https://doi.org/10.69639/arandu.v13i2.2316

Análisis de factores para la enseñanza efectiva de ciberseguridad en entornos universitarios multidisciplinarios

Analysis of factors for the effective teaching of cybersecurity in multidisciplinary university environments

Jose Belisario Vera Vera
belisariovera@espam.edu.ec
https://orcid.org/0000-0002-9101-3426
Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López
Calceta – Ecuador

Cinthya Pamela Alvarez Moreira
cinthya.alvarez@espam.edu.ec
https://orcid.org/0009-0001-0187-9868
Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López
Calceta – Ecuador

Yimmy Salvador Loor Vera
yloor@espam.edu.ec
https://orcid.org/0009-0004-7516-3207
Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López
Calceta – Ecuador

María Elizabeth Cedeño Navarrete
mecedeno@espam.edu.ec
https://orcid.org/0009-0000-6080-560X
Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López
Calceta - Ecuador

John Kevin Cevallos Estrada
jkcevallos@espam.edu.ec
https://orcid.org/0009-0001-0795-0071
Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López
Calceta - Ecuador

Artículo recibido: 10 mayo 2026- Aceptado para publicación:16 junio 2026
Conflictos de intereses: Ninguno que declarar.

RESUMEN

El presente estudio tuvo como propósito identificar los elementos clave que inciden en la enseñanza y aprendizaje de la ciberseguridad en instituciones de educación superior con estudiantes de diversas áreas del conocimiento. Actualmente, la ciberseguridad constituye un componente transversal del desarrollo tecnológico y profesional, por lo que su enseñanza requiere estrategias adaptadas a distintos perfiles académicos. La metodología se basó en una revisión sistemática de literatura científica reciente sobre modelos, enfoques pedagógicos y factores de éxito en la enseñanza de la ciberseguridad. Esta revisión permitió establecer un marco teórico para identificar variables relevantes en el proceso educativo. De manera complementaria, se aplicaron encuestas a estudiantes universitarios de diferentes carreras con el objetivo de obtener

evidencia empírica sobre percepciones, dificultades y motivaciones relacionadas con el aprendizaje de esta temática. El análisis conjunto de la literatura y los resultados de las encuestas permitió establecer recomendaciones concretas sobre qué contenidos enseñar y cómo abordarlos, considerando aspectos técnicos, pedagógicos e interdisciplinarios. Los hallazgos de los 20 artículos científicos analizados destacan la importancia de la ciberseguridad en la educación superior, debido a su aporte en la formación digital segura y la protección institucional. Asimismo, las encuestas evidenciaron una brecha conductual significativa: aunque el 84 % de los estudiantes reconoce la relevancia de la ciberseguridad, una proporción considerable mantiene prácticas de alto riesgo, como la reutilización de credenciales, lo que evidencia la necesidad de fortalecer programas educativos orientados a promover una cultura universitaria de seguridad digital y protección de la información.

Palabras clave: Ciberseguridad, factores, desarrollo, educación

ABSTRACT

This study aimed to identify the key factors influencing the teaching and learning of cybersecurity in higher education institutions with students from diverse fields of knowledge. Currently, cybersecurity constitutes a cross-cutting component of technological and professional development; therefore, its teaching requires strategies adapted to different academic profiles. The methodology was based on a systematic review of recent scientific literature on models, pedagogical approaches, and success factors in cybersecurity education. This review made it possible to establish a theoretical framework to identify relevant variables in the educational process. Additionally, surveys were conducted with university students from different academic programs in order to obtain empirical evidence regarding perceptions, difficulties, and motivations related to learning this subject. The combined analysis of the literature and survey results enabled the formulation of concrete recommendations on what content should be taught and how it should be addressed, considering technical, pedagogical, and interdisciplinary aspects. The findings from the 20 scientific articles analyzed highlight the importance of cybersecurity in higher education due to its contribution to secure digital training and institutional protection. Likewise, the surveys revealed a significant behavioral gap: although 84% of students recognize the relevance of cybersecurity, a considerable proportion still engage in high-risk practices, such as credential reuse. This demonstrates the need to strengthen educational programs aimed at promoting a university culture of digital security and information protection.

