

**CAPACITACIÓN DOCENTE EN CIBERSEGURIDAD Y REDES INALÁMBRICAS
MEDIANTE UNA PLATAFORMA DIGITAL INTEGRADA
TEACHER TRAINING IN CYBERSECURITY AND WIRELESS NETWORKS THROUGH
AN INTEGRATED DIGITAL PLATFORM**

Autores: ¹Edison Javier Usca Paguay, ²Carlos Alberto Chacón Terán.

¹ORCID ID: <https://orcid.org/0009-0006-2691-8532>

²ORCID ID: <https://orcid.org/0009-0003-3939-9725>

¹E-mail de contacto: eusca@euroamericano.edu.ec

²E-mail de contacto: cchacon@euroamericano.edu.ec

Afiliación: ^{1*2}Instituto Superior Tecnológico EuroAmericano, (Ecuador).

Artículo recibido: 8 de Septiembre del 2026.

Artículo revisado: 15 de Septiembre del 2026.

Artículo aprobado: 15 de Septiembre del 2026.

¹Ingeniero en Sistemas Computacionales, graduado de la Universidad de Guayaquil, (Ecuador). Maestrante en Inteligencia Artificial Aplicada en la Universidad Internacional del Ecuador, (Ecuador), con 6 años de experiencia como Especialista en Sistemas de Mando y Control en la Armada del Ecuador.

²Ingeniero en Sistemas Computacionales, graduado de la Universidad de Guayaquil, (Ecuador). Máster Universitario en Diseño y Gestión de Proyectos Tecnológicos, graduado de la Universidad Internacional de La Rioja, (España). Docente investigador del Instituto Superior Tecnológico Universitario EuroAmericano, con 9 años de experiencia en Educación Superior.

Resumen

Formar docentes capaces de enseñar ciberseguridad y redes inalámbricas es una tarea que muchas instituciones tecnológicas dan por sentada, sin verificar realmente si el profesorado cuenta con las bases para hacerlo. Este estudio analiza la percepción docente sobre la necesidad y viabilidad de implementar un módulo de capacitación continua dentro de la plataforma digital institucional MODVS IV, en la carrera de Redes y Telecomunicaciones del Instituto Superior Tecnológico Universitario EuroAmericano. Se adoptó un enfoque mixto, con diseño no experimental y corte transversal, aplicando una encuesta estructurada a 6 docentes y una entrevista semiestructurada a 3 informantes clave: el vicerrector académico, el director de carrera y un consultor TIC. Los resultados muestran una alta aceptación del módulo propuesto, con un 83% de acuerdo en funcionalidades como el acceso a materiales, las simulaciones y el seguimiento del progreso. Sin embargo, solo la mitad de los docentes se siente preparada para abordar temas de ciberseguridad en sus asignaturas, mientras dos tercios demandan de forma explícita espacios institucionales de capacitación continua. Las entrevistas coinciden en que las principales brechas se concentran en tecnologías emergentes, ciberseguridad aplicada y la falta de entornos prácticos. Se concluye que, aunque

la aceptación de una plataforma digital integrada es mayoritaria, persiste una brecha formativa significativa que valida la pertinencia del módulo propuesto.

Palabras clave: Capacitación docente, Ciberseguridad, Redes inalámbricas, Plataforma digital, Educación superior.

Abstract

Training instructors capable of teaching cybersecurity and wireless networking is a task many technological institutions take for granted, without actually verifying whether the faculty has the necessary foundations. This study examines teacher perceptions regarding the need and feasibility of implementing a continuous training module within the institutional digital platform MODVS IV, in the Networking and Telecommunications program at Instituto Superior Tecnológico Universitario EuroAmericano. A mixed approach was adopted, with a non-experimental, cross-sectional design, applying a structured survey to 6 instructors and a semi-structured interview to 3 key informants: the academic vice-rector, the program director, and an IT consultant. Results show high acceptance of the proposed module, with 83% agreement on functionalities such as access to materials, simulations, and progress tracking. However, only half of the instructors feel prepared to address cybersecurity topics in

their courses, while two-thirds explicitly demand institutional spaces for continuous training. The interviews converge in identifying the main gaps in emerging technologies, applied cybersecurity, and the lack of practical environments. It is concluded that, although acceptance of an integrated digital platform is widespread, a significant training gap persists that validates the relevance of the proposed module.

Keywords: Teacher training, Cybersecurity, Wireless networks, Digital platform, Higher education.

