Cuaderno de Pedagogía Universitaria

El impacto de *TryHackMe* en la enseñanza de la cátedra de Ciberseguridad

The Impact of TryHackMe on the Teaching of the Cybersecurity Course

Rafael Miguel Dorville Collado[a]
Carlos Camacho[b]
Pablo Domínguez[c]
José Aníbal Rosa[d]
[a,b,c,d] Pontificia Universidad Católica Madre y Maestra, Santo Domingo, República Dominicana.

Autor de correspondencia: rm.dorville@ce.pucmm.edu.do

Resumen

La enseñanza de la ciberseguridad en educación superior requiere experiencias formativas capaces de articular teoría, práctica y reflexión en contextos seguros y controlados. En la Escuela de Ingeniería en Computación y Telecomunicaciones (EICT) de la Pontificia Universidad Católica Madre y Maestra (PUCMM), la incorporación de la plataforma *TryHackMe* desde enero de 2024 buscó fortalecer la docencia en la cátedra de Ciberseguridad mediante laboratorios virtuales, retos guiados y simulaciones progresivas. En este sentido, el presente artículo ofrece un relato de experiencia que documenta el proceso de implementación, la estrategia diseñada para su integración curricular, los mecanismos de evaluación y las acciones motivacionales destinadas a fomentar el aprendizaje activo. Desde un enfoque centrado en el estudiantado, se lograron avances en la adquisición de competencias técnicas, la participación en torneos tipo *Capture The Flag* y la consolidación de una cultura de práctica continua. Además, se destacan las certificaciones obtenidas por el cuerpo docente y el reconocimiento institucional como factores que consolidaron el valor pedagógico del proyecto. Finalmente, se propone un modelo replicable de innovación educativa en el ámbito de la ciberseguridad universitaria.

Palabras clave: ciberseguridad, educación superior, aprendizaje activo, gamificación, innovación pedagógica, TryHackMe

ISSN (en línea): 1814-4152 / Sitio web: **http://cuaderno.pucmm.edu.do**
CÓMO CITAR: Dorville, R., Camacho, C., Domínguez, P. y Rosa, J. (2026). El impacto de TryHackMe en la enseñanza de la cátedra de Ciberseguridad. *Cuaderno de Pedagogía Universitaria, 23,* e711.

Abstract

The teaching of cybersecurity in higher education requires learning experiences that combine theory, practice, and reflection within safe and controlled environments. At the School of Computing and Telecommunications Engineering (EICT) of the Pontificia Universidad Católica Madre y Maestra (PUCMM), the integration of the TryHackMe platform since January 2024 has aimed to strengthen cybersecurity instruction through virtual labs, guided challenges, and progressive simulations. In this context, this article presents an experience report documenting the implementation process, curricular integration methodology, assessment mechanisms, and motivational strategies used to foster active learning. Through a student-centered approach, progress was achieved in developing technical competencies, participating in Capture The Flag tournaments, and building a culture of continuous practice. In addition, faculty certifications and institutional recognition are highlighted as key factors that reinforced the pedagogical value of the project. Finally, the lessons learned and sustainability challenges are discussed, offering a replicable model of educational innovation in university-level cybersecurity.

Keywords: *cybersecurity, higher education, active learning, gamification, pedagogical innovation, TryHackMe*

Introducción

La formación en ciberseguridad constituye una prioridad estratégica para las instituciones de educación superior que buscan responder a las demandas del contexto tecnológico actual. En un entorno global marcado por la digitalización acelerada y el incremento de las amenazas informáticas, las universidades enfrentan el desafío de preparar a un profesional capaz de anticipar vulnerabilidades, mitigar riesgos y gestionar incidentes de seguridad de manera ética y efectiva. Este reto implica cerrar la brecha señalada en la literatura entre los conocimientos teóricos impartidos y las habilidades prácticas que demanda la industria (Hentea, 2021; Beuran et al., 2020; Hall & Allen, 2022).

Este problema de aprendizaje se manifiesta cuando el estudiantado evidencia dificultades para trasladar el contenido técnico a escenarios auténticos, interpretar fallas de seguridad o realizar análisis de incidentes con autonomía (Beuran et al., 2020). Por esta razón, resulta indispensable adoptar estrategias pedagógicas que integren práctica guiada, simulación y retroalimentación inmediata, lo que favorece un aprendizaje activo y contextualizado (Cruz y González, 2023; Prince, 2004; Freeman et al., 2014).

En tal sentido, la Pontificia Universidad Católica Madre y Maestra (PUCMM), a través de la Escuela de Ingeniería en Computación y Telecomunicaciones (EICT), ha impulsado la integración de la plataforma TryHackMe en la cátedra de Ciberseguridad —iniciada en enero de 2024—. Se trata de una plataforma en línea diseñada para el entrenamiento en ciberseguridad mediante laboratorios guiados, simulaciones y retos de tipo *Capture The Flag (CTF)*, los cuales permiten al estudiante asumir el rol de analista, atacante o defensor en entornos controlados y gamificados, lo que ha demostrado incrementar la motivación y

participación estudiantil (Alotaibi y Almagwashi, 2023; Deterding et al., 2011; Chothia et al., 2022).

Antes de su adopción, los ejercicios prácticos se realizaban en entornos locales, con máquinas virtuales preconfiguradas, lo que dificultaba la reproducción de incidentes complejos y el seguimiento del progreso de los estudiantes. En este contexto, TryHackMe ofrece una alternativa pedagógica más flexible, accesible y alineada con las tendencias internacionales de la enseñanza en ciberseguridad (Beuran et al., 2020; Alotaibi y Almagwashi, 2023) que ha sido utilizada con resultados positivos en el desempeño técnico, la autogestión y las competencias colaborativas (Hall & Allen, 2022; Jovanovic & Popovic, 2020). Su modelo permite desarrollar competencias técnicas mientras se fortalecen habilidades transversales como el pensamiento crítico, la resolución de problemas y la colaboración.

