ISSN-L: 0798-1015 • eISSN: 2739-0071 (En línea)

https://doi.org/10.48082/espacios-a25v46n06p11

ARTÍCULO ORIGINAL

Implementación de un laboratorio de bajo costo para el desarrollo de prácticas de ciberseguridad

Implementation of a low-cost laboratory for the development of cybersecurity practices

Oscar D. MORENO [1]
Enrique AYALA [2]

[1] Universidad Autónoma de Yucatán. México. daniel.m0r3n0fl@gmail.com
[2] Universidad Autónoma de Yucatán. México. enrique.ayala@correo.uady.mx

RESUMEN

Este trabajo describe la implementación de un laboratorio de ciberseguridad empleando recursos de bajo costo en la Universidad Autónoma de Yucatán, México. El diseño de las actividades estuvo basado en un ambiente lúdico de tipo Captura la Bandera. Los resultados muestran mayor motivación y aceptación del entorno. La discusión destaca la relevancia de innovaciones para mejorar las destrezas de ciberdefensa, cruciales en nuestros días. En conclusión, el aprendizaje activo es efectivo para fomentar las habilidades de ciberseguridad.

Palabras clave: ciberseguridad, aprendizaje activo, captura la bandera, contenedores

ABSTRACT

This paper describes the implementation of a cybersecurity laboratory using low-cost resources at the Autonomous University of Yucatán, México. The activities were designed based on a playful Capture the Flag-type environment. The results show greater motivation and acceptance of the environment. The discussion highlights the relevance of innovations to improve cyber defense skills, which are crucial in today's world. In conclusion, active learning is effective in fostering cybersecurity skills.

Key words: cybersecurity, active learning, capture the flag, containers

Recibido: 26/08/2025
Aprobado: 16/10/2025
Publicado: 30/11/2025

1. INTRODUCCIÓN

La ciberseguridad es un concepto que ha tomado mayor relevancia en los últimos años, debido al impacto que tienen las amenazas e incidentes de seguridad en la vida de la gente y a la frecuencia con que se presentan en nuestros días. El tema despierta interés en el ámbito tecnológico y académico, pues se reconoce la necesidad de contar con especialistas preparados para un mundo lleno de retos en el ámbito digital y que está en constante evolución. Los profesionistas en ciberseguridad tienen una gran responsabilidad pues de ellos depende la continuidad de los procesos basados en la tecnología digital al hacer aplicar sus conocimientos en el aseguramiento de la información y sistemas, en beneficio del bien común en general.

La sociedad utiliza sistemas digitales en todos los ámbitos de la vida diaria, sin embargo, estos pueden estar vulnerables ante los diversos tipos de ciberataques que ponen en riesgo la información sensible de los usuarios y la operación de empresas e instituciones (World Economic Forum [WEF], 2024). Estos ataques suelen representar pérdidas millonarias por lo que se vuelve un tema de interés para los afectados el hecho de evitar que sucedan estos eventos; considerando lo anterior, se observa la necesidad de contar con profesionales preparados para responder ante eventuales incidentes de seguridad de manera oportuna y establecer medidas adecuadas de protección de la información de los usuarios.

1.1. Antecedentes

En el ámbito internacional han existido diversos esfuerzos para preparar en temas de ciberseguridad a las nuevas generaciones de profesionistas. Por ejemplo, existe el marco de trabajo NICE que significa National Initiative on Cybersecurity Education (Iniciativa Nacional para la Educación en Ciberseguridad), el cual es un programa liderado por el NIST (National Institute of Standards and Technology) de Estados Unidos que busca desarrollar, promover y mantener un marco de referencia para la educación, capacitación y desarrollo de la fuerza laboral en ciberseguridad (Petersen *et al*., 2023). Lo cual supone una forma de alinear y poder cumplir la demanda de las empresas para obtener estudiantes con conocimientos en ciberseguridad listos para trabajar.

Una experiencia basada en el marco de trabajo NICE es la desarrollada por Pattanayak *et al*. (2022) en la cual elaboraron un entorno de laboratorio llamado CYOTEE (Cybersecurity Oriented Training Enviroment and Exercises). Este entorno está compuesto de varias máquinas virtuales, las cuales incluyen un servidor de correos, un servidor de archivos, un servicio DNS y un servidor web. Con las actividades diseñadas para el laboratorio se logró preparar a los alumnos y fortalecer sus competencias en ciberdefensa.

En este sentido, de Resende *et al*. (2020) en su propuesta hacen uso de un marco de trabajo alineado con el estándar ACM/IEEE CE2017 para fomentar el conocimiento en temas de seguridad y redes; mediante el aprendizaje en laboratorios de ciberseguridad, se hace un énfasis en actividades prácticas y algunas clases teóricas como introducción a los temas que se enseñarán. Asimismo, se mencionan actividades como accesos remotos a dispositivos en la red, crear un punto de acceso WIFI o manipular el ancho de banda de una red, por mencionar algunos casos de actividades.