Sumário

Formar docentes capazes de ensinar cibersegurança e redes sem fio é uma tarefa que muitas instituições tecnológicas dão por certa, sem verificar realmente se o corpo docente possui as bases necessárias. Este estudo analisa a percepção docente sobre a necessidade e a viabilidade de implementar um módulo de capacitação contínua dentro da plataforma digital institucional MODVS IV, no curso de Redes e Telecomunicações do Instituto Superior Tecnológico Universitario EuroAmericano. Adotou-se uma abordagem mista, com desenho não experimental e corte transversal, aplicando uma pesquisa estruturada a 6 docentes e uma entrevista semiestruturada a 3 informantes-chave: o vice-reitor acadêmico, o diretor de curso e um consultor de TIC. Os resultados mostram uma alta aceitação do módulo proposto, com 83% de concordância em funcionalidades como acesso a materiais, simulações e acompanhamento do progresso. No entanto, apenas metade dos docentes se sente preparada para abordar temas de cibersegurança em suas disciplinas, enquanto dois terços demandam explicitamente espaços institucionais de capacitação contínua. As entrevistas concordam que as principais lacunas se concentram em tecnologias emergentes, cibersegurança aplicada e falta de ambientes práticos. Conclui-se que, embora a aceitação de uma plataforma digital integrada seja majoritária, persiste uma lacuna formativa significativa que valida a pertinência do módulo proposto.

Palavras-chave: Capacitação docente, Cibersegurança, Redes sem fio, Plataforma digital, Ensino superior.

Introducción

La transformación digital en la educación superior ha impuesto nuevas exigencias a la formación docente, especialmente en áreas tecnológicas como la ciberseguridad y las redes inalámbricas. Estos campos del conocimiento se actualizan a gran velocidad, lo que demanda procesos formativos continuos y bien estructurados. Córdova et al. (2024) señalan que los entornos virtuales permiten organizar el desarrollo de competencias docentes mediante criterios de selección de contenidos, análisis de información y seguimiento académico sistemático. Moreno y Ayala (2025) sostienen que incorporar recursos tecnológicos de manera adecuada favorece tanto la comprensión conceptual como la aplicación del conocimiento dentro del proceso educativo, lo que subraya la importancia de no limitarse al uso instrumental de la tecnología, sino de integrarla con criterios pedagógicos claros. Sin embargo, en muchas instituciones persiste una formación docente heterogénea y limitada en áreas críticas como la seguridad de redes y la gestión de vulnerabilidades.

La seguridad de la información en entornos académicos ha sido objeto de diversos estudios. Chuqui y Orellana (2023), por ejemplo, identificaron que las bases de datos, los respaldos institucionales y los mecanismos de autenticación constituyen activos críticos que requieren controles adecuados. En esta misma línea, el análisis de vulnerabilidades se entiende como un proceso sistemático para identificar y priorizar debilidades dentro de los sistemas informáticos (Castillo y Ortiz, 2025). En el ámbito de las redes inalámbricas, la situación es similar. Cruz (2025) explica que implementar mecanismos de control de acceso resulta

determinante para garantizar la seguridad de los sistemas y prevenir accesos no autorizados. Estas evidencias revelan una brecha significativa entre las demandas del entorno tecnológico actual y las competencias disponibles en el profesorado de educación superior tecnológica.

Ecuador no ha sido ajeno a esta realidad. Diversas investigaciones nacionales han advertido sobre la necesidad de fortalecer las competencias digitales y de ciberseguridad en los docentes de institutos superiores y universidades. Un diagnóstico del Ministerio de Telecomunicaciones (2022) confirma que la formación en seguridad informática y redes continúa siendo una de las áreas con mayores déficits en el sector educativo ecuatoriano. Las plataformas digitales institucionales, como MODVS IV, ofrecen una oportunidad para centralizar y sistematizar la formación continua. Tamayo (2024) sostiene que las herramientas digitales integradas a entornos de aprendizaje contribuyen a mejorar la adopción y la calidad de los procesos formativos, siempre que exista un diseño metodológico claro y un enfoque institucional sostenido.

En el Instituto Superior Tecnológico Universitario EuroAmericano, la carrera de Redes y Telecomunicaciones enfrenta este desafío de manera directa. Los docentes requieren no solo competencias técnicas especializadas, sino también la capacidad de actualizarse continuamente. No obstante, no se cuenta con un diagnóstico sistemático sobre el nivel de preparación del profesorado en ciberseguridad y redes inalámbricas, ni se ha explorado la percepción docente sobre la utilidad de un espacio de formación continua integrado a la plataforma institucional MODVS IV. Por ello, el presente estudio se plantea como pregunta central de investigación: ¿una

plataforma digital integrada es la respuesta para la capacitación docente en ciberseguridad y redes inalámbricas? El objetivo general consiste en analizar la percepción docente sobre la necesidad y viabilidad de implementar un módulo de capacitación continua dentro de dicha plataforma. Específicamente, se busca identificar el nivel actual de conocimientos docentes, establecer las funcionalidades prioritarias del módulo, percibir el grado de aceptación hacia su implementación y verificar la relación entre el nivel de conocimiento y la necesidad de capacitación.