Keywords: Cybersecurity, factors, development, education

INTRODUCCIÓN

En la era digital contemporánea, la ciberseguridad se posiciona como un componente esencial del quehacer académico y profesional. Las universidades tienen la responsabilidad de formar profesionales capaces de entender y responder a riesgos tecnológicos complejos, por lo que la enseñanza de ciberseguridad trasciende lo puramente técnico y demanda un enfoque transversal que incluya aspectos éticos, organizacionales y socioculturales. Este reto se intensifica en entornos multidisciplinarios, donde confluyen estudiantes de carreras técnicas, humanísticas, administrativas y artísticas, cada uno con niveles dispares de conocimiento previo, motivaciones distintas y expectativas profesionales variadas. Consecuentemente, diseñar estrategias educativas eficaces requiere un análisis riguroso de los factores que influyen en el aprendizaje y la apropiación de competencias en ciberseguridad.

Actualmente, la ciberseguridad se ha convertido en una preocupación creciente dentro del ámbito de la educación superior y, especialmente, en la enseñanza virtual, donde el uso de entornos digitales es cada vez más frecuente. La digitalización de procesos académicos, la gestión de datos personales y el acceso a plataformas educativas en línea han convertido a las universidades en objetivos atractivos para ataques cibernéticos (López et al., 2024). La reciente transición hacia el aprendizaje en línea ha expuesto nuevas vulnerabilidades, como el incremento de intentos de phishing y accesos no autorizados, lo que exige a las universidades una actualización constante de sus protocolos de ciberseguridad (González et al., 2024). Al respecto, Jain y Gupta (2021) señalan que el phishing constituye una forma de robo de identidad que manipula a los usuarios de Internet para que revelen información confidencial, como credenciales de acceso y datos de tarjetas de crédito.

La enseñanza efectiva de la ciberseguridad implica articular modelos pedagógicos activos que favorezcan el aprendizaje experiencial y la resolución de problemas reales. Metodologías como el aprendizaje basado en proyectos, el aprendizaje por problemas y las actividades prácticas en laboratorio permiten que los estudiantes enfrenten retos concretos, desarrollen pensamiento crítico y apliquen conceptos teóricos en contextos reales. Asimismo, la incorporación de simulaciones, ejercicios tipo "capture the flag" y escenarios de laboratorio virtual contribuye a consolidar habilidades técnicas y a mejorar la motivación y la retención del conocimiento. En entornos multidisciplinarios, estas metodologías deben adaptarse para ser accesibles y relevantes a perfiles no técnicos, integrando explicaciones contextuales y vínculos con problemáticas propias de otras disciplinas.

Otro factor determinante es la evaluación diagnóstica del nivel de competencia previa y la percepción del riesgo entre los estudiantes. La heterogeneidad de conocimientos exige estrategias de diferenciación curricular que permitan ofrecer trayectos formativos escalonados: módulos introductorios para quienes parten de cero y contenidos avanzados para estudiantes con

formación técnica. La sensibilización sobre amenazas cibernéticas y la construcción de una cultura de seguridad dentro de la comunidad académica son igualmente críticas, pues la conducta segura depende tanto del conocimiento como de la actitud y la percepción de responsabilidad profesional.

La interdisciplinariedad en el currículo potencia la formación integral: integrar contenidos técnicos con temas de política, derecho, ética y gestión de riesgos facilita que los estudiantes comprendan la dimensión social y regulatoria de la seguridad digital. Proyectos interdisciplinarios que vinculen, por ejemplo, informática, derecho y administración favorecen la comprensión de cómo la ciberseguridad impacta los procesos organizacionales, la toma de decisiones y el cumplimiento normativo. Además, la colaboración con la industria y la oferta de prácticas profesionales y clínicas de seguridad aportan realismo y pertinencia a la formación académica.

No menos importante es el rol institucional: la disponibilidad de infraestructura adecuada, laboratorios físicos y virtuales, recursos didácticos actualizados y la capacitación continua del profesorado son condiciones que sostienen programas de calidad. Las políticas institucionales que promueven la innovación pedagógica, el apoyo a la investigación educativa en ciberseguridad y la articulación con actores externos fortalecen la sostenibilidad y la pertinencia del proceso formativo.

No obstante, la literatura disponible sobre la enseñanza de ciberseguridad en entornos universitarios multidisciplinarios es aún escasa y fragmentada, con pocos estudios que aborden de manera simultánea los factores pedagógicos, institucionales y actitudinales desde la perspectiva del estudiante. Esta brecha justifica la necesidad de investigaciones que integren dichas dimensiones y orienten el diseño de programas formativos más inclusivos y pertinentes.