Las herramientas y sistemas especializadas son elementos centrales en el despliegue de laboratorios de ciberseguridad, en el caso del trabajo de Karagiannis et al. (2020) se estudia el estado del arte sobre el diseño de ejercicios de ciberseguridad y compara las herramientas utilizadas en estos laboratorios, resaltando las ventajas y desventajas de virtualización, así como el uso de contenedores para temas de seguridad. Este tema se profundiza en el artículo de Karagiannis et al. (2021) en donde se describe una plataforma llamada PocketCTF que busca reducir los tiempos y recursos necesarios para ejecutar ejercicios prácticos de ciberseguridad, realizan pruebas y comparaciones con el uso de contenedores en lugar de tecnologías de virtualización para desplegar los laboratorios. Además, en el trabajo de Chingo y Gómez (2020) se busca caracterizar el uso de contenedores para la educación de la ciberseguridad, concluyendo que una de las principales razones de utilizar contenedores es la optimización de recursos, además de una mayor escalabilidad y flexibilidad.

En el ámbito local, en la Península de Yucatán están surgiendo iniciativas en las que se puede observar un interés por implementar entornos que permitan desarrollar habilidades en temas de ciberseguridad y temas afines, como es el caso del trabajo de Martinez-García et al. (2023) en donde se realiza una

propuesta de diseño de un laboratorio de Hacking Ético para el Tecnológico Nacional de México campus Progreso, en el cual se destaca el uso de dispositivos Raspberry-Pi para tener una implementación que se consideraría de bajo costo.

Por otro lado, un aspecto importante que se ha popularizado en los Laboratorios de Ciberseguridad es la gamificación de los ejercicios. Kim *et al*. (2023) explican el proceso de aplicar esta estrategia didáctica a las prácticas por desarrollar en procesos de enseñanza o capacitación; el enfoque de su trabajo es principalmente pedagógico, en él se muestran los principios para convertir ejercicios de laboratorios tradicionales a laboratorios gamificados, considerando aspectos de planeación de actividades y recursos requeridos. De igual forma, Kebande (2024) resalta el aprendizaje activo como un elemento relevante en el diseño de actividades para desarrollar en los laboratorios, este enfoque permite que los alumnos puedan llegar a soluciones por su propia cuenta, lo cual impacta positivamente el proceso de aprendizaje.

Otras iniciativas en este sentido son las propuestas de Prinetto *et al*. (2020) quienes describieron ejercicios para laboratorios, pero de captura la bandera (CTF, del inglés Capture de Flag) basados en hardware, lo cual es un tipo de ejercicios de CTF que no es muy común. Por otro lado, el artículo de Alexander *et al*. (2021) da un enfoque que describe más el ámbito del aprendizaje en sí, mencionando principios para poder realizar ejercicios de laboratorios prácticos que puedan ser aprovechados por los alumnos al retener su atención y fomentar la resolución de problemas y en el caso de Kerr y Hynninen (2023) tomaron un enfoque sobre phishing y spoofing, los cuales ayudan a que los alumnos tomen conciencia sobre la seguridad en línea.

1.2. Justificación

El presente trabajo tiene como propósito implementar un laboratorio de ciberseguridad, para el desarrollo de prácticas por parte del alumnado, con elementos y herramientas de libre acceso o bajo costo. A través del análisis de su implementación se busca identificar sus fortaleza y debilidades, de manera que pueda servir como una experiencia inicial en el diseño de estrategias educativas innovadoras y enriquecedoras que promuevan el desarrollo de habilidades de ciberseguridad en los alumnos de educación superior, alineadas a las expectativas de la industria y la sociedad.

Para lograr un aprendizaje duradero y significativo, es necesario considerar expectativas, conocimientos y experiencias previas de los estudiantes; adicionalmente, el entorno de aprendizaje es fundamental para facilitar la interacción de los estudiantes y dotarlos de un ambiente realista en el que puedan practicar y desarrollar habilidades tanto técnicas como sociales (Acosta, 2025; Díaz y Hernández, 2010). En este sentido, los laboratorios virtuales siguen un enfoque de aprendizaje activo y están alineados con los principios de la teoría constructivista, ya que dotan a los estudiantes con los elementos para realizar actividades prácticas y obtener experiencias que promueven la construcción de su conocimiento, además de facilitar la interacción entre los participantes, fomentando habilidades sociales, críticas y de resolución de problemas en temas de ciberseguridad (Kebande, 2024).

Con los resultados esperados se contará con información valiosa para sustentar la planificación de actividades de aprendizaje más efectivas, así como la adopción de nuevos enfoques pedagógicos basados en metodologías activas que hagan uso de una infraestructura tecnológica de bajo costo, disponible en la mayoría de las instituciones educativas, para el desarrollo de actividades en el laboratorio de ciberseguridad.