Materiales y Métodos

Se empleó un enfoque mixto que integró técnicas cuantitativas y cualitativas con el fin de examinar la percepción del profesorado acerca de la capacitación en ciberseguridad y redes inalámbricas. El estudio se inscribió en un diseño no experimental, dado que no se ejerció control ni manipulación intencionada de las variables, y de corte transversal, ya que la recolección de datos ocurrió en un solo momento. Esta estrategia metodológica permitió describir la realidad del cuerpo docente sin alterar su entorno habitual.

La población objeto de análisis correspondió a los profesores de la carrera de Redes y Telecomunicaciones del Instituto Superior Tecnológico Universitario EuroAmericano. La muestra cuantitativa estuvo integrada por 6 docentes, seleccionados mediante un muestreo no probabilístico por conveniencia, atendiendo a la accesibilidad y su vinculación directa con el área de estudio. No se recabaron datos sobre género ni rangos etarios, puesto que el interés del estudio se centró en las percepciones y competencias autodeclaradas por los participantes. En el componente cualitativo participaron tres informantes estratégicos: el director de la carrera de Redes y

Telecomunicaciones, con 3 años de experiencia en el cargo; el vicerrector académico de la institución, con 20 años de trayectoria en gestión educativa; y un consultor TIC independiente, con 22 años de trabajo en el sector tecnológico. La selección de estos actores respondió a su mirada estratégica, su conocimiento profundo de la problemática y su procedencia de ámbitos complementarios: el operativo, el institucional y el técnico especializado.

Para la obtención de datos cuantitativos se diseñó un cuestionario estructurado con escala Likert de cinco opciones (1 = totalmente en desacuerdo; 5 = totalmente de acuerdo). El instrumento se distribuyó en tres bloques: utilidad del módulo de capacitación propuesto (5 ítems), autopercepción de competencias actuales (4 ítems) y necesidades y expectativas de formación (3 ítems). Para la fase cualitativa se elaboró una guía de entrevista semiestructurada con preguntas abiertas dirigidas a diagnosticar el nivel de preparación docente, identificar competencias prioritarias, reconocer dificultades institucionales y valorar beneficios y funcionalidades deseables en una plataforma digital.

El trabajo de campo se organizó en fases sucesivas. Primero se realizó una contextualización del entorno académico y tecnológico institucional. Luego se diseñaron y validaron los instrumentos mediante revisión por pares. Durante enero de 2026 se aplicaron las encuestas de forma presencial a los 6 docentes, y en marzo del mismo año se realizaron las entrevistas a los tres informantes clave. Posteriormente se procesaron y analizaron los datos, se interpretaron los resultados y se formularon las conclusiones. Se redactó el informe y se socializaron los resultados. El procesamiento de los datos

cuantitativos consistió en un análisis descriptivo basado en frecuencias absolutas y relativas para cada reactivo, utilizando Microsoft Excel. El análisis cualitativo se realizó mediante la técnica de análisis de contenido temático, partiendo de la transcripción de las entrevistas, con procedimientos de codificación abierta, agrupación por categorías emergentes y síntesis interpretativa, aplicando triangulación entre los investigadores para asegurar la confiabilidad de los hallazgos. La investigación respetó los principios éticos establecidos. Todos los participantes recibieron información clara sobre los propósitos del estudio y otorgaron su consentimiento informado por escrito. La participación fue voluntaria y anónima, y se garantizó la confidencialidad de los datos. No se sometió a los participantes a riesgos físicos ni psicológicos, y la información recolectada se destinó exclusivamente a fines académicos.

Resultados y Discusión

Este bloque indagó la valoración docente acerca de las funcionalidades y beneficios de un módulo de capacitación en ciberseguridad y redes inalámbricas integrado a la plataforma MODVS IV. La tabla 1 evidencia que el consenso alcanzado por la gran mayoría del profesorado revela que se identifica valor agregado en la integración de un espacio formativo dentro de la plataforma institucional. Resulta llamativo, sin embargo, que una minoría se haya posicionado sistemáticamente en "totalmente en desacuerdo" en todos los ítems.

Este grupo, correspondiente al perfil con mayor especialización en redes y ciberseguridad, sugiere una posible resistencia a la estandarización de la formación continua o una preferencia por metodologías de actualización autogestionadas y no mediadas por la plataforma. Este hallazgo indica que incluso

una propuesta mayoritariamente bien valorada puede encontrar reparos entre los perfiles más especializados, lo que obliga a considerar

estrategias diferenciadas o flexibles para no generar rechazo en un sector del profesorado.

