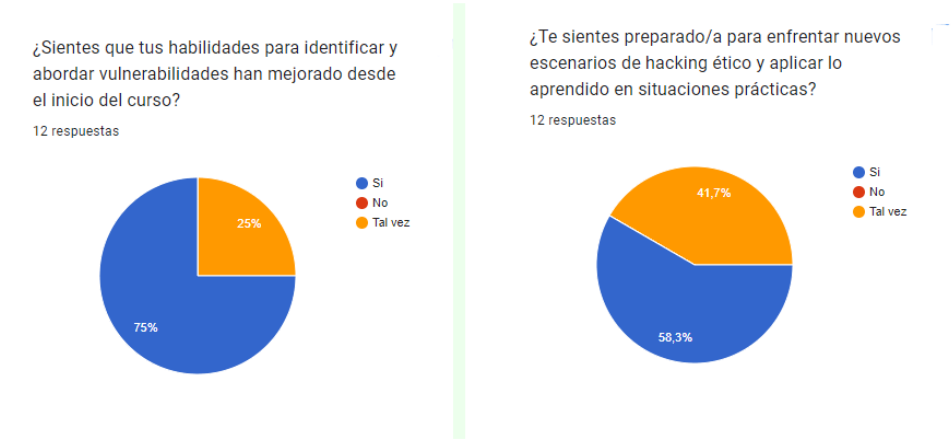
Revista Iberoamericana para la Investigación y el Desarrollo Educativo
ISSN 2007 - 7467

Figura 12. Experiencia de los participantes durante las prácticas



Fuente: Elaboración propia

Figura 13. Percepción personal posterior a las prácticas con EthkLab



Fuente: Elaboración propia

La figura 12 muestra los datos de la segunda sección del instrumento, donde todos los participantes afirmaron haber identificado al menos una vulnerabilidad durante las prácticas, lo que indica una ejecución efectiva de las actividades y la aplicación práctica de conocimientos en situaciones reales. Además, todos utilizaron las herramientas recomendadas, lo que sugiere una aplicación activa de herramientas clave en pruebas de penetración y exploración de vulnerabilidades.

Asimismo, la mayoría logró una explotación exitosa, lo cual destaca la efectividad de sus habilidades en la aplicación de técnicas de explotación. En cuanto al entendimiento del proceso, la mayoría se situó en un nivel razonable de cuatro y cinco en la escala subjetiva, aunque algunos indicaron un nivel ligeramente inferior con un puntaje de tres. Este aspecto puede señalar áreas de mejora o revisión para futuras sesiones de formación que se puedan ajustar a los objetivos y expectativas del curso.

En general, los resultados indican un buen desempeño, pero también ofrecen oportunidades para refinamiento y mejora continua. Esta afirmación se respalda con los datos mostrados en la figura 13, donde las respuestas a las últimas dos preguntas, que se centran en la percepción personal y la preparación para enfrentar nuevos escenarios de *hacking* ético, reflejan una variedad de respuestas. En otras palabras, algunos participantes se sienten seguros, mientras que otros expresan dudas, lo que indica que la mejora en habilidades no siempre se traduce en una completa confianza en la aplicación de esos conocimientos en situaciones nuevas.

Lo anterior puede sugerir la necesidad de enfoques pedagógicos adicionales, práctica continua o recursos que refuercen la confianza de los participantes en la aplicación práctica de sus habilidades de *hacking* ético. Es decir, estos resultados proporcionan una visión integral de la experiencia del curso y áreas potenciales para ajustes o mejoras en futuras iteraciones del programa de formación.

Finalmente, la figura 14 muestra que la percepción de los participantes hacia EthkLab es mayoritariamente positiva, ya que la mayoría considera que la interfaz es fácil de usar y que las herramientas integradas proporcionaron una experiencia completa de *hacking* ético. De hecho, la calificación general de la experiencia del usuario es predominantemente alta, con varias respuestas en el rango de cuatro y cinco. Sin embargo, algunas calificaciones más bajas indican que algunos participantes pudieron haber enfrentado desafíos o áreas de mejora en la integración de sus equipos o en la efectividad de ciertas herramientas.

Figura 14. Percepción de los participantes sobre EthkLab

Fuente: Elaboración propia

Discusión

Como mencionan Yamin *et al.* (2020), la primera línea de defensa contra amenazas y delitos cibernéticos es estar consciente y preparado, por ejemplo, a través de la capacitación en ciberseguridad, para lo cual se requieren plataformas de prueba e infraestructuras dedicadas que faciliten la materialización y ejecución de escenarios de capacitación.