Desde su implementación, la experiencia ha involucrado a estudiantes de tres asignaturas del área: Seguridad en Tecnologías de la Información, Hacking Ético y Ciberseguridad y Protección de Sistemas. Cada cuatrimestre participan entre 20 y 30 estudiantes por grupo, bajo la coordinación de docentes que actúan como facilitadores del proceso de aprendizaje. El uso de licencias institucionales con esquemas de rotación garantizó la participación equitativa y promovió la gestión responsable del tiempo y los recursos.

La presente propuesta pedagógica se justifica en su contribución a la formación profesional orientada a la práctica y responde a la necesidad de preparar talento altamente competente para enfrentar escenarios reales de seguridad digital dentro y fuera del país. A este respecto, el objetivo de este artículo consiste en describir la experiencia de integración de la plataforma *TryHackMe* en la cátedra de Ciberseguridad de la PUCMM, con énfasis en su impacto en el aprendizaje, la motivación y el desarrollo de competencias técnicas y transversales en el estudiantado.

En tal sentido, este artículo constituye un relato de experiencia que sistematiza los aprendizajes obtenidos a lo largo de cinco cuatrimestres de implementación. En los siguientes apartados se detallan las fases de diseño, ejecución y seguimiento académico, junto con los criterios utilizados para asegurar la coherencia entre los objetivos formativos y las actividades implementadas. Asimismo, se analizan las estrategias metodológicas que orientaron la propuesta, la articulación entre teoría y práctica, las certificaciones docentes obtenidas por el profesorado y la validación institucional del proceso.

De este modo, se busca aportar una reflexión fundamentada sobre el potencial de las plataformas virtuales de entrenamiento en ciberseguridad como herramientas pedagógicas en la educación superior. Asimismo, se muestra cómo la integración de recursos tecnológicos, el acompañamiento docente y el aprendizaje activo pueden contribuir a la formación de profesionales más competentes y comprometidos con la seguridad digital.

Metodología

La experiencia pedagógica se basa en el modelo de investigación-acción, sustentado en la sistematización de un proceso de innovación docente orientado a integrar entornos virtuales

de práctica en la enseñanza de la ciberseguridad. El diseño metodológico se fundamentó en el análisis reflexivo de la práctica pedagógica, al considerar la experiencia docente como fuente principal de generación de conocimiento educativo.

Por un lado, la estrategia metodológica se estructuró en tres momentos: diagnóstico inicial, implementación pedagógica y sistematización de resultados. A partir de la incorporación de *TryHackMe*, cada fase fue diseñada con el propósito de comprender los cambios producidos en los procesos de aprendizaje, la participación estudiantil y el desarrollo de habilidades técnicas y transversales. Por otra parte, la recolección de información se realizó a través de múltiples fuentes cualitativas, dentro de las cuales se incluyeron la observación directa en sesiones prácticas, el análisis de informes técnicos elaborados por el estudiantado, la revisión de bitácoras de seguimiento docente y la aplicación de cuestionarios de percepción al finalizar cada período académico.

Finalmente, el proceso de análisis se desarrolló mediante la categorización temática de los registros, que consistió en organizar la información en dimensiones relacionadas con: desempeño técnico, niveles de autonomía, calidad de la documentación elaborada por los estudiantes, interacción colaborativa y actitudes frente al aprendizaje práctico. Estas permitieron estructurar de manera sistemática la interpretación de los hallazgos.

Instrumentos de evaluación

Para la valoración del desempeño del estudiantado durante la implementación de la plataforma TryHackMe, se definieron tres instrumentos principales: una rúbrica analítica de evaluación de laboratorios, una bitácora estructurada de seguimiento docente y un cuestionario mixto de percepción estudiantil. Estos instrumentos fueron seleccionados por su coherencia con el enfoque por competencias y por permitir una valoración integral del proceso formativo en sus dimensiones cognitivas, procedimentales y actitudinales.

La rúbrica analítica se aplicó de forma individual y grupal a los productos de laboratorio. Asimismo, se mantuvo alineada con los resultados de aprendizaje de las asignaturas de Ciberseguridad y contempló criterios de dominio técnico, análisis y documentación, resolución de problemas, gestión del tiempo y trabajo colaborativo. Este instrumento permitió valorar el producto final y, al mismo tiempo, reconocer el proceso de aprendizaje desarrollado por el estudiantado.

La bitácora de seguimiento docente se utilizó como instrumento de observación sistemática durante cada sesión práctica. En ella se registraron aspectos relacionados con la participación, el nivel de autonomía, las dificultades técnicas recurrentes, las interacciones colaborativas y las estrategias de resolución aplicadas. Su aplicación semanal permitió documentar la dinámica del aula en los entornos virtuales de práctica.

En el mismo orden, el cuestionario de percepción estudiantil fue de carácter mixto e incorporó preguntas cerradas tipo escala de valoración y preguntas abiertas orientadas a recoger opiniones cualitativas sobre la experiencia formativa. Se administró al finalizar cada periodo académico con el fin de conocer la valoración de los estudiantes sobre el uso de la plataforma, el acompañamiento docente y el impacto percibido en su aprendizaje.