Tabla 1. *Percepción docente sobre la utilidad del módulo en MODVS IV.*

Ítem	Totalmente en desacuerdo	En desacuerdo	Ni acuerdo ni desacuerdo	De acuerdo	Totalmente de acuerdo
P1. Facilitaría el acceso a materiales	16,7%	0%	0%	0%	83,3%
P2. Actividades prácticas y simulaciones contribuirían al desarrollo de competencias	16,7%	0%	0%	0%	83,3%
P3. Los recursos formativos actualizarían conocimientos técnicos	16,7%	0%	0%	0%	83,3%
P4. Permitiría realizar seguimiento del avance docente	16,7%	0%	0%	0%	83,3%
P5. Facilitaría la organización y gestión de programas de formación	16,7%	0%	0%	0%	83,3%

Fuente: Elaboración propia.

Este bloque midió el nivel de preparación que los docentes declararon poseer en ciberseguridad y redes inalámbricas. En la tabla 2 mientras en el bloque I la aceptación del módulo era casi unánime, en el bloque II solo una parte del profesorado se siente preparado para abordar ciberseguridad en sus asignaturas o para identificar riesgos en redes. Esta brecha entre la valoración positiva de la herramienta y la autopercepción de competencias limitadas constituye el hallazgo central del estudio: los

docentes reconocen su déficit formativo y, al mismo tiempo, demandan un recurso institucional para superarlo. Un grupo considerable se ubicó en la categoría "ni de acuerdo ni en desacuerdo" en estos ítems, lo que puede interpretarse como inseguridad o falta de claridad metacognitiva sobre sus propias capacidades, un perfil que probablemente ha recibido formación básica sin sentirse competente para aplicarla en el aula.

Tabla 2. *Autopercepción de competencias actuales.*

Ítem	Totalmente en desacuerdo	En desacuerdo	Ni acuerdo ni desacuerdo	De acuerdo	Totalmente de acuerdo
P6. Preparación para abordar ciberseguridad en asignaturas	16,7%	0%	33,3%	16,7%	33,3%
P7. Conocimiento para identificar riesgos en redes	16,7%	0%	33,3%	16,7%	33,3%
P8. Competencias para explicar funcionamiento de redes inalámbricas	16,7%	0%	16,7%	16,7%	50,0%
P9. La capacitación recibida ha fortalecido habilidades técnicas	16,7%	0%	33,3%	50,0%	0%

Fuente: Elaboración propia.

En relación con las redes inalámbricas, la confianza docente es mayor, alcanzando a la mayoría del profesorado que se declara competente para explicar su funcionamiento. Esta disparidad sugiere que la institución ha logrado mejores niveles de formación en conectividad que en seguridad, lo que podría deberse a que las redes inalámbricas son

contenidos más antiguos o integrados en el currículo, mientras la ciberseguridad es un área de incorporación más reciente y de evolución más vertiginosa. Solo una parte del profesorado reconoce, además, que la capacitación recibida hasta ahora ha fortalecido sus habilidades técnicas, dato que cuestiona la efectividad de los programas formativos previos y refuerza la

necesidad de rediseñar las estrategias de actualización docente. El tercer bloque exploró

la demanda de formación continua y la preferencia por la plataforma institucional.

Tabla 3. *Necesidad de capacitación y preferencia por plataforma integrada.*

Ítem	Totalmente en desacuerdo	En desacuerdo	Ni acuerdo ni desacuerdo	De acuerdo	Totalmente de acuerdo
P10. Mayor capacitación mejoraría la formación de los estudiantes	16,7%	0%	0%	16,7%	66,7%
P11. Necesidad de espacios de capacitación continua	16,7%	0%	16,7%	0%	66,7%
P12. Preferencia por integración en MODVS IV frente a plataformas externas	16,7%	16,7%	0%	33,3%	33,3%

Fuente: Elaboración propia.

El respaldo a la afirmación de que una mayor capacitación mejoraría la formación de los estudiantes es contundente: la inmensa mayoría del profesorado así lo cree. Este hallazgo valida el supuesto fundamental del proyecto, pues la inversión en formación docente no es un fin en sí mismo, sino un medio para elevar la calidad educativa. Existe, sin embargo, una discrepancia entre la valoración del impacto formativo y la demanda explícita de espacios de capacitación continua, algo menor, aunque sigue siendo mayoritaria. Una minoría se mantuvo neutral y otra se opuso, lo que sugiere que, aunque la mayoría reconoce los beneficios, un sector no percibe como urgente la institucionalización de dichos espacios, quizás por autosuficiencia o por experiencias previas insatisfactorias.

El ítem más polarizado fue la preferencia por integrar el módulo en MODVS IV frente a plataformas externas. La mayoría del profesorado se inclinó por la integración, mientras una minoría relevante mostró rechazo o prefirió herramientas externas. Esta polarización es relevante porque indica que el diseño del módulo no puede ser cerrado ni excluyente; debería contemplar mecanismos de interoperabilidad o permitir que los docentes complementen su formación con recursos de su elección sin abandonar el entorno institucional.

La resistencia de una parte del profesorado a la plataforma propia podría deberse a experiencias previas con limitaciones técnicas de MODVS, a la familiaridad con otras herramientas como laboratorios externos o entornos comerciales, o a una preferencia por la autonomía en la elección de recursos.