Este estudio se propone identificar y priorizar los factores que facilitan una enseñanza efectiva de la ciberseguridad en contextos universitarios multidisciplinarios, mediante una revisión exhaustiva de la literatura y la aplicación de encuestas a estudiantes de distintas disciplinas. El objetivo es generar recomendaciones claras sobre qué contenidos son esenciales y cómo deben enseñarse para maximizar la inclusión, la pertinencia y la eficacia del aprendizaje. Al centrar la atención en metodologías activas, diagnóstico previo, interdisciplinariedad, experiencias prácticas y soporte institucional, se busca contribuir al diseño de programas educativos que preparen a los futuros profesionales para enfrentar los desafíos de un entorno digital cada vez más complejo e interconectado.

MATERIALES Y MÉTODOS

Esta investigación se desarrolló bajo metodología mixta donde se combinó un análisis de los resultados de encuestas aplicadas mediante Google Form a 395 estudiantes de distintas carreras y semestres de la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix

López (ESPAM MFL), ubicada en el cantón Bolívar, provincia de Manabí, Ecuador. Para el análisis cualitativo, cuantitativo y la fase teórica se desarrolló bajo la metodología STAMP (Standardized Sampling for Systematic Literature Reviews), adaptada de Lectong y Morales (2025), con el fin de garantizar un proceso sistemático, transparente y replicable en la revisión de literatura sobre enseñanza de ciberseguridad. Esta metodología se estructuró en cuatro fases: definición de criterios de elegibilidad, búsqueda de literatura científica, evaluación basada en resúmenes (ABS) y evaluación de textos completos (FTR).

Definición de criterios de elegibilidad

En esta fase se determinaron los lineamientos que establecieron qué publicaciones serían incluidas o excluidas dentro del proceso de revisión, asegurando que el análisis se mantuviera coherente con los propósitos de la investigación orientada a la enseñanza de la ciberseguridad en contextos universitarios multidisciplinarios. Con este fin, se definieron tres grupos de criterios: de búsqueda, de contenido y de exclusión como se visualiza (tabla 1).

Tabla 1

Criterios de elegibilidad

Tipo de criterio	Descripción
De búsqueda	Idioma: inglés y español. Periodo: 2020–2025. Tipo de documento: artículos científicos, libros y capítulos revisados por pares, indexados en bases de datos reconocidas.
De contenido	Estudios que aborden explícitamente la enseñanza o formación en ciberseguridad, el desarrollo de competencias digitales seguras, factores pedagógicos o modelos educativos en educación superior, incluyendo enfoques multidisciplinarios con dimensiones técnicas, humanas, legales y organizacionales.
De exclusión	Documentos sin texto completo, duplicados o que traten la ciberseguridad desde un enfoque puramente técnico o empresarial.

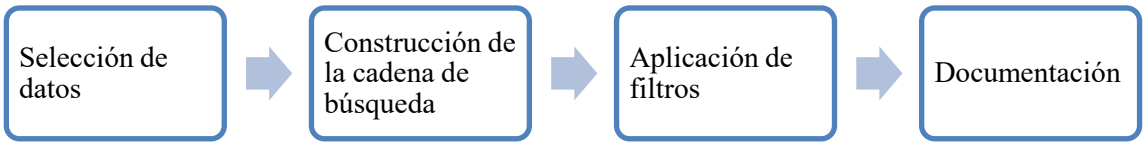
Se incluyeron artículos de revistas científicas, capítulos de libros y documentos académicos indexados en bases de datos reconocidas como ScienceDirect, REDALYC, IEEE Xplore, ERIC,DIALNET, SCIELO Y SCOPUS priorizando aquellas fuentes revisadas por pares.

Búsqueda de literatura científica

Esta fase tuvo como objetivo identificar y recopilar estudios recientes relacionados con la enseñanza de la ciberseguridad en educación superior siguiendo los objetivos de la investigación, con la finalidad de obtener información bibliografía completa lo que permitió reunir un conjunto representativo de fuentes que sirvieron como base teórica para el análisis de los factores que inciden en la enseñanza efectiva de la ciberseguridad para realizar la búsqueda se definieron cuatro pasos, detallados en la (figura 1).

Figura 1

Pasos para la búsqueda de literatura científica



Términos principales Inglés: "Cybersecurity Education" OR "Cybersecurity Teaching" AND "Higher Education" OR "University Learning" AND "Learning Factors".