Diagnóstico inicial

Antes de la incorporación de la plataforma TryHackMe, se realizó un proceso de caracterización diagnóstica con el propósito de identificar el nivel de preparación de los estudiantes en relación con el uso de entornos virtuales de práctica en ciberseguridad. Este diagnóstico se desarrolló al inicio de cada cuatrimestre y combinó técnicas de observación en aula, revisión de productos académicos previos y aplicación de cuestionarios abiertos. Los hallazgos evidenciaron que la mayoría del estudiantado poseía una comprensión conceptual adecuada de los principios básicos de seguridad informática, redes y sistemas operativos.

Sin embargo, se identificaron limitaciones significativas en la aplicación de estos conocimientos, especialmente en la identificación de vulnerabilidades, el análisis de tráfico de red y la gestión de incidentes simulados. Asimismo, se constató que el grupo presentaba escasa familiaridad con plataformas de entrenamiento en ciberseguridad y una experiencia limitada en la elaboración de informes técnicos estructurados. Este escenario confirmó la necesidad de implementar entornos virtuales de práctica como estrategia pedagógica para fortalecer la articulación entre teoría y aplicación.

Desarrollo de la experiencia

El proceso de integración de la plataforma *TryHackMe* en la cátedra de Ciberseguridad de la PUCMM se enmarca en una estrategia institucional orientada a fortalecer la enseñanza práctica en áreas críticas de la ingeniería y la tecnología. Desde sus inicios, el propósito central consistió en promover un aprendizaje experiencial, en el que el estudiantado pudiera asumir un rol activo en la construcción del conocimiento y aplicar los conceptos teóricos en situaciones simuladas que reprodujeran la complejidad de los entornos profesionales, conforme a los principios del aprendizaje activo y basado en la experiencia (Kolb, 1984; Bonwell & Eison, 1991).

La decisión de incorporar una herramienta de entrenamiento como *TryHackMe* surgió de la identificación de una necesidad concreta: los laboratorios tradicionales, basados en entornos locales o configuraciones individuales, limitan la capacidad del alumnado para experimentar escenarios de ataque y defensa en red, además de que generan dificultades logísticas y de mantenimiento. Esta situación evidenció un problema de aprendizaje asociado a la falta de entornos auténticos que permitieran poner en práctica los conocimientos de seguridad en sistemas, redes y gestión de vulnerabilidades.

La experiencia se desarrolló bajo la coordinación de un equipo docente con formación especializada en ciberseguridad, integrado por profesores de la Escuela de Ingeniería en Computación y Telecomunicaciones (EICT). La planificación contempló la articulación entre los contenidos curriculares y las competencias específicas del área, con lo cual se aseguró que cada práctica respondiera a un objetivo formativo claramente definido. En este sentido, la integración de *TryHackMe* no se limitó a la ejecución de laboratorios, sino que implicó la revisión de las estrategias de enseñanza, los criterios de evaluación y los mecanismos de acompañamiento estudiantil. La planificación del proceso se estructuró en tres fases que

abarcaron cinco cuatrimestres consecutivos de implementación, como se muestra en la Tabla 1.

Tabla 1

Planificación y ejecución de la experiencia pedagógica

Fase	Duración aproximada	Actividades principales	Resultados esperados
Planificación y diseño	1 mes	Selección de laboratorios por nivel de complejidad, definición de competencias, elaboración del cronograma rotativo de licencias y ajustes en los instrumentos de evaluación.	Alineación de actividades con el plan de estudios y los resultados de aprendizaje de las tres asignaturas.
Implementación guiada	2 meses	Desarrollo de laboratorios introductorios y ejercicios intermedios en aulas, acompañamiento docente y documentación reflexiva de los procesos.	Adquisición de destrezas técnicas y fortalecimiento de la autogestión.
Consolidación y cierre	Último mes del cuatrimestre	Ejecución de retos avanzados y torneos tipo CTF, elaboración de informes técnicos y evaluación integral.	Demostración de competencias técnicas, trabajo colaborativo y pensamiento crítico.

Durante las primeras etapas, se adoptó un enfoque de aprendizaje sustentado en teorías constructivistas que destacan el papel del alumnado como agente de su propio proceso de aprendizaje (Vygotsky, 1978; Kolb, 1984). Desde esta perspectiva, el aprendizaje significativo ocurre cuando se participa de manera práctica, reflexiva y colaborativa en la resolución de problemas reales o simulados (Romero y Barberà, 2021). Bajo este marco teórico, se debe demostrar no solo el dominio técnico, sino también la capacidad de análisis, documentación y resolución de problemas.

Así, el estudiantado fue organizado en parejas o pequeños equipos, con el objetivo de fomentar el trabajo conjunto en la resolución de problemas y el intercambio de conocimientos. Este modelo se reforzó con la organización de torneos internos tipo *Capture The Flag* (CTF), una dinámica de competencia ampliamente utilizada en la formación en ciberseguridad, donde los participantes deben resolver retos técnicos y capturar “banderas” digitales que validan cada logro. Estas actividades permitieron poner en práctica las habilidades adquiridas en un entorno controlado y promovieron la colaboración, la creatividad y la aplicación del conocimiento en contextos simulados. Además, el estudiantado elaboró informes técnicos con la siguiente estructura: a) descripción del escenario simulado; b) identificación de vulnerabilidades detectadas; c) herramientas utilizadas; d) evidencias técnicas (capturas, registros, salidas de comandos); e) análisis de impacto y f)

recomendaciones de mitigación.

Implementación

El proyecto comenzó con cuatro licencias institucionales, un número reducido para la cantidad de estudiantes por grupo (entre 20 y 30 por cuatrimestre). Esta limitación exigió un esquema de rotación cuidadosamente planificado:

- Cada usuario contó con un período específico de acceso, generalmente de una o dos semanas, durante el cual debía completar los laboratorios asignados.
- El equipo docente gestionó un calendario compartido, con lo cual se garantizó la equidad en la distribución del recurso y se supervisó el cumplimiento de las actividades.
- Se diseñó una escala de estimación centrada en el logro de competencias, de modo que, aun con tiempos limitados, cada estudiante pudiera demostrar progreso y dominio técnico.