En tal sentido, los laboratorios prácticos, también conocidos como *hands-on*, ofrecen experiencias valiosas que incluyen casos de estudio novedosos, oportunos y pertinentes para el ambiente laboral real (Pearson *et al*., 2020). En la formación de expertos en ciberseguridad, Castro-León y Rendón-Burgos (2021) indican que es crucial reconocer la necesidad de una adecuada formación para los futuros profesionales de las carreras informáticas. Esto es especialmente relevante dado el drástico cambio que el internet ha provocado en varios sectores, de los cuales el de las comunicaciones ha sido uno de los más afectados. Por lo tanto, estudiar ciberseguridad de manera práctica es una forma efectiva de desarrollar la experticia en el estudiante, ya que le permite desarrollar habilidades técnicas y adaptarse a

escenarios dinámicos. Esto, además, profundiza su comprensión de las vulnerabilidades, mejora la conciencia sobre la importancia de la seguridad cibernética y los prepara para el mundo laboral al demostrar habilidades directamente aplicables, cumpliendo con el enfoque de ciberseguridad basada en el factor humano (Grobler *et al.*, 2021; Marble *et al*., 2015; Zimmerman y Renaud, 2019). Asimismo, fomenta la ética profesional al realizar pruebas de manera ética y legal, lo cual promueve la responsabilidad y la integridad en el manejo de información sensible.

Por todo lo anterior, se consideró pertinente el desarrollo de EthkLab para el fortalecimiento de las habilidades en *hacking* ético de los estudiantes de la carrera de Ingeniería en Sistemas Computacionales del Tecnológico Nacional de México, campus Progreso. Este desarrollo tecnológico de bajo costo puede realizar las mismas funciones que laboratorios de otras instituciones, aunque cabe resaltar que las preguntas iniciales sobre su desempeño efectivo deben comprobarse, tal como se realizó en este estudio.

En este caso concreto, si bien los resultados preliminares indican que EthkLab puede ser utilizado en un curso de capacitación, es importante considerar algunos aspectos de mejora basados en la percepción final de una minoría de los participantes. Aspectos como el entendimiento del proceso integral de las prácticas, la complejidad de la integración de EthkLab con el equipo de cómputo personal y la experiencia general de satisfacción no alcanzaron el 80 % de aceptación, lo que sugiere la necesidad de abordar estos aspectos con mayor profundidad. No obstante, otros indicadores respaldan la hipótesis de que las prácticas incluidas en EthkLab pueden mejorar significativamente las habilidades de los estudiantes.

Conclusiones

EthkLab emerge como una innovadora solución en el campo de la enseñanza en ciberseguridad, proporcionando un laboratorio físico basado en Raspberry Pi 4 que integra entornos simulados de *hacking* ético y *pentesting*. Aunque se encuentra en sus primeras etapas, este enfoque ofrece a los usuarios un entorno práctico y realista para el desarrollo de habilidades, ya que permite la aplicación y exploración segura de técnicas y estrategias relacionadas con el *hacking* ético.

Aunque algunas pruebas no alcanzaron el 100 % de éxito, los resultados obtenidos revelan un sólido potencial para afinar y perfeccionar los detalles operativos. Estos datos iniciales proporcionan valiosos conocimientos y experiencias que pueden utilizarse para optimizar la eficacia del laboratorio y mejorar el porcentaje de éxito con los estudiantes

participantes. La flexibilidad y versatilidad inherentes a EthkLab, debido a su construcción con dispositivos de bajo costo y modulares, permiten un ajuste y mejora continuos, lo que brinda la oportunidad de abordar áreas específicas que requieren atención adicional. Por último, la retroalimentación recopilada durante estas pruebas iniciales sirve como un recurso valioso para el perfeccionamiento futuro del sistema, y allana el camino para un despliegue más efectivo y la obtención de resultados aún más robustos en futuras iteraciones.