Español: "Enseñanza de la Ciberseguridad" O "Formación en Ciberseguridad" Y "Educación Superior" O "Aprendizaje Universitario" Y "Factores de Aprendizaje".

Expansión de términos Se incluyeron sinónimos y conceptos relacionados como "Cybersecurity Training", "Digital Competence Development", "Pedagogical Models", y en español "Capacitación en Ciberseguridad", "Competencias Digitales", "Modelos Pedagógicos" o "Estrategias de Aprendizaje".

Tabla 2

Términos de la cadena de búsqueda

Términos principales	Inglés: "Cybersecurity Education" OR "Cybersecurity Teaching" AND "Higher Education" OR "University Learning" AND "Learning Factors". Español: "Enseñanza de la Ciberseguridad" O "Formación en Ciberseguridad" Y "Educación Superior" O "Aprendizaje Universitario" Y "Factores de Aprendizaje".
Expansión de términos	Se incluyeron sinónimos y conceptos relacionados como "Cybersecurity Training", "Digital Competence Development", "Pedagogical Models", y en español "Capacitación en Ciberseguridad", "Competencias Digitales", "Modelos Pedagógicos" o "Estrategias de Aprendizaje".

Cada búsqueda fue registrada de forma sistemática, anotando la fecha de consulta, la base de datos utilizada, los términos empleados y el número total de resultados obtenidos, lo que garantizó la trazabilidad y transparencia del proceso.

Evaluación basada en resúmenes

En esta fase, denominada ABS (Abstract-Based Screening), se revisaron los resúmenes de las publicaciones recopiladas para determinar su pertinencia con el objeto de estudio. Cada documento fue evaluado mediante tres parámetros con puntaje binario (1 = cumple; 0 = no cumple), y se incluyeron en la siguiente fase aquellas publicaciones que alcanzaron un 70% o más de cumplimiento (Tabla 3).

Tabla 3

Parámetros de la evaluación basada en resúmenes (ABS)

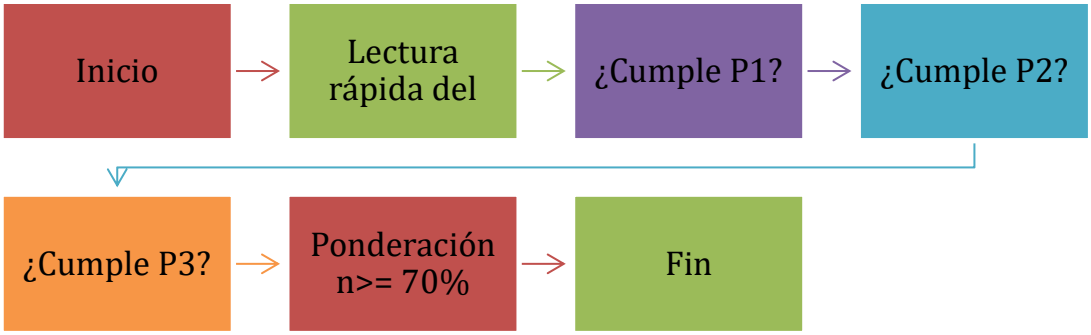
Parámetro de evaluación	Criterios incluidos / Preguntas de evaluación
P1. Pertinencia temática	¿El resumen aborda la enseñanza o formación en ciberseguridad en el ámbito de la educación superior?
P2. Enfoque pedagógico	¿El estudio analiza factores educativos, metodologías o modelos pedagógicos aplicados al aprendizaje de la ciberseguridad?
P3. Dimensión multidisciplinaria	¿La investigación considera la participación de diversas áreas del conocimiento o la integración de competencias digitales y humanas?
Puntaje binario	1 = Cumple el criterio; 0 = No cumple el criterio.
Porcentaje de inclusión	Publicaciones con al menos un 70% de cumplimiento en las categorías fueron seleccionadas para la siguiente etapa

Para la selección de las preguntas se analizaron cada una de manera individual y se le dio una ponderación Primero, se realizó una lectura rápida del resumen del artículo. A partir de esa lectura, se respondieron tres preguntas clave (P1, P2 y P3), relacionadas con los criterios de selección. Cada vez que un artículo cumplía con una de las preguntas, se le asignaba un puntaje de 1. Si no la cumplía, se le asignaba un 0.

Una vez evaluadas las tres preguntas, se sumaron los puntajes obtenidos y se calculaba un porcentaje de cumplimiento mediante una regla de tres simple, si el artículo alcanzaba un 70% o más, se consideraba que cumplía con los criterios suficientes y se incluía en la siguiente fase de revisión a texto completo. En caso contrario, era excluido del proceso (Figura 2).