El proceso de evaluación se estructuró mediante una rúbrica analítica basada en criterios técnicos y actitudinales, alineados con los resultados de aprendizaje de las asignaturas. Esta rúbrica permitió valorar de forma sistemática el desempeño de los estudiantes durante la ejecución de los laboratorios en TryHackMe, al considerar tanto la calidad de los procesos técnicos como las habilidades transversales desarrolladas durante la experiencia. En la Tabla 2 se presenta la estructura general utilizada para la valoración del desempeño.

Tabla 2

Estructura utilizada para la valoración del desempeño

Criterio de evaluación	Indicador	Ponderación
Dominio técnico	Identifica vulnerabilidades, ejecuta pruebas y aplica medidas correctivas adecuadas.	40 %
Análisis y documentación	Explica de forma clara los procedimientos, resultados y conclusiones del laboratorio.	25 %
Resolución de problemas	Aplica pensamiento crítico ante incidencias o errores técnicos.	15 %
Cumplimiento y gestión del tiempo	Realiza las actividades dentro del período asignado y evidencia organización.	10 %
Trabajo colaborativo y participación	Colabora en la resolución de retos grupales y contribuye al aprendizaje del equipo.	10 %

El modelo funcionó como proyecto piloto durante los cuatrimestres enero–abril y mayo–agosto de 2024, con la participación del estudiantado de las asignaturas *Seguridad en Tecnologías de la Información, Hacking Ético y Ciberseguridad y Protección de Sistemas*, pertenecientes a las carreras de Ingeniería en Telemática e Ingeniería en Ciencias de la Computación. En cada cuatrimestre hubo entre 20 y 30 participantes por grupo, que se distribuyeron en tres secciones académicas coordinadas por distintos profesores. Cada docente tuvo a su cargo un promedio de dos grupos, con apoyo técnico del personal de

laboratorio de la Escuela de Ingeniería en Computación y Telecomunicaciones (EICT).

Antes de la implementación, se aplicó un diagnóstico inicial que permitió identificar el nivel de familiaridad del alumnado con entornos virtuales de práctica y herramientas de ciberseguridad. Los resultados mostraron un dominio teórico adecuado, pero una experiencia limitada en la resolución práctica de incidentes, lo que reforzó la pertinencia de la estrategia. Tras comprobar su efectividad y alta aceptación, el número de licencias activas se amplió a ocho en el cuatrimestre septiembre–diciembre de 2024, lo que duplicó la capacidad de participación y redujo los tiempos de espera.

Complicaciones iniciales

Pese al entusiasmo general, la implementación enfrentó varios desafíos:

1. Limitación de recursos: el número inicial de licencias llevó a una logística intensiva en la planificación de turnos, seguimiento y rotación. Este aspecto demandó un esfuerzo adicional del profesorado y puso de manifiesto la importancia de una administración eficiente de los recursos tecnológicos.
2. Conectividad y ancho de banda: hubo quienes experimentaron dificultades al ejecutar las actividades técnicas desde sus hogares, especialmente en ejercicios que requerían conexiones estables o acceso remoto prolongado. En respuesta, se habilitaron sesiones guiadas en los laboratorios de la universidad con infraestructura garantizada.
3. Idioma de la plataforma: la mayoría de los contenidos de TryHackMe se encuentran en inglés, lo que representó una barrera inicial para una parte del alumnado. Sin embargo, esta dificultad se transformó en una oportunidad pedagógica que impulsó el fortalecimiento del vocabulario técnico en inglés y la lectura comprensiva de documentación especializada (Romero y Barberà, 2021).
4. Gestión del tiempo: la naturaleza de los retos requiere concentración y autonomía. Una parte del grupo subestimó el tiempo necesario para completar los laboratorios, lo que obligó a ajustar el cronograma e incorporar sesiones presenciales de acompañamiento.
5. Curva de aprendizaje docente: aunque la plataforma es intuitiva, el profesorado necesitó un período de familiarización para adaptar la estructura de los cursos, definir secuencias didácticas y vincular los resultados de la plataforma con los criterios de evaluación académica.

Resultados

La implementación sostenida de *TryHackMe* a lo largo de cinco períodos académicos consecutivos permitió recopilar una cantidad significativa de datos observacionales, informes técnicos y percepciones estudiantiles. Estos resultados fueron clasificados en tres dimensiones principales: desempeño técnico, motivación y compromiso y desarrollo de competencias transversales.

Desempeño técnico

El primer indicador de éxito fue la mejora en la ejecución de los laboratorios y la comprensión de los conceptos clave. En los primeros cuatrimestres, el estudiantado mostraba dificultades para completar los escenarios avanzados sin asistencia directa del docente; sin embargo, a partir del tercer período se observó una evolución significativa en la capacidad de los grupos para resolver los retos de forma autónoma.

Los informes técnicos evidenciaron una transición de descripciones superficiales hacia análisis estructurados, con uso de terminología especializada y una mejor interpretación de vulnerabilidades. Por ejemplo, mientras al inicio los reportes se limitaban a listar puertos abiertos o resultados de escaneo, en los últimos informes se documentaron vectores de ataque, impacto potencial y medidas de mitigación, lo que evidenció una comprensión más integral del ciclo de vulnerabilidad. Además, las evaluaciones prácticas mostraron un aumento promedio del 25 % en el desempeño técnico respecto a grupos previos sin acceso a la plataforma, junto con un mayor dominio de herramientas como Nmap, Burp Suite, Wireshark y Metasploit (véase Tabla 3).