El análisis cuantitativo presentado en la tabla 4 revela una paradoja central: la mayoría del profesorado acepta entusiastamente todas las funcionalidades del módulo de capacitación propuesto, pero solo la mitad se siente realmente preparado en ciberseguridad, y un segmento considerable muestra inseguridad sobre sus propias competencias. Esta brecha entre la valoración de la herramienta y la autopercepción del saber evidencia que los docentes reconocen su déficit formativo y demandan un recurso institucional para superarlo. Las redes inalámbricas constituyen un área de mayor confianza, probablemente por su mayor antigüedad en el currículo. Aunque la necesidad de capacitación continua es explícita y se asocia con la mejora del aprendizaje estudiantil, la preferencia por la plataforma institucional, siendo mayoritaria, no es homogénea: una minoría significativa prefiere entornos externos, lo que obliga a diseñar un módulo flexible, interoperable y atento a la heterogeneidad del profesorado.

Tabla 4. Matriz de análisis cualitativo de entrevistas a informantes clave.

Pregunta	Director de carrera (3 años)	Vicerrector académico (20 años)	Consultor TIC (22 años)	Interpretación crítica
Diagnóstico del nivel actual de preparación docente	Nivel variado. Base sólida, pero con brechas en tecnologías emergentes y ciberseguridad.	Nivel heterogéneo. Base técnica sólida, pero no uniforme. Brechas en ciberseguridad aplicada y herramientas actualizadas	Nivel aceptable; requiere actualización y mayor práctica.	Existe una base sólida, pero desigual; se requiere actualización continua institucionalizada.
Competencias técnicas prioritarias a fortalecer	Ciberseguridad y redes inalámbricas, con enfoque práctico de nivel intermedio a especializado.	Seguridad, vulnerabilidades e incidentes, con nivel progresivo.	Hardening, hacking ético y redes avanzadas, de nivel intermedio-avanzado.	Consenso en fortalecer seguridad y vulnerabilidades mediante una formación práctica y progresiva, de nivel intermedio a especializado.
Dificultades institucionales para la capacitación	Falta de tiempo, presupuesto limitado, infraestructura insuficiente	Falta de tiempo, recursos limitados, rápida evolución tecnológica	Presupuesto limitado, carga académica, obsolescencia tecnológica, falta de infraestructura	Las principales barreras son tiempo, presupuesto, infraestructura y cambio tecnológico.
Beneficios percibidos de una plataforma digital integrada	Acceso flexible, aprendizaje autónomo, actualización continua, simulaciones, seguimiento, reducción de costos	Accesibilidad, formación continua, centralización, seguimiento, evidencia para decisiones	Capacitación sistematizada, acceso flexible, aprendizaje continuo, simulaciones, certificación interna	Favorece el acceso, formación continua, seguimiento y eficiencia institucional.
Funcionalidades y recursos necesarios	Contenidos teóricos, simulaciones, laboratorios virtuales, evaluaciones, foros, analíticas, certificaciones	Contenidos estructurados, simulaciones, evaluaciones con retroalimentación, seguimiento, certificaciones	Contenidos actualizados, laboratorios virtuales, evaluaciones, foros, analítica, certificaciones	Existe consenso en integrar teoría, práctica, evaluación, colaboración y certificación.

Fuente: Elaboración propia.

Tabla 5. Matriz de triangulación.

Dimensión	Docentes (encuesta)	Informantes clave (entrevistas)	Relación
Aceptación del módulo	Aceptación mayoritaria de todas las funcionalidades	Los tres coinciden en beneficios: accesibilidad, formación continua, centralización, trazabilidad	Convergencia fuerte
Competencias en ciberseguridad	Solo la mitad se siente preparada; un tercio muestra inseguridad	Base sólida pero heterogénea; brechas en lo aplicado y en tecnologías emergentes	Convergencia
Competencias en redes inalámbricas	Mayor confianza que en ciberseguridad	Mejor dominio, con brechas en tecnologías modernas (WiFi 6, seguridad avanzada)	Convergencia
Necesidad de capacitación continua	Dos tercios demandan espacios institucionales	La evolución tecnológica exige formación sistemática y progresiva	Convergencia
Preferencia por MODVS IV vs. externas	Mayoría prefiere MODVS IV; minoría prefiere plataformas externas	Solo destacan beneficios de MODVS IV; no reconocen resistencia	Divergencia
Dificultades institucionales	No se midió; se infiere una brecha entre aceptación y preparación	Barreras: tiempo, presupuesto, infraestructura, evolución tecnológica	Complementa
Funcionalidades prioritarias	Respaldo general a todas las funcionalidades propuestas	Consenso específico: contenidos, laboratorios virtuales, evaluaciones, foros, analítica, certificación	Complementa
Impacto en la formación estudiantil	La mayoría reconoce mejora en la calidad educativa	Se asume impacto positivo en la calidad académica institucional	Convergencia

Fuente: Elaboración propia.