Figura 2

Diagrama de flujo del proceso de evaluación rápida de resúmenes según criterios de inclusión



Evaluación de textos completos (FTR – Full Text Reading)

En esta etapa, denominada FTR (Full Text Reading), se procedió a la lectura y análisis completo de los documentos previamente seleccionados durante la fase ABS. El propósito de esta fase fue examinar en profundidad el contenido de los estudios para confirmar su aporte teórico o empírico a la enseñanza de la ciberseguridad, así como su relación con los factores y modelos identificados en la revisión.

Durante la lectura detallada, se elaboró una matriz de análisis que registró los campos detallados en la Tabla 4, facilitando la comparación entre estudios, la identificación de patrones comunes y el reconocimiento de vacíos de conocimiento.

Tabla 4

Campos incluidos en la tabla de análisis FTR

Campo	Descripción
ID del documento	Identificador único asignado a cada publicación.
Título	Título de la publicación.
Autor(es)	Nombre(s) del autor(es) del estudio.
Año de publicación	Año en que fue publicado el documento.
Base de datos	Fuente de origen (ERIC, IEEE Xplore…)
Resultados clave	Hallazgos destacados relacionados con la investigación.

RESULTADOS Y DISCUSIÓN

En la tabla 5 se muestran los resultados obtenidos de búsqueda sistemática de diversas fuentes de datos académicas, en varios de los casos se omite los términos de filtro "OR" usando los términos principales tanto en español como en inglés. Se obtuvo como resultado un total de 31293 artículos.

Tabla 5

Resultados de la búsqueda en bases de las bases de la investigación

Fecha de consulta	**Base de datos**	**Términos de búsqueda**	**Resultados obtenidos**
06/10/2025	REDALYC	Inglés: "Cybersecurity Education" OR "Cybersecurity Teaching" AND "Higher Education" OR "University Learning" AND "Learning Factors". Español: "Enseñanza de la Ciberseguridad" O "Formación en Ciberseguridad" Y "Educación Superior" O "Aprendizaje Universitario" Y "Factores de Aprendizaje".	17395
06/10/2025	ERIC		28
06/10/2025	IEEE		13800
15/10/2025	DIALNET		60
15/10/2025	SCIELO		10
Resultados obtenidos			**31293**

De los resultados obtenidos se escogieron 20 artículos que incluyen todos los criterios enmarcados en los objetivos de la investigación, como es el tema de la ciberseguridad en entornos universitarios multidisciplinarios.

El análisis de los veinte artículos revisados evidencia un consenso sobre la importancia de la ciberseguridad en la educación superior, resaltando su papel en la formación digital segura y la protección institucional. Se identifican diversos enfoques metodológicos: revisiones sistemáticas (artículos 1, 10, 12, 19 y 20), estudios mixtos (2, 5, 11 y 13) y cualitativos

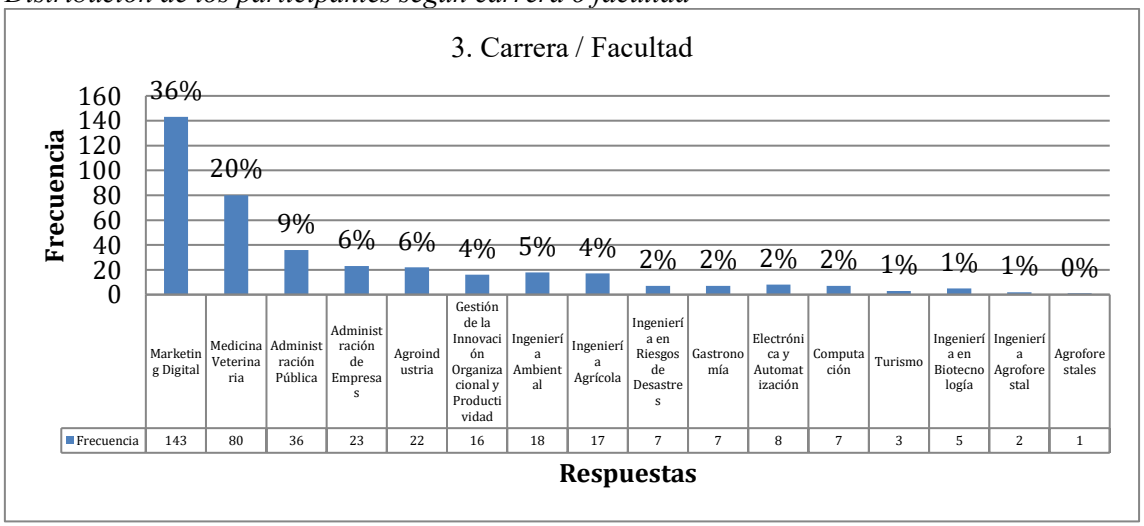
descriptivos (4, 6, 7, 8 y 18), lo que demuestra un interés interdisciplinario por abordar la ciberseguridad desde dimensiones técnicas, educativas y organizacionales.