Motivación y compromiso

La naturaleza gamificada de *TryHackMe*, con niveles, insignias y progresión visible, funcionó como un estímulo extrínseco, mientras que la satisfacción de resolver desafíos complejos fortaleció la motivación intrínseca (Alotaibi y Almagwashi, 2023). De igual manera, las encuestas aplicadas al cierre de cada cuatrimestre reflejaron una valoración promedio de 4.8/5 sobre satisfacción general y los comentarios destacaron el valor del aprendizaje práctico y la conexión con escenarios reales. Este resultado se complementó con observaciones docentes que evidenciaron una mejora sostenida en la asistencia, la colaboración y la discusión técnica en foros académicos.

Asimismo, el uso de la plataforma fomentó la participación fuera del horario formal de clase, lo que demostró un compromiso académico que trascendió el espacio tradicional del aula (Tabla 4). El equipo docente observó que los grupos con mejor desempeño no necesariamente eran los más experimentados, sino aquellos que mostraban mayor disposición al aprendizaje colaborativo, lo que coincide con investigaciones previas sobre entornos gamificados (Chothia et al., 2022) (véase Tabla 4).

Competencias transversales

Más allá del componente técnico, la experiencia con TryHackMe contribuyó de manera significativa al desarrollo de competencias transversales. En cuanto al pensamiento crítico,

el estudiantado participó en la resolución de incidentes simulados que requerían identificar causas raíz, proponer contramedidas y justificar técnicamente sus decisiones. Estas tareas fueron evaluadas mediante rúbricas con indicadores de análisis, argumentación y coherencia.

Por otra parte, la comunicación técnica se fortaleció mediante exposiciones orales y la entrega de reportes formales revisados por pares y docentes, en los que se valoró la precisión terminológica y la capacidad para explicar procedimientos y resultados. En términos de autonomía y autogestión, el sistema de retos progresivos promovió la planificación independiente y el cumplimiento responsable de las tareas en los tiempos establecidos.

Finalmente, la ética profesional fue trabajada a través de simulaciones que implicaron la toma de decisiones ante vulneraciones de seguridad, con lo que se fomentó la reflexión crítica sobre el uso responsable del conocimiento técnico en contextos reales (véase Tabla 5).

Tabla 3

Desempeño técnico

Dimensión evaluada	**Situación inicial observada**	**Evolución durante la implementación**	**Evidencias recopiladas**
Identificación de vulnerabilidades	Dificultad para reconocer patrones de ataque	Mayor precisión en el análisis de escenarios simulados	Informes técnicos de laboratorio
Uso de herramientas de análisis	Uso básico de herramientas de escaneo	Aplicación autónoma de herramientas como Nmap, Wireshark y Metasploit	Registros de laboratorio
Dimensión evaluada	**Situación inicial observada**	**Evolución durante la implementación**	**Evidencias recopiladas**
Interpretación de resultados	Interpretaciones descriptivas	Análisis críticos con justificación técnica	Reportes técnicos estructurados

Tabla 4

Motivación y participación

Indicador	**Situación inicial**	**Evolución observada**	**Fuente de evidencia**
Participación en laboratorios	Baja participación autónoma	Incremento sostenido de la participación	Registros de asistencia
Interacción entre pares	Escasa colaboración	Trabajo colaborativo frecuente	Observaciones docentes
Persistencia ante dificultades	Alta dependencia del docente	Mayor autonomía en la resolución de retos	Bitácoras de seguimiento

Tabla 5

Desarrollo de habilidades transversales

Habilidad	**Evidencia inicial**	**Cambio observado**	**Instrumentos de registro**
Pensamiento crítico	Resoluciones guiadas	Argumentación técnica propia	Informes técnicos

Habilidad	Evidencia inicial	Cambio observado	Instrumentos de registro
Comunicación técnica	Documentación superficial	Informes estructurados y claros	Rúbricas de evaluación
Autogestión	Baja planificación	Organización independiente del trabajo	Bitácoras de seguimiento y rúbricas de evaluación

Caso 1. Evolución individual en el desarrollo de competencias técnicas

Durante las primeras semanas de implementación, se identificó un estudiante con dificultades para interpretar los resultados de escaneos de red y reconocer servicios expuestos en los escenarios simulados. En las primeras prácticas, sus reportes se limitaban a descripciones generales sin análisis técnico profundo. A medida que avanzó el proceso formativo y se fortaleció el acompañamiento docente, este estudiante logró identificar vulnerabilidades básicas asociadas a configuraciones inseguras, documentar hallazgos con evidencias técnicas y proponer medidas elementales de mitigación, lo que evidencia una evolución significativa en su desempeño técnico y en su capacidad de análisis.

Caso 2. Evolución grupal y trabajo colaborativo en entornos virtuales de práctica

Se observó también la evolución de un equipo de trabajo que, al inicio de la experiencia, dependía de manera constante de la mediación del docente para ejecutar los laboratorios. Durante las primeras sesiones, el grupo presentaba dificultades para la organización de tareas, la interpretación de instrucciones técnicas y la elaboración de informes estructurados. Al cierre del proceso, este equipo fue capaz de ejecutar de forma autónoma simulaciones de ataques básicos, distribuir funciones de trabajo entre sus integrantes y elaborar informes técnicos completos con evidencias, análisis de impacto y recomendaciones. Estos resultados reflejan avances en autonomía, comunicación técnica y trabajo colaborativo.