Los hallazgos de este estudio confirman que la aceptación de un módulo de capacitación en ciberseguridad y redes inalámbricas integrado en la plataforma MODVS IV es mayoritaria, pero coexiste con una preocupante brecha en la autopercepción de competencias docentes. Esta paradoja no es nueva en la literatura especializada. Alulema et al. (2024) señalan que

la capacitación docente en TIC suele enfocarse en el uso instrumental de la tecnología, descuidando la integración pedagógica y técnica necesaria para transferir conocimientos al aula. Bravo et al. (2025) documentan, en el mismo sentido que, aunque los docentes valoran positivamente las plataformas digitales, persiste una desconexión entre la percepción de utilidad

y la habilidad real para explotar sus funcionalidades formativas. Los resultados aquí presentados añaden evidencia a esta línea: la alta aceptación del módulo no se traduce automáticamente en preparación para enseñar ciberseguridad, lo que sugiere que el mero diseño tecnológico no resuelve el déficit formativo.

Otro hallazgo relevante es la asimetría entre las competencias declaradas en redes inalámbricas, mayores, y las de ciberseguridad, notablemente más limitadas. Esta diferencia puede explicarse por la trayectoria curricular de ambas áreas: las redes inalámbricas han estado presentes en los programas de formación técnica durante más tiempo, mientras la ciberseguridad es un campo de incorporación más reciente y de evolución acelerada. Estacio (2025) encontró resultados similares en institutos tecnológicos de la provincia del Guayas, donde los docentes mostraban niveles de competencia muy desiguales entre los fundamentos de redes y las temáticas avanzadas de seguridad, atribuyendo esa brecha a la falta de programas de actualización continua que respondan a la velocidad del cambio tecnológico, conclusión que converge plenamente con lo observado en esta investigación.

Las entrevistas a los informantes clave permitieron identificar cuatro barreras estructurales que explican por qué la aceptación del módulo no se ha traducido en acciones formativas efectivas: disponibilidad de tiempo, limitaciones presupuestarias, infraestructura tecnológica insuficiente y rápida evolución tecnológica. Estos obstáculos no son exclusivos del contexto ecuatoriano. Fuentes (2025) documentó que, en la Universidad Técnica del Norte, la implementación de entornos de entrenamiento en ciberseguridad tipo Capture The Flag se vio seriamente limitada por la falta

de laboratorios actualizados y por las restricciones de tiempo del profesorado. Ramírez (2025) señala, de manera complementaria, que incluso cuando las instituciones cuentan con plataformas digitales, la ausencia de políticas de formación continua y de incentivos para la participación reduce drásticamente la efectividad de los programas. Estos antecedentes refuerzan la necesidad de que el módulo propuesto no sea una solución aislada, sino que se acompañe de una estrategia institucional que aborde simultáneamente las cuatro barreras identificadas.

Una divergencia significativa entre los datos cuantitativos y cualitativos merece atención especial. Mientras la encuesta reveló que una minoría del profesorado prefiere plataformas externas a la integración en MODVS IV, los informantes clave no reconocieron esta resistencia en sus discursos. Esta discrepancia puede interpretarse a la luz de lo señalado por Bitrián et al. (2024), quienes advirtieron que las resistencias tecnológicas suelen ser silenciosas y no se manifiestan en espacios formales de consulta, especialmente cuando existen jerarquías institucionales. Estos autores, en un estudio sobre gamificación en la formación laboral, encontraron que los empleados con mayor especialización técnica mostraban menor disposición a utilizar plataformas corporativas estandarizadas, prefiriendo entornos de aprendizaje autogestionados.

Este fenómeno parece replicarse en el presente estudio: el docente con mayor especialización en redes fue quien sistemáticamente mostró rechazo al módulo, lo que sugiere que la resistencia está asociada a perfiles de alta autonomía y a experiencias previas posiblemente insatisfactorias con la plataforma institucional. El diseño del módulo, por tanto, no puede ser cerrado ni excluyente. Castelo et

al. (2025) demostraron que las plataformas LMS que incorporan mecanismos de interoperabilidad con herramientas externas logran mayores niveles de adopción entre el profesorado, especialmente cuando se respetan las preferencias individuales de aprendizaje. En la misma línea, los resultados de esta investigación apuntan a la necesidad de que MODVS IV no reemplace los entornos que los docentes ya utilizan, sino que los complemente, ofreciendo una capa de seguimiento, certificación y recursos especializados que añadan valor sin imponer una única vía de acceso.