Las métricas evaluadas abarcan la conciencia, el conocimiento, la vulnerabilidad, la gobernanza y la efectividad de los marcos de referencia (artículos 9, 14, 16 y 17). Los estudios cuantitativos (3 y 14) emplearon cuestionarios para medir niveles de conocimiento y protección, mientras que los cualitativos (6, 7 y 18) priorizaron el análisis documental y la identificación de buenas prácticas. En general, se concluye que la educación en ciberseguridad fortalece la conciencia y reduce la exposición a riesgos digitales (artículo 14), siendo clave la cooperación entre academia e industria (artículo 6) y la creación de marcos adaptativos e integrales (artículos 1, 10 y 19) para lograr instituciones seguras y resilientes.

En complemento al análisis teórico realizado mediante la metodología STAMP, se aplicó una encuesta a estudiantes de diferentes carreras de la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López (ESPAM MFL). Esta recolección de datos permitió identificar las percepciones, conocimientos y actitudes de los participantes en torno a la ciberseguridad y su enseñanza en contextos universitarios multidisciplinarios. Los resultados obtenidos fueron contrastados con los hallazgos derivados de la revisión sistemática, lo que permitió relacionar los hallazgos teóricos con las percepciones de los estudiantes, ofreciendo una visión más completa sobre los aspectos que influyen en la enseñanza y el aprendizaje de la ciberseguridad en la universidad. A continuación, se muestran los resultados de los datos mayor peso dentro de la encuesta en cuanto a los objetivos de la investigación:

Gráfico 1

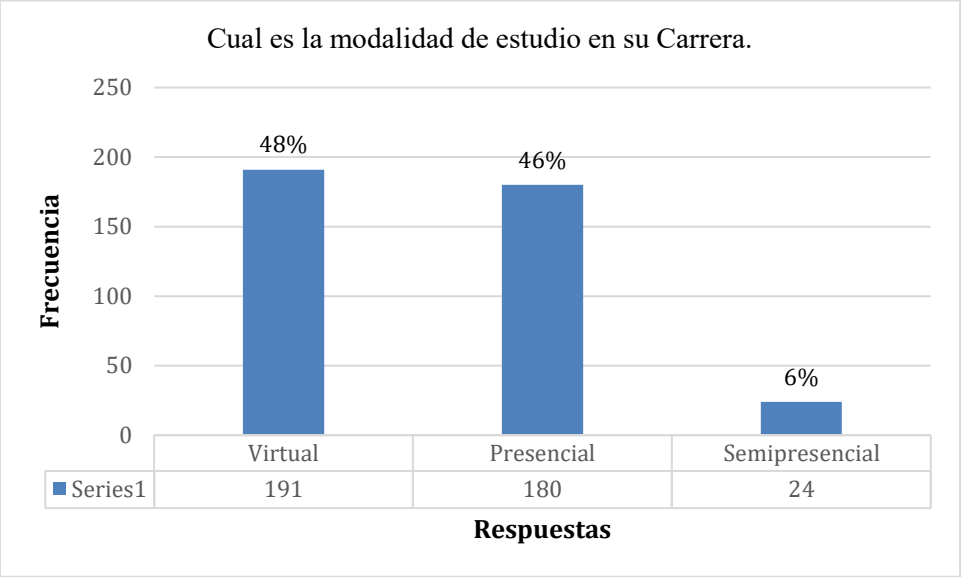
Distribución de los participantes según carrera o facultad



La población encuestada estuvo conformada por estudiantes de distintas disciplinas, predominando Marketing Digital (35,3%) y Medicina Veterinaria (20,5%), seguidas de Ingeniería, Administración y Agroindustria. Esta composición refleja la diversidad disciplinar del entorno estudiado y es coherente con el objetivo de analizar la