Discusión

Los resultados sistematizados evidenciaron patrones consistentes de mejora en el desempeño del estudiantado, tanto en el dominio de habilidades técnicas como en el desarrollo de capacidades cognitivas y actitudinales. El análisis de los informes mostró una evolución progresiva en la profundidad de razonamiento, la precisión en la identificación de vulnerabilidades y la calidad de las propuestas de mitigación. De igual forma, las bitácoras docentes registraron un aumento sostenido de la autonomía y una reducción gradual de la dependencia de la guía directa del profesorado.

Los hallazgos obtenidos confirman que la integración de la plataforma TryHackMe fortaleció el aprendizaje técnico y el desarrollo de competencias transversales, lo que concuerda con estudios previos que destacan el valor del aprendizaje activo en entornos virtuales de ciberseguridad (Beuran et al., 2020; Alotaibi y Almagwashi, 2023). En particular, los resultados muestran que el uso de laboratorios guiados, con desafíos progresivos y componentes de gamificación promovió la autonomía, la colaboración y la motivación

intrínseca del alumnado, aspectos que se consideran esenciales en el marco del aprendizaje experiencial y situado (Kolb, 1984; Lave y Wenger, 1991).

Desde una perspectiva pedagógica, la experiencia se alinea con el enfoque por competencias, el cual busca integrar conocimientos, habilidades y actitudes para resolver problemas reales en contextos simulados. En este marco, la propuesta didáctica promovió el desarrollo de capacidades para el análisis de vulnerabilidades, la toma de decisiones fundamentadas, la comunicación técnica y la autorregulación del aprendizaje. De igual modo, la plataforma permitió que el grupo asumiera un rol activo en la resolución de incidentes de seguridad al transitar de una práctica centrada en la instrucción hacia un aprendizaje mediado por la acción, la reflexión y la autoevaluación. Este modelo de enseñanza-aprendizaje ha sido ampliamente documentado en la literatura como uno de los más eficaces para favorecer la empleabilidad y la transferencia del conocimiento técnico al ámbito profesional (Biggs y Tang, 2011; Salas-Rueda, 2022).

Asimismo, la incorporación de estrategias de gamificación favoreció la persistencia del estudiantado y la reducción de la brecha entre teoría y práctica. La retroalimentación inmediata, los sistemas de logros y la progresión visible reforzaron la motivación intrínseca y el aprendizaje autorregulado, coherente con lo planteado por Deterding et al. (2011) sobre la aplicación de mecánicas de juego en entornos educativos. Estos resultados son consistentes con los reportes de Hall y Allen (2022) y Chothia et al. (2022), quienes señalan mejoras en la retención del conocimiento y la participación al incorporar dinámicas competitivas controladas en la enseñanza de ciberseguridad.

Por otro lado, la experiencia docente evidenció el potencial de la resolución de problemas como estrategia formativa, al situar al alumnado en contextos que requieren análisis crítico, toma de decisiones y aplicación práctica de la teoría. Esta aproximación refuerza el principio del aprendizaje situado, según el cual el conocimiento adquiere sentido cuando se construye dentro de una comunidad de práctica y bajo condiciones similares a las del entorno profesional (Lave y Wenger, 1991).

La experiencia de integración de *TryHackMe* en la cátedra de Ciberseguridad dejó múltiples aprendizajes que trascienden lo tecnológico. Más allá de incorporar una herramienta práctica, el proceso implicó repensar el modelo de enseñanza, las estrategias de acompañamiento y la manera en que se construye el conocimiento en el aula universitaria. Estas lecciones, fruto de la reflexión docente y del análisis del impacto obtenido, ofrecen orientaciones valiosas para futuras experiencias pedagógicas basadas en entornos virtuales de práctica:

1. **La tecnología no reemplaza la mediación docente**
   Aunque la plataforma promueve el autoaprendizaje, el acompañamiento docente sigue siendo insustituible. La orientación del profesorado permitió guiar la interpretación de resultados, resolver dudas técnicas y fomentar la reflexión ética sobre las acciones realizadas en los laboratorios. Los grupos que recibieron retroalimentación constante mostraron mejor desempeño y comprensión conceptual.

   Se reafirmó que la tecnología debe entenderse como un instrumento pedagógico y no como un fin en sí mismo. El rol del docente se transformó: de transmisor de información

a facilitador del aprendizaje, diseñador de experiencias y mentor académico. Este cambio fortaleció la interacción profesor–estudiante, con lo que se consolidó un entorno de aprendizaje colaborativo y significativo.

2. Las dificultades son oportunidades formativas

Durante la implementación surgieron barreras que inicialmente parecían limitantes, pero se convirtieron en oportunidades para desarrollar competencias transversales. Por ejemplo, el inglés técnico pasó de ser un obstáculo a una herramienta de crecimiento, pues ayudó a fortalecer la lectura comprensiva de documentación profesional. Por su parte, los retos de conectividad promovieron la planificación y el uso responsable de los recursos y las limitaciones de tiempo impulsaron la autogestión y el trabajo colaborativo. En conjunto, estas experiencias demostraron la importancia de enseñar al estudiantado a aprender en contextos inciertos, una habilidad esencial en ciberseguridad, donde la adaptabilidad es clave.

3. La evaluación formativa potencia la mejora continua

Un aprendizaje clave fue mover la evaluación del terreno de lo sumativo a lo formativo. El equipo docente implementó un sistema centrado en el proceso más que en el resultado, al valorar la capacidad de análisis, la calidad de la documentación y la reflexión crítica. Para lograrlo, se diseñaron escalas de estimación que permitieron dar seguimiento a la progresión de cada estudiante y se combinó la evaluación automática de la plataforma con la retroalimentación cualitativa del profesor. Esto favoreció el aprendizaje autorregulado y la toma de conciencia sobre los errores como parte del proceso formativo.