En cuanto a las limitaciones del estudio, la principal es el tamaño reducido de la muestra cuantitativa, que impide extrapolar los hallazgos a otras instituciones o contextos. La ausencia de análisis inferencial limita, además, la capacidad de establecer relaciones causales entre variables, y el diseño transversal captura un momento específico sin permitir evaluar cambios en las percepciones docentes a lo largo del tiempo. No obstante, la triangulación con datos cualitativos provenientes de tres informantes con visiones complementarias (operativa, institucional y técnica especializada) otorga solidez interpretativa a los hallazgos y compensa parcialmente las limitaciones cuantitativas.

Futuras investigaciones deberían ampliar la muestra docente e incluir un diseño cuasiexperimental que evalúe si la implementación efectiva del módulo modifica las competencias auto percibidas y objetivas del profesorado en ciberseguridad y redes inalámbricas. También sería pertinente explorar en profundidad las causas de la resistencia a la plataforma institucional mediante grupos focales o entrevistas longitudinales, y desarrollar un estudio de caso comparativo

entre instituciones tecnológicas ecuatorianas que hayan implementado programas similares, con el fin de identificar buenas prácticas y factores críticos de éxito.

Conclusiones

La capacitación docente en ciberseguridad y redes inalámbricas constituye una necesidad fundamental en la educación superior tecnológica. Los resultados reflejan una amplia aceptación respecto a la implementación de un módulo de formación continua integrado en la plataforma institucional MODVS IV; aun así, esta valoración favorable contrasta con el nivel de preparación docente, lo que permite identificar una brecha formativa relevante. Solo una parte del profesorado se percibe con las competencias necesarias para abordar contenidos de ciberseguridad, mientras otro grupo expresa limitaciones, especialmente en aspectos prácticos y en tecnologías emergentes. El nivel de confianza resulta mayor en redes inalámbricas, lo que sugiere un desarrollo más consolidado en esta área en comparación con la seguridad informática.

La mayoría de los docentes reconoce que la formación continua incide de manera directa en la calidad del aprendizaje estudiantil. A pesar de ello, la preferencia por el uso de la plataforma institucional no es completamente homogénea, lo que pone de relieve la necesidad de incorporar enfoques flexibles que contemplen diferentes dinámicas de aprendizaje y el uso complementario de herramientas externas. La implementación del módulo exige considerar diversos factores que inciden en su viabilidad institucional, entre ellos la disponibilidad de tiempo, las limitaciones presupuestarias, la infraestructura tecnológica y la constante evolución del campo. Bajo estas condiciones, la efectividad de la propuesta dependerá no solo de su diseño, sino también del respaldo

institucional para su sostenibilidad. Los hallazgos respaldan la pertinencia de desarrollar un entorno de formación continua integrado, al tiempo que resaltan la necesidad de impulsar acciones institucionales orientadas a fortalecer las competencias docentes y a responder de manera progresiva a las demandas del entorno tecnológico actual.

Referencias Bibliográficas

Alulema, M., Sarzosa, M., Lagla, V., Castillo, C., & Basantes, M. (2024). La capacitación al docente en el uso de las TIC y su importancia en el quehacer educativo. *Ciencia Latina Revista Científica Multidisciplinar*, 8(4), 9205-9217.

https://doi.org/10.37811/cl_rcm.v8i4.13066

Bitrián, P., Buil, I., Catalán, S., & Merli, D. (2024). Gamificación en la formación de la fuerza laboral: mejora de la autoeficacia de los empleados y de los comportamientos en materia de seguridad de la información y protección de datos. *Journal of Business Research*, 179, 114685.

<https://doi.org/10.1016/j.jbusres.2024.114685>

Bravo, L., Pincay, K., Villafuerte, K., & Llanqui, J. (2025). Impacto de las plataformas digitales en la enseñanza y adquisición de habilidades prácticas por estudiantes de educación superior tecnológica. *Sinergia Académica*, 8(1).

<https://sinergiaacademica.com/index.php/sa/article/view/418>

Castelo, L., Zhuma, T., Villa, A., Ramírez, X., & Olalla, G. (2025). Efecto del uso de plataformas LMS sobre el rendimiento académico en asignaturas virtualizadas. *Ciencia Latina Revista Científica Multidisciplinar*, 9(4), 10222-10238.

https://doi.org/10.37811/cl_rcm.v9i5.19581

Castillo, M., & Ortiz, G. (2025). Análisis de vulnerabilidades en el uso de las redes

sociales en ataque cibernético para fortalecer la seguridad de la información (Tesis de pregrado). Universidad Estatal del Sur de Manabí.

<http://repositorio.unesum.edu.ec/handle/53000/7255>

Chuqui, J., & Orellana, D. (2023). Análisis de las vulnerabilidades del sistema de información académica: caso de estudio Instituto Superior Tecnológico del Azuay. Universidad Politécnica Salesiana.