2. METODOLOGÍA

Esta investigación emplea un enfoque mixto, considerando aspectos cuantitativos como cualitativos, específicamente usa un diseño descriptivo debido a que se busca caracterizar las condiciones de implementación del laboratorio de ciberseguridad y registrar la percepción por parte de los usuarios en términos de su motivación e interés (Creswell, 2014; Hernández et al., 2014). Incluye datos recuperados de una encuesta *ad hoc* y algunas reflexiones personales de los usuarios del laboratorio.

El trabajo se realizó siguiendo los pasos indicados en la figura 1, en la que se resumen las principales actividades que permitieron el despliegue del laboratorio de ciberseguridad. El primer paso fue la recopilación de información sobre sistemas, herramientas y actividades, lo cual permitió identificar las características deseables del laboratorio de ciberseguridad. A partir de estos elementos, se continuó con el diseño lógico y físico del laboratorio, con lo cual se estuvo en la posibilidad de realizar la configuración

física de los dispositivos de red, de estaciones de trabajo y de servidores. Una vez verificado el funcionamiento de las comunicaciones en red, se realizó la instalación de servicios típicos de red, así como de plataformas para la gestión y realización ejercicios prácticos de ciberseguridad. Se continuó con el diseño y selección de los ejercicios que serían desarrollados por los estudiantes, para en seguida realizar una revisión y prueba de los escenarios planificados. Finalmente, se desplegó el laboratorio en dos sesiones prácticas y se recopilaron las opiniones de los estudiantes mediante una encuesta, cuyos datos serían analizados e interpretada con el fin de obtener conclusiones y reflexionar sobre los resultados alcanzados.

Figura 1 Etapas del proceso de implementación del laboratorio de ciberseguridad

La población considerada fueron los estudiantes de la Facultad de Matemáticas de la Universidad Autónoma de Yucatán. La muestra, de tipo no probabilístico y de tipo intencional, se seleccionó mediante dos criterios: 1) Formar parte de la asignatura de Redes y Seguridad de Computadoras y 2) Mostrar interés en temas de ciberseguridad, con algún conocimiento básico en ciberseguridad, esto debido a la necesidad de trabajar con participantes que tuvieran las bases suficientes para interactuar con computadoras, servidores y sistemas de redes. En total se obtuvieron 18 encuestas de alumnos matriculados en el período agosto-diciembre de 2024.

Para la recopilación de datos sobre la opinión de los alumnos, se diseñó una encuesta adaptada a partir de instrumentos previamente elaborados por Chi *et al*. (2022) y Konstantinou (2020), la cual fue aplicada después de la realización de las prácticas de laboratorio planificadas, lo cual permitió analizar la motivación y el interés del alumnado después de probar el laboratorio. La encuesta se elaboró en Microsoft *Forms* y estuvo compuestas de diez ítems con opciones de respuesta en escala de Likert de cinco puntos. Con las opciones típicas: 1) Totalmente en desacuerdo, 2) En desacuerdo, 3) Ni de acuerdo ni en desacuerdo, 4) De acuerdo y 5) Totalmente de acuerdo. Asimismo, se incluyeron dos preguntas abiertas para ampliar y flexibilizar la retroalimentación de los alumnos. Se cuidó el manejo de los datos sensibles, respetando los principios éticos del manejo de información establecidos por la universidad.

Para verificar la consistencia del instrumento se calculó el Alfa de Cronbach para los grupos de ítems en las dimensiones indicadas: 1) Claridad y organización: 0.8234, 2) Promoción de habilidades: 0.6203 y 3) Relevancia pedagógica: 0.7576. Las dimensiones 1 y 3 presentan buena consistencia, mientras que la dimensión 2 es moderada.

Para el análisis de los datos recolectados se calcularon estadísticas descriptivas de la muestra. También, se analizaron las respuestas de las preguntas abiertas para identificar elementos del entorno desarrollado que tuvieran influencia en la docencia empleando el laboratorio. Finalmente, se buscó la triangulación de los métodos para verificar la congruencia de sus resultados.

2.1. Descripción del laboratorio

El laboratorio ya contaba con computadoras y varios equipos de redes, se adaptó el espacio para ciberseguridad mediante la incorporación de equipos recuperados de otras áreas de la facultad e instalando software y sistemas de libre distribución y con bajos requerimientos de recursos. En la figura 2 se puede observar la topología física del laboratorio de ciberseguridad y redes de computadoras. Esencialmente el espacio contiene 30 computadoras de escritorio, 10 enrutadores, 12 conmutadores y 2 enrutadores inalámbricos. Se realizó el cableado para contar con una topología fija para acceso vía cable y se configuraron dos redes inalámbricas para acceso de equipos móviles. En el espacio dedicado a

ciberseguridad se ubicaron dos gabinetes para colocar los equipos inalámbricos, conmutadores y servidores, todos estos equipos fueron recuperados de otras áreas en donde ya no se les daba uso.