Desde la teoría, esta práctica responde al modelo de **evaluación formativa** en educación superior, que promueve la mejora continua y la autoevaluación como estrategias de aprendizaje significativo (Black y Wiliam, 2009; Boud y Molloy, 2013; López, 2011). De este modo, la retroalimentación se convirtió en un elemento pedagógico que no solo medía resultados, sino que impulsaba la reflexión, la revisión y la mejora permanente.

4. La motivación requiere visibilidad y propósito

La motivación del estudiantado no se sostuvo únicamente por la gamificación, sino también por el reconocimiento y la conexión con el futuro profesional. Al vincular los retos de TryHackMe con escenarios reales y mostrar su relación con certificaciones y roles laborales, se reforzó la percepción de utilidad del aprendizaje.

Esta articulación se enmarca en los principios del **aprendizaje situado**, según los cuales el conocimiento adquiere significado cuando se aplica en contextos auténticos (Lave y Wenger, 1991); y del **enfoque por competencias**, que busca integrar saberes técnicos, cognitivos y actitudinales orientados al desempeño profesional (Biggs y Tang, 2011). Asimismo, la visibilidad institucional del proyecto y su difusión en medios académicos reforzaron el sentido de pertenencia y orgullo, lo que resultó en el desarrollo de una motivación con propósito, más allá del entorno de clase.

La integración requiere visión institucional

Finalmente, la sostenibilidad de proyectos de este tipo depende de la articulación entre docentes, directivos e instituciones. El respaldo de la dirección, la inversión en licencias y la validación de las certificaciones fueron factores determinantes para consolidar el modelo. Esta sinergia no solo garantizó la continuidad, sino que abrió paso a un modelo replicable de innovación pedagógica con potencial de expansión hacia otras carreras.

En síntesis, las lecciones aprendidas muestran que la integración de herramientas digitales en la educación superior debe entenderse como un proceso sistémico, donde la tecnología, la pedagogía y la gestión académica convergen en un propósito común: formar profesionales competentes, autónomos y éticamente responsables. La experiencia con TryHackMe reafirmó que la enseñanza de la ciberseguridad trasciende el dominio técnico, mientras involucra la construcción de una cultura educativa basada en la práctica reflexiva, la colaboración y la mejora continua.

Conclusiones

Los resultados presentados muestran una mejora progresiva en el desempeño técnico, la motivación, la autonomía y el desarrollo de habilidades transversales del estudiantado. La sistematización de informes técnicos, bitácoras de seguimiento y cuestionarios de percepción permitió constatar que la integración de la plataforma *TryHackMe* favoreció de manera consistente la articulación entre los contenidos teóricos y la práctica en escenarios simulados propios de la ciberseguridad.

La experiencia de integrar *TryHackMe* en la cátedra de Ciberseguridad de la Pontificia Universidad Católica Madre y Maestra evidenció que la tecnología, cuando se articula con una planificación pedagógica sólida, puede transformar de manera profunda los procesos de enseñanza y aprendizaje en la educación superior. Este proyecto no se limitó a la implementación de una herramienta digital, sino que constituyó una innovación curricular y metodológica orientada al desarrollo de competencias técnicas, cognitivas y éticas en los futuros profesionales del área.

En primer lugar, se demostró que el aprendizaje activo basado en la práctica incrementa la motivación, la retención del conocimiento y la autonomía. Asimismo, el enfoque progresivo de laboratorios guiados hacia retos autónomos favoreció la construcción del conocimiento de manera gradual y contextualizada. En segundo lugar, la formación y certificación docente se consolidaron como elementos indispensables para garantizar la calidad del proceso. Los profesores no solo guiaron el aprendizaje, sino que también se certificaron en las mismas competencias que enseñaban, modelaron el aprendizaje continuo y fortalecieron la legitimidad del proyecto. Este aspecto constituye una práctica ejemplar de desarrollo profesional docente con impacto directo en la mejora de la enseñanza universitaria.

Por otro lado, el proceso ayudó a identificar desafíos que orientan líneas futuras de mejora. Entre ellos, la necesidad de ampliar el acceso a licencias institucionales, diversificar los recursos de apoyo para el estudiantado con menor dominio del inglés técnico y establecer mecanismos de evaluación interinstitucional con el fin de comparar datos entre cohortes.

Abordar estos aspectos será clave para garantizar la sostenibilidad y escalabilidad del modelo.

De cara al futuro, se proyecta la expansión del uso de *TryHackMe* hacia otras asignaturas del plan de estudios de Ingeniería en Computación y Telecomunicaciones, así como su integración en programas de posgrado y educación continua. Igualmente, se contempla desarrollar investigaciones pedagógicas que analicen el impacto longitudinal de la plataforma en el desempeño académico y la inserción profesional de los egresados.

Esta experiencia deja como legado un modelo replicable para la enseñanza universitaria en contextos tecnológicos, donde la práctica se convierte en motor del aprendizaje, la tecnología en aliada de la docencia y la reflexión en eje de la innovación. En un entorno global caracterizado por la constante evolución de las amenazas digitales, formar profesionales capaces de aprender, adaptarse y responder éticamente constituye no solo una meta académica, sino una responsabilidad social.