<http://dspace.ups.edu.ec/handle/123456789/25183>

Córdova, D., Romero, J., López, R., García, M., & Sánchez, D. (2024). Desarrollo de competencias digitales docentes mediante entornos virtuales: una revisión sistemática. *Apertura*, 16(1).

https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1665-61802024000100142

Cruz, G. (2025). Portal cautivo para la gestión de acceso en el centro de desarrollo de aplicaciones de la carrera Tecnologías de la Información (Tesis de pregrado). Universidad Estatal del Sur de Manabí.

<https://repositorio.unesum.edu.ec/handle/53000/7877>

Estacio, K. (2025). Análisis de competencias en ciberseguridad de docentes en entornos virtuales de un IST en Guayas. *Revista InGenio*, 8(2), 66-81.

<https://doi.org/10.18779/ingenio.v8i2.981>

Fuentes, E. (2025). Desarrollo de un entorno seguro Capture The Flag (CTF) con integración de escenarios de ciberataques basados en MITRE ATT&CK como estrategia de prevención de ciberataques. Caso de estudio: Universidad Técnica del Norte (Tesis de postgrado). Universidad Técnica del Norte.

<https://repositorio.utn.edu.ec/handle/123456789/17339>

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2022). Diagnóstico de las capacidades de ciberseguridad.

<https://www.telecomunicaciones.gob.ec/wp-content/uploads/2023/05/DIAGNO%CC%81f>

Moreno, O., & Ayala, E. (2025). Implementación de un laboratorio de bajo costo para el desarrollo de prácticas de ciberseguridad. Revista ESPACIOS, 46(6), 11.

https://ve.scielo.org/scielo.php?script=sci_arttext&pid=S0798-10152025000600125

Ramírez, K. (2025). Plataforma de simulación en ciberseguridad para la capacitación de estudiantes universitarios (Tesis).

Universidad Autónoma del Estado de México.

<http://hdl.handle.net/20.500.11799/143797>

Tamayo, J. (2024). Herramientas digitales en el perfeccionamiento de la enseñanza-aprendizaje de asignaturas del área de matemática (Tesis de maestría). Universidad Técnica del Norte.

<https://repositorio.utn.edu.ec/handle/123456789/15563>



Esta obra está bajo una licencia de Creative Commons Reconocimiento-No Comercial 4.0 Internacional. Copyright © Edison Javier Usca Paguy y Carlos Alberto Chacón Terán.

Declaraciones éticas y editoriales del artículo
Contribución de los autores (Taxonomía CRediT) Edison Javier Usca Paguy: conceptualización de la investigación, formulación del problema y objetivos, revisión bibliográfica, diseño metodológico, elaboración y aplicación de los instrumentos, recopilación y organización de la información, análisis e interpretación de los resultados, redacción del borrador original y coordinación general del estudio. Carlos Alberto Chacón Terán: apoyo en el diseño metodológico y componente tecnológico de la investigación, revisión de contenidos relacionados con ciberseguridad, redes inalámbricas y tecnologías emergentes, organización y análisis de la información, participación en la triangulación de los resultados, revisión crítica del contenido científico y edición final del manuscrito.
Declaración de conflicto de intereses Los autores declaran que no existen conflictos de intereses relacionados con la investigación, la autoría ni la publicación del presente artículo.
Declaración de financiamiento La presente investigación no recibió financiamiento específico de agencias públicas, comerciales ni de organizaciones sin fines de lucro.
Declaración del editor No aplica en la versión presentada por los autores. Esta declaración corresponde al equipo editorial de la revista una vez concluido el proceso de evaluación y publicación del manuscrito.
Declaración de los revisores No aplica en la versión presentada por los autores. Esta declaración corresponde a la revista una vez finalizado el proceso de revisión por pares.
Declaración ética de la investigación Los autores declaran que la investigación se desarrolló respetando los principios de integridad científica, participación voluntaria, anonimato y confidencialidad. Los participantes fueron informados sobre los objetivos y características del estudio y otorgaron su consentimiento informado por escrito. Los datos obtenidos fueron utilizados exclusivamente con fines académicos y científicos, garantizando la protección de la identidad de los participantes y el manejo responsable de la información.
Declaración sobre el uso de inteligencia artificial Los autores declaran que, en caso de haberse utilizado herramientas de inteligencia artificial durante la elaboración del manuscrito, estas fueron empleadas únicamente como apoyo técnico para la organización de información, revisión del lenguaje y mejora de la claridad del texto. La formulación metodológica, el análisis e interpretación de los resultados, la revisión científica y la responsabilidad intelectual sobre el contenido corresponden exclusivamente a los autores. Las herramientas de inteligencia artificial no fueron consideradas autoras ni sustituyeron el criterio académico y científico de los investigadores.
Disponibilidad de datos Los autores declaran que los datos que respaldan los resultados de la investigación estarán disponibles previa solicitud razonable al autor de correspondencia, siempre que su entrega no comprometa la confidencialidad, el anonimato de los participantes ni la protección de la información recopilada durante el estudio.