Futuras líneas de investigación

El presente estudio ha arrojado resultados alentadores sobre la viabilidad y aceptación de un ciberentorno controlado (EthkLab) para el aprendizaje de *pentesting* y *hacking* ético utilizando dispositivos de bajo costo, específicamente el conjunto de tarjetas Raspberry Pi 4. Sin embargo, aún quedan áreas de investigación por explorar para mejorar tanto el desempeño como la eficacia de estos entornos. Entre las propuestas de líneas futuras de investigación se recomiendan las siguientes:

1. Optimización del ciberentorno de bajo costo: Se sugiere una investigación exhaustiva para optimizar el ciberentorno de bajo costo mediante diferentes configuraciones y sistemas de *software*, así como la evaluación de diferentes *hardware*. Aunque el uso de tarjetas Raspberry Pi 4 ha demostrado ser efectivo, es importante explorar otras opciones de *hardware* que puedan ofrecer un mayor poder de cómputo a un precio similar. Por ende, se podría considerar el uso de tarjetas Jetson Nano o incluso mini PC con arquitectura de 64 bits. Investigar estas alternativas podría proporcionar información sobre cómo mejorar la capacidad de procesamiento y la eficiencia del entorno de aprendizaje. Además, se podría evaluar la posibilidad de sustituir los sistemas operativos preconfigurados, como Kali Linux, con la opción de configurar manualmente el laboratorio con sistemas operativos minimalistas que incluyan únicamente las herramientas necesarias para los escenarios de prueba. Esta aproximación podría permitir un mayor control sobre el *software* utilizado y optimizar el rendimiento del sistema, así como ofrecer una experiencia de aprendizaje más personalizada.
2. Evaluación cuantitativa y cualitativa del aprendizaje con EthkLab: Se propone realizar evaluaciones progresivas a los estudiantes con planes definidos en el ámbito de *hacking* ético y *pentesting* como parte de otro estudio, con especial énfasis en el desarrollo y evolución de las habilidades adquiridas. Asimismo, se sugiere llevar a

cabo una evaluación exhaustiva del aprendizaje utilizando EthkLab, abordando tanto aspectos cuantitativos como cualitativos. Esta investigación buscaría comprender en profundidad el impacto y la efectividad de EthkLab como herramienta de enseñanza en el ámbito de la ciberseguridad, mediante la recopilación y análisis de datos cuantitativos sobre el rendimiento y los resultados de aprendizaje, así como datos cualitativos que indaguen en la experiencia y percepción de los usuarios. El objetivo es proporcionar una visión integral y fundamentada sobre el uso de EthkLab como recurso educativo con el fin de mejorar la calidad y eficacia de la enseñanza en este campo.

Agradecimientos

Los autores agradecen al Tecnológico Nacional de México por el financiamiento económico de este proyecto, realizado del 1 de enero de 2023 al 31 de diciembre de 2023. También agradecen a los estudiantes de séptimo semestre, generación 2020, de la carrera de Ingeniería en Sistemas Computacionales del Tecnológico Nacional de México campus Progreso, y al Mtro. Edgar Alejandro Sagundo Duarte por su colaboración y el tiempo de clases cedido para las pruebas realizadas.

Referencias

Arreola-García, A. (2019). Desafíos a las estrategias de ciberseguridad en América. *Revista del Centro de Estudios Superiores Navales*, *40*(4), 25–53.

Castro-León, G. K. y Rendón-Burgos, C. E. (2021). *Creación de un entorno virtual de aprendizaje para un laboratorio de enseñanza de seguridad informática en carreras técnicas* (trabajo de grado). Universidad de Guayaquil. http://repositorio.ug.edu.ec/handle/redug/57097

Fuentes-Penna, A. F., Gómez-Cárdenas, R. y González-Ibarra, J. de D. (2023). La Ciberseguridad en México y los derechos humanos en la era digital. *Espacios Públicos*, *24*(61), 110–130.

Grobler, M., Gaire, R. and Nepal, S. (2021). User, Usage and Usability: Redefining Human Centric Cyber Security. *Frontiers in Big Data*, *4*. https://www.frontiersin.org/articles/10.3389/fdata.2021.583723

Legg, P., Mills, A. and Johnson, I. (2023). Teaching Offensive and Defensive Cyber Security in Schools using a Raspberry Pi Cyber Range. *Journal of The Colloquium for Information Systems Security Education*, *10*(1), Article 1. https://doi.org/10.53735/cisse.v10i1.172

Marble, J. L., Lawless, W. F., Mittu, R., Coyne, J., Abramson, M. and Sibley, C. (2015). The Human Factor in Cybersecurity: Robust & Intelligent Defense. In S. Jajodia, P. Shakarian, V. S. Subrahmanian, V. Swarup and C. Wang (eds.), *Cyber Warfare: Building the Scientific Foundation* (pp. 173–206). Springer International Publishing. https://doi.org/10.1007/978-3-319-14039-1_9