A partir de los resultados sistematizados en este estudio y de los casos documentados de evolución individual y grupal, se derivan las siguientes recomendaciones para futuras implementaciones en contextos universitarios que busquen fortalecer la enseñanza de la ciberseguridad mediante entornos virtuales de práctica:

- **Fortalecer la formación docente** en metodologías activas, evaluación formativa y uso pedagógico de plataformas tecnológicas, de modo que se asegure que el profesorado asuma el rol de mediador y diseñador de experiencias de aprendizaje.
- **Garantizar la sostenibilidad institucional** mediante la planificación de licencias, recursos y apoyo técnico continuo, para que el modelo continúe más allá de proyectos aislados.
- **Integrar la práctica virtual en el currículo** desde el diseño de asignaturas al alinear los laboratorios con las competencias y resultados de aprendizaje definidos en cada plan de estudios.
- **Sistematizar la evidencia pedagógica** y promover la investigación educativa y la publicación de experiencias, con el fin de consolidar una comunidad académica en torno a la innovación docente.
- **Fomentar la colaboración interinstitucional** para que el modelo pueda escalarse y adaptarse a otros contextos universitarios o programas técnicos en Latinoamérica.

En síntesis, la experiencia con *TryHackMe* demuestra que la convergencia entre tecnología, pedagogía y gestión académica puede generar un impacto transformador en la enseñanza superior. Esta convergencia contribuye a la consolidación de una educación más pertinente, práctica y humana.

Recibido: 1/10/2025 / **Revisado**: 14/10/2025 / **Aprobado:** 5/12/2025

Referencias bibliográficas

Alotaibi, A., & Almagwashi, H. (2023). Enhancing cybersecurity education through gamified learning platforms: A case study using TryHackMe. *International Journal of Computer Applications in Technology, 71*(1), 45–57. https://doi.org/10.1504/IJCAT.2023.127890

Beuran, R., Tang, D., & Chinen, K. (2020). Cybersecurity hands-on training: A case study using CyberRange and gamification. *IEEE Transactions on Education, 63*(4), 294–301. https://doi.org/10.1109/TE.2020.2983662

Biggs, J., & Tang, C. (2011). *Teaching for quality learning at university: What the student does* (4th ed.). McGraw-Hill Education.

Black, P., & Wiliam, D. (2009). Developing the theory of formative assessment. *Educational Assessment, Evaluation and Accountability, 21*(1), 5–31. https://doi.org/10.1007/s11092-008-9068-5

Bonwell, C., & Eison, J. (1991). *Active learning: Creating excitement in the classroom.* ASHE-ERIC Higher Education Reports. https://files.eric.ed.gov/fulltext/ED336049.pdf

Boud, D., & Molloy, E. (2013). Rethinking models of feedback for learning: The challenge of design. *Assessment & Evaluation in Higher Education, 38*(6), 698–712. https://doi.org/10.1080/02602938.2012.691462

Chothia, T., Novakovic, C., & Parker, R. (2022). Capture the Flag competitions: Motivating student engagement in cybersecurity. *Journal of Cybersecurity Education, Research and Practice*,(1), Article 2. https://digitalcommons.kennesaw.edu/jcerp/vol2022/iss1/2

Cruz, E. y González, J. (2023). Integración de entornos virtuales de práctica en la enseñanza universitaria de la ciberseguridad. *Revista Iberoamericana de Tecnología en Educación y Educación en Tecnología, 32*(2), 56–68. https://doi.org/10.24215/18509959e134

Deterding, S., Dixon, D., Khaled, R., & Nacke, L. (2011). From game design elements to gamefulness: Defining "gamification". In *Proceedings of the 15th International Academic MindTrek Conference: Envisioning Future Media Environments* (pp. 9–15). ACM. https://doi.org/10.1145/2181037.2181040

Freeman, S., Eddy, S. L., McDonough, M., Smith, M. K., Okoroafor, N., Jordt, H., & Wenderoth, M. P. (2014). Active learning increases student performance in science, engineering, and mathematics. *Psychological and Cognitive Sciences, 111*(23), 8410–8415. https://doi.org/10.1073/pnas.1319030111

Hall, J., & Allen, J. (2022). Building practical cybersecurity skills through simulated environments. *Journal of Information Security Education, 13*(3), 113–129. https://doi.org/10.5121/jise.2022.13306

Hentea, M. (2021). Perspectives on improving cybersecurity education. *Journal of Information Security, 12*(3), 177–192. https://doi.org/10.4236/jis.2021.123011

Jovanovic, J., & Popovic, S. (2020). Virtual labs in higher education: A systematic review. *Education and Information Technologies, 25*(6), 5791–5822. https://doi.org/10.1016/j.compedu.2016.01.015

Kolb, D. (1984). *Experiential learning: Experience as the source of learning and development.* Prentice Hall.

Lave, J., & Wenger, E. (1991). *Situated learning: Legitimate peripheral participation.* Cambridge University Press.

López, V. (2011). Evaluación formativa y compartida en educación superior: Propuestas, técnicas, instrumentos y experiencias. *Revista de Docencia Universitaria, 9*(1), 159–188. https://doi.org/10.4995/redu.2011.6180

Prince, M. (2004). Does active learning work? A review of the research. *Journal of Engineering Education, 93*(3), 223–231. https://doi.org/10.1002/j.2168-9830.2004.tb00809.x

Romero, M. y Barberà, E. (2021). Competencias digitales para la educación superior: Nuevos escenarios de enseñanza y aprendizaje. *Comunicar, 29*(66), 9–20. https://doi.org/10.3916/C66-2021-01

Salas-Rueda, R.-A. (2022). Gamificación y aprendizaje basado en problemas para la enseñanza universitaria: Análisis desde el enfoque por competencias. *Revista Electrónica de Investigación Educativa, 24*(2), e17. https://doi.org/10.24320/redie.2022.24.e17

Vygotsky, L. (1978). *Mind in society: The development of higher psychological processes.* Harvard University Press.