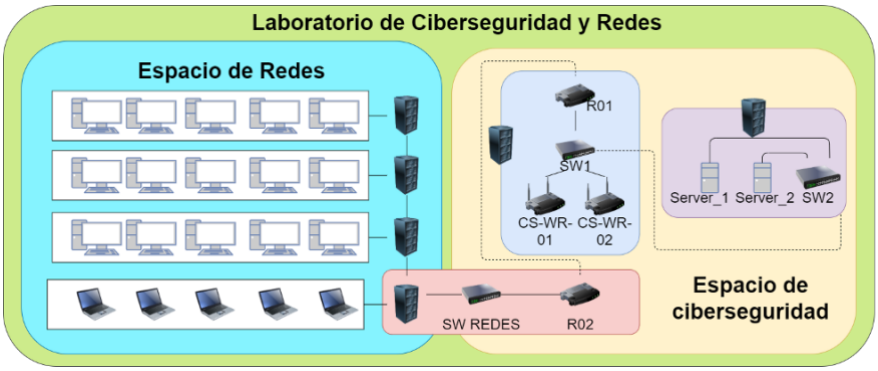

Figura 2 Topología física del laboratorio de ciberseguridad y redes

Con respecto a los servicios que ofrece el laboratorio de ciberseguridad, la figura 3 muestra dos servidores. El servidor 1 ejecuta Kali Linux versión 2024.3 y se encarga de albergar las instancias correspondientes a los ejercicios de explotación de vulnerabilidades con ayuda de la página web de OWASP Juice Shop como entorno en el cual se desarrollarán los ejercicios, este sitio está diseñado con varios tipos de vulnerabilidades que deben ser encontradas por los alumnos, a manera de retos. Adicionalmente, el servidor integra CTFd la cual es una aplicación que funciona como una plataforma mediante la cual el profesor gestiona las actividades y visualiza el progreso de los alumnos, facilitando la evaluación de su desempeño. También, en esta plataforma los alumnos acceden a la descripción de las actividades y van registrando su progresión.

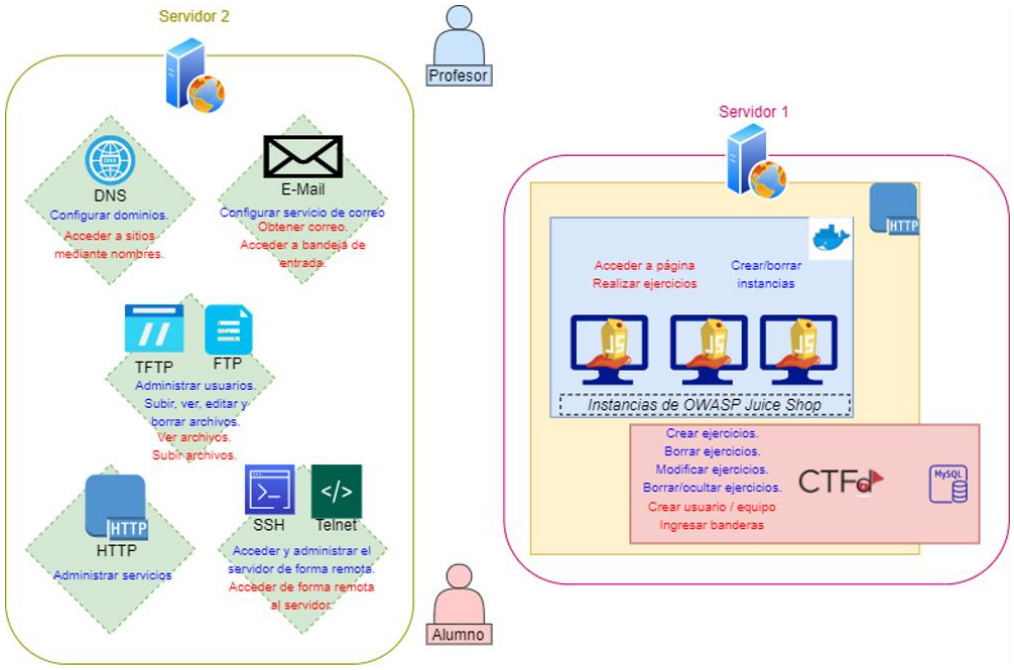

Figura 3 Arquitectura del laboratorio y sus servicios

El servidor 2 tiene instalado el sistema operativo Lubuntu versión 16.04.3 LTS, una distribución ligera de Linux. Se encarga de ejecutar distintos servicios esenciales de redes que permiten la integración del laboratorio de ciberseguridad en actividades prácticas, ya sea dando credenciales para acceder de forma remota al servidor con SSH y Telnet, o permitiendo a los alumnos utilizar los servicios para transferencia de archivos como FTP y TFTP. Además, el servidor 2 proporciona al laboratorio la opción de acceder al servicio de CTFd mediante la resolución de nombres (DNS), y acceder a los ejercicios mediante un correo proporcionado por el servicio de E-Mail el cual ayuda a replicar escenarios profesionales para poder aplicar la teoría en un entorno real. En conjunto ambos servidores se complementan para poder optimizar la

utilización de recursos y proporcionar una mayor flexibilidad en caso de requerirse una actualización o mejora de los servicios proporcionados.