Martínez-Luengo, D. (2021). Anonimato y Pentesting con Raspberry Pi. http://e-spacio.uned.es/fez/view/bibliuned:master-ETSInformatica-CBS-Dmartinez

Muñoz-Martínez, M. (2020). Políticas educativas e incorporación de las TIC en la educación superior mexicana. *Revista Digital Universitaria*, *21*(6). https://biblat.unam.mx/es/revista/revista-digital-universitaria/articulo/politicas-educativas-e-incorporacion-de-las-tic-en-la-educacion-superior-mexicana

Oh, S. K., Stickney, N., Hawthorne, D. and Matthews, S. J. (2020). *Teaching Web-Attacks on a Raspberry Pi Cyber Range*. Proceedings of the 21st Annual Conference on Information Technology Education, 324–329. https://doi.org/10.1145/3368308.3415364

Pearson, B., Luo, L., Zou, C., Crain, J., Jin, Y. and Fu, X. (2020). Building a Low-Cost and State-of-the-Art IoT Security Hands-On Laboratory. En A. Casaca, S. Katkoori, S. Ray and L. Strous (eds.), *Internet of Things. A Confluence of Many Disciplines* (pp. 289–306). Springer International Publishing. https://doi.org/10.1007/978-3-030-43605-6_17

Raspberry Pi Ltd. (s. f.). Buy a Raspberry Pi 400 Personal Computer Kit. Raspberry Pi. https://www.raspberrypi.com/products/raspberry-pi-400/

Salazar-Mata, J. M., Cruz-Navarro, C., Balderas-Sánchez, A. V. y Díaz-Uribe, H. F. (2021). La seguridad informática en las instituciones de educación superior. TECTZAPIC: *Revista Académico-Científica*, *7*(2), 72–79.

Torres-Knight, R. R. T. y Méndez-Morales, O. A. M. (2023). Esfuerzo dentro del estado de Chihuahua, México en materia de ciberseguridad. Informática y Derecho. *Revista Iberoamericana de Derecho Informático*, *13*(2.ª época).

Velasco-Arellanes, F. J., Vera-Noriega, J. Á. y Durazo-Salas, F. F. (2020). La educación universitaria pública mexicana en el libre mercado: necesidades, ausencias y confusiones en su mejoramiento. *Voces y Silencios. Revista Latinoamericana de Educación*, *11*(2). https://doi.org/10.18175/VyS11.2.2020.9

Yamin, M. M., Katt, B. and Gkioulos, V. (2020). Cyber ranges and security testbeds: Scenarios, functions, tools and architecture. *Computers & Security*, *88*, 101636. https://doi.org/10.1016/j.cose.2019.101636

Zimmermann, V. and Renaud, K. (2019). Moving from a 'human-as-problem" to a 'human-as-solution" cybersecurity mindset. *International Journal of Human-Computer Studies*, *131*, 169–187. https://doi.org/10.1016/j.ijhcs.2019.05.005

Rol de Contribución	Autor (es)
Conceptualización	Holzen Atocha Martínez García (principal).
Metodología	Holzen Atocha Martínez García (principal).
Instalación de Software	Holzen Atocha Martínez García (principal).
Validación	Holzen Atocha Martínez García (principal). Enrique Camacho Pérez (igual). Ligia Beatriz Chuc Us (igual).
Análisis Formal	Holzen Atocha Martínez García (principal).
Investigación	Holzen Atocha Martínez García (igual). Enrique Camacho Pérez (igual). Ligia Beatriz Chuc Us (igual).
Recursos	Holzen Atocha Martínez García (igual). Enrique Camacho Pérez (igual).
Curación de datos	Enrique Camacho Pérez (igual). Ligia Beatriz Chuc Us (igual).
Escritura - Preparación del borrador original	Holzen Atocha Martínez García (principal).
Escritura - Revisión y edición	Holzen Atocha Martínez García (principal). Enrique Camacho Pérez (igual)
Visualización	Holzen Atocha Martínez García (igual). Enrique Camacho Pérez (igual).
Supervisión	Holzen Atocha Martínez García (principal). Edgar Alejandro Sagundo Duarte (que apoya).
Administración de Proyectos	Holzen Atocha Martínez García (principal).
Adquisición de fondos	Holzen Atocha Martínez García (principal). Enrique Camacho Pérez (igual). Ligia Beatriz Chuc Us (igual).