2.2. Descripción de las actividades prácticas

Para probar el uso del laboratorio se planificaron dos actividades prácticas. El experimento se llevó a cabo a lo largo de dos sesiones de clase, las cuales acumularon cuatro horas en total del experimento. La primera sesión, relacionada con temas de redes de computadoras y servicios, aterrizó conceptos vistos en las clases teóricas sobre acceso inalámbrico seguro, creación y manejo de usuarios, transferencia de archivos, accesibilidad mediante nombres de dominio, generación y uso de cuentas de correo, acceso remoto seguro y no seguro, acceso a páginas web seguras y no seguras. Para esta actividad se utilizaron varios de los servicios instalados en el Servidor 2. En la misma sesión se dio a conocer las instrucciones de lo que se espera de la actividad y se entregaron credenciales a los alumnos para poder acceder a los servicios. Dadas las características de los participantes, se dio por sentado que tenían los conocimientos necesarios para poder llevar a cabo las actividades, por lo que el involucramiento del instructor para guiar a los alumnos fue mínimo.

Para la segunda sesión se les indicó a los participantes que ingresaran a la plataforma de CTFd, en la cual se encontraban 10 ejercicios seleccionados para que los alumnos intentaran resolver en el tiempo disponible. Los ejercicios versan sobre explotación de vulnerabilidades en el sitio web de OWASP Juice Shop, previamente preparado en el laboratorio. Cada reto contaba con instrucciones detalladas para poder obtener la bandera, por lo que simplemente se les tuvo que mostrar cómo encontrar la página de inicio de OWASP Juice Shop y dejarlos trabajar de forma libre, incluso podían asociarse con sus compañeros. A lo largo de la sesión se estuvo presente en caso de que el alumnado tuviera alguna duda o se tuviera que hacer resolver alguna situación relacionada con el servidor, la red o las instancias de la plataforma de práctica.

Concluidas las actividades, en una sesión posterior, se les indicó el enlace para contestar el instrumento de retroalimentación y se registraron las respuestas.

3. RESULTADOS Y DISCUSIÓN

Se presentan los resultados del trabajo desarrollado, en relación con las opiniones de los usuarios del laboratorio de ciberseguridad recabadas mediante la encuesta. Las preguntas se agruparon en tres grupos o dimensiones para facilitar el análisis posterior.

- Claridad y organización:
  1) Las instrucciones de las actividades fueron preparadas correctamente.
  2) Reconocí qué es lo que se espera que se realice en el laboratorio.
  3) Entiendo el propósito del laboratorio.
- Promoción de habilidades:
  4) El laboratorio promueve el pensamiento crítico y la resolución de práctica de problemas.
  5) Las actividades del laboratorio fueron interesantes.
  6) El contenido del laboratorio me motiva a dar mi esfuerzo en la resolución de ejercicios.
- Relevancia pedagógica:
  7) El laboratorio refuerza temas relacionados a lo aprendido en clases.
  8) El contenido del laboratorio hace crecer mi conocimiento en temas de ciberseguridad.
  9) El contenido del laboratorio despierta mi curiosidad sobre temas de ciberseguridad.
  10) El contenido del laboratorio me ayuda a aprender nuevas técnicas relacionadas con ciberseguridad.

En total se obtuvieron 18 respuestas de los participantes, que incluyeron las 10 preguntas de opción múltiple y las 2 preguntas abiertas, que en conjunto reflejan la percepción de los estudiantes en las dimensiones evaluadas y ofrecen una visión sobre el uso y beneficios de este entorno tecnológico para el desarrollo de habilidades de ciberseguridad.

En la tabla 1 podemos observar un análisis con las medidas de tendencia central y de dispersión relevantes en las dimensiones evaluadas. En general se tiene una media de las tres dimensiones de 4.76, es decir, la mayoría de las respuestas corresponden al sentimiento de "Totalmente de acuerdo". También se observa que la mediana y la moda es de 5 en las dimensiones Promoción de habilidades y Relevancia

pedagógica, con una desviación estándar de 0.34 y 0.30 que indican una variabilidad baja, y la mediana de Claridad y organización es de 4.83 con una media es de 4.62 y una desviación estándar de 0.45, es decir, es la dimensión en la que se observa una variabilidad moderada. En general, los valores obtenidos sugieren una alta satisfacción de los participantes con el entorno, sin embargo, para la dimensión de Claridad y organización es importante prestar atención a las respuestas de las preguntas 1) Las instrucciones de las actividades fueron preparadas correctamente y 2) Reconocí qué es lo que se espera que se realice en el laboratorio, pues puede haber áreas de mejora con respecto a la claridad de las instrucciones proporcionadas, lo cual pudo haber tenido un impacto en la motivación del alumnado al no tener claro el propósito buscado en la actividad. Las tres dimensiones recibieron valoraciones muy positivas, en especial Relevancia pedagógica, lo cual sugiere que los participantes consideran al laboratorio altamente relevante pedagógicamente y promotor de habilidades de ciberseguridad.

Tabla 1 Estadísticos descriptivos por cada dimensión del estudio

Estadístico	Claridad y organización	Promoción de habilidades	Relevancia pedagógica
Media	4.62962963	4.777777778	4.875
Error típico	0.107418676	0.080845208	0.070739557
Mediana	4.833333333	5	5
Moda	5	5	5
Desviación estándar	0.455738844	0.34299717	0.300122524
Varianza de la muestra	0.207697894	0.117647059	0.090073529
Curtosis	-0.666461685	1.222530864	4.262390671
Coeficiente de asimetría	-0.864397229	-1.498230695	-2.294981066
Rango	1.333333333	1	1
Mínimo	3.666666667	4	4
Máximo	5	5	5
Suma	83.33333333	86	87.75
Cuenta	18	18	18
Nivel de confianza (95.0%)	0.226633595	0.17056848	0.14924742

Con respecto a las dos preguntas abiertas de retroalimentación se solicitó a los alumnos expresar sus opiniones sobre su experiencia utilizando el laboratorio de ciberseguridad, realizándose su análisis y codificación temática.

La primera pregunta abierta fue la siguiente: Describe cuáles fueron los mejores aspectos del laboratorio de ciberseguridad. En el gráfico 1 se resumen los principales comentarios asociados a esta pregunta. Podemos ver que el Enfoque práctico y didáctico tuvo un 31% de menciones, la Plataforma CTFd y gamificación un 24% y Recursos y entorno un 15%, lo que refleja la aceptación de las herramientas implementadas para la realización de las prácticas. En menor medidas, la Dinámica motivacional y competitividad, el Rol del docente y la Colaboración y autonomía fueron aspectos que se identificaron como positivos por parte de los alumnos. Con mayor énfasis en la disponibilidad del entorno y el enfoque práctico, pero dando margen de mejora en el diseño pedagógico, en general los comentarios indican el interés y la utilidad del laboratorio.

Por otro lado, en la segunda pregunta abierta se pidió que indicaran aspectos que podrían implementarse para mejorar el uso del laboratorio: Describe cambios que se podrían implementar para mejorar la experiencia del laboratorio de ciberseguridad.

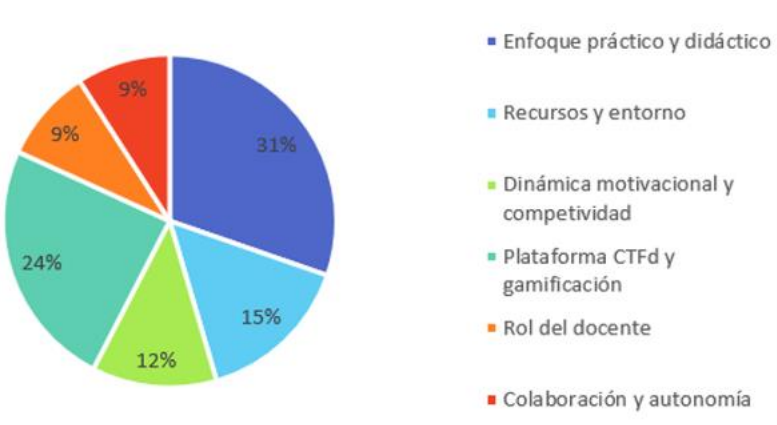

Gráfico 1 Aspectos positivos del laboratorio de ciberseguridad

Cómo se observa en el gráfico 2, el tema Equipos y recursos tuvo un 55% de menciones, en el que los encuestados sugieren mejorar en algunos elementos de los equipos o de los recursos con los que cuenta el laboratorio de ciberseguridad. Esto es esperado y lógico, dado que los recursos empleados son de bajo costo con algunas limitaciones en cuando a rendimiento y capacidad de memoria, por ejemplo, se presentaron algunas dificultades debido al tráfico de red cuando se conectaron de manera simultánea todos los alumnos del grupo. El entorno fue muy bien recibido, sin embargo, presenta aspectos que se podrían mejorar al emplear equipos con mejores características. Por otro lado, un 25% de los encuestados considera relevante que se mejore la Claridad y la gestión de las sesiones desarrolladas, particularmente en algunos aspectos de las explicaciones, la claridad de las instrucciones o el tiempo empleado para realizar las actividades. A pesar de que existen varias respuestas que mencionan que no se necesitan hacer cambios, si es necesario priorizar los dos temas anteriores para poder tener una mejor experiencia al momento de utilizar el laboratorio de ciberseguridad.

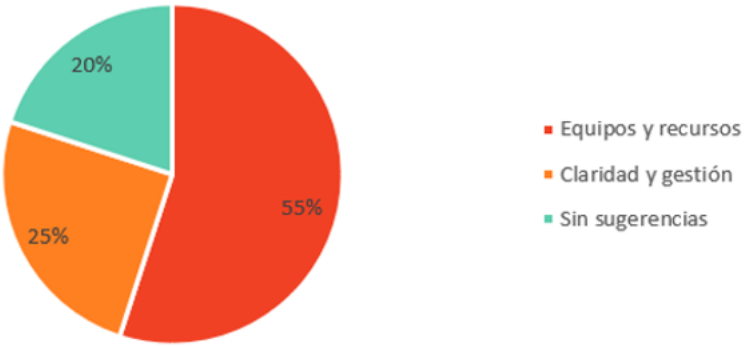

Gráfico 2 Aspectos a mejorar en el laboratorio de ciberseguridad

3.1. Discusión

Se tuvieron valoraciones muy positivas en las preguntas cerradas, sin embargo, también hubo bastantes sugerencias de mejora del laboratorio. Este contraste puede reflejar que los alumnos valoran el esfuerzo y la oportunidad de trabajar en un entorno realista para el desarrollo de prácticas de redes y ciberseguridad, a pesar de que las condiciones de operación aún presentan algunas áreas de mejora.

Algunas limitaciones que afectaron el rendimiento fueron fallos de los servidores debido a alta demanda de los usuarios, en relación con los recursos disponibles, así como la alta latencia de los enrutadores inalámbricos, por lo cual se recomienda que el diseño de las actividades se apegue a las capacidades máximas de los equipos.

Al comparar los resultados obtenidos en los trabajos Chi *et al*. (2022) y de Konstantinou (2020) se puede notar que igual hubo una buena recepción por parte del alumnado al presentarse un conjunto de ejercicios prácticos que permitieron el desarrollo de habilidades y un mayor interés por temas relacionados de ciberseguridad, como también se afirma en el trabajo de Kebande (2024), al considerar las estrategias

de aprendizaje activo como elemento clave en el aprendizaje de los alumnos al resolver ejercicios de ciberseguridad por su propia cuenta.

Entre las similitudes encontradas de la implementación del laboratorio con respecto a trabajos previos, se puede observar coincidencias con los hallazgos de Pattanayak *et al*. (2022) en el uso de servicios como correos, archivos, DNS y web. Particularmente, el trabajo de Karagiannis et al. (2020) destaca el uso de contenedores con Docker para mejorar aspectos de utilización de recursos del sistema, misma estrategia empleada en este trabajo.

4. CONCLUSIONES

Tomando en cuenta los resultados alcanzados, podemos considerar que se logró el objetivo de implementar un laboratorio de ciberseguridad empleando para ello software de libre acceso y recursos de bajo costo; además, los ejercicios propuestos pudieron realizarse considerando un mínimo de requisitos para desplegarlo. Su uso también fue exitoso, al ser integrado en la enseñanza de temas de ciberseguridad y redes, basado en el diseño de actividades que permitieron un aprendizaje significativo y práctico, esto a pesar de las limitaciones inherente consideradas en su diseño, el presupuesto y los equipos disponibles.

Entre los principales resultados de este trabajo se destaca:

1. La ejecución de un laboratorio de ciberseguridad con equipos de bajo costo, demostrando qué equipos considerados obsoletos en otras áreas pueden ser utilizados para realizar prácticas significativas al ofrecer experiencias realistas de trabajo.

2. La implementación de servidores como entornos de prácticas de ciberseguridad y redes, con herramientas de código abierto, accesibles y convenientes para su transferencia a proyectos similares en otras instituciones.

3. El diseño de ejercicios tomando en cuenta aspectos del aprendizaje activo y lúdico, con retos por resolver, corroborando su eficacia para despertar el interés de los alumnos, en temas relacionados con ciberseguridad.

Basado en los productos de este trabajo y los comentarios de retroalimentación, se identificaron aspectos a mejorar en un trabajo futuro para el laboratorio de ciberseguridad. Por ejemplo, una mayor automatización del despliegue de las instancias de contenedores en los servidores, para hacer más eficiente la realización de los ejercicios para los alumnos. Asimismo, se considera apropiado integrar nuevas actividades o variaciones de las ya existentes, procurando una mayor sencillez y claridad en instrucciones y contenidos, así como optimizar el tiempo de dedicación a las sesiones de prácticas.

Criterios éticos y transparencia

Este artículo cumple con los criterios éticos y de transparencia en la investigación. Todos los procedimientos realizados cuidaron la protección de la confidencialidad de los datos y no existen conflictos de interés. También, se declara que no se utilizaron herramientas de Inteligencia Artificial (IA) en la conceptualización, redacción, análisis de datos o revisión del manuscrito. El contenido es exclusivamente resultado del trabajo intelectual y crítico de los autores.

REFERENCIAS BIBLIOGRÁFICAS

Acosta Haro, S. (2025). Uso de un laboratorio virtual de automatización industrial y su relación con la actitud hacia el aprendizaje de estudiante de ingeniería. *Tecnología, Ciencia y Educación, 32*. https://doi.org/10.51302/tce.2025.24325

Alexander, C., Ma, L., Cai, Z., & Cheng, W. (2021). Eureka Labs: Enhancing Cybersecurity Education through Inquiry-based Hands-on Activities. *2021 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Internet of People and Smart City Innovation* (SmartWorld/SCALCOM/UIC/ATC/IOP/SCI), 552–557. https://doi.org/10.1109/SWC50871.2021.00082

Chi, H., Liu, J., Xu, W., Peng, M., & DeGoicoechea, J. (2022). Design Hands-on Lab Exercises for Cyber-physical Systems Security Education. *Journal of The Colloquium for Information Systems Security Education, 9*(1), 8. https://doi.org/10.53735/cisse.v9i1.140

Chingo, R. A., & Gómez, O. S. (2020). Tecnología de contenedores y su aplicación en el aprendizaje de ciberseguridad: una revisión sistemática de literatura. ReCIBE. *Revista Electrónica de Computación, Informática, Biomédica y Electrónica, 9*(2), 1–20. https://www.redalyc.org/articulo.oa?id=512267931004

Creswell, J. (2014). Research design: Qualitative, quantitative, and mixed methods approaches (4th ed.). SAGE Publications

de Resende, H. C., Slamnik-Krijestorac, N., Both, C. B., & Marquez-Barja, J. (2020). Introducing Engineering Undergraduate Students to Network Management Techniques: A Hands-on approach using the Citylab Smart City. 2020 IEEE Global Engineering Education Conference (EDUCON), 1316–1324. https://doi.org/10.1109/EDUCON45650.2020.9125159

Díaz Barriga Arceo, F. & Hernández Rojas, G. (2010). Estrategias docentes para un aprendizaje significativo (3.ª ed.). McGraw-Hill.

Hernández, R., Fernández, C., & Baptista, M. (2014). *Metodología de la investigación*. McGraw-Hill.

Karagiannis, S., Magkos, E., Ntantogian, C., & Ribeiro, L. (2020). Computer Security (I. Boureanu, C. C. Drăgan, M. Manulis, T. Giannetsos, C. Dadoyan, P. Gouvas, R. A. Hallman, S. Li, V. Chang, F. Pallas, J. Pohle, & A. Sasse, Eds.; Vol. 12580). Springer International Publishing. https://doi.org/10.1007/978-3-030-66504-3

Karagiannis, S., Ntantogian, C., Magkos, E., Ribeiro, L. L., & Campos, L. (2021). PocketCTF: A Fully Featured Approach for Hosting Portable Attack and Defense Cybersecurity Exercises. *Information*, 12(8), 318. https://doi.org/10.3390/info12080318

Kebande, V. R. (2024). The Impact of Virtual Laboratories on Active Learning and Engagement in Cybersecurity Distance Education. http://arxiv.org/abs/2404.04952

Kerr, A., & Hynninen, T. (2023). Towards Improving Online Security Awareness Skills with Phishing and Spoofing Labs. *2023 46th MIPRO ICT and Electronics Convention (MIPRO),* 1225–1229. https://doi.org/10.23919/MIPRO57284.2023.10159861

Kim, J. B., Zhong, C., & Liu, H. (2023). Teaching Tip: What You Need to Know about Gamification Process of Cybersecurity Hands-on Lab Exercises: Lessons and Challenges. Journal of Information Systems Education, 34(4), 387-405. https://jise.org/Volume34/n4/JISE2023v34n4pp387-405.html

Konstantinou, C. (2020). Cyber-Physical Systems Security Education Through Hands-on Lab Exercises. *IEEE Design & Test, 37*(6), 47–55. https://doi.org/10.1109/MDAT.2020.3005365

Martínez-García, H. A., Camacho-Pérez, E., Chuc-Us, L. B., & Sagundo-Duarte, E. A. (2023). Propuesta de arquitectura de laboratorio de hacking ético portátil basada en hardware de bajo costo para el aprendizaje en ciberseguridad. *Revista El Centro de Graduados e Investigación. Instituto Tecnológico de Mérida*, 38(98), 01–04.

Pattanayak, A., Steiner, S., & Conte De Leon, D. (2022). *Hands-on Educational Labs for Cyber Defense Competition Training*. https://github.com/CenterForSecureAndDependableSystems/

Petersen, R., Santos, D., Wetzel, K., Smith, M., & Witte, G. (2020) Workforce Framework for Cybersecurity (NICE Framework). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-181, Rev. 1. https://doi.org/10.6028/NIST.SP.800-181r1

Prinetto, P., Roascio, G., & Varriale, A. (2020). Hardware-based Capture-The-Flag Challenges. *2020 IEEE East-West Design & Test Symposium (EWDTS)*, 1–8. https://doi.org/10.1109/EWDTS50664.2020.9224932

World Economic Forum [WEF] (2024). *The Global Risks Report 2024*. Recuperado de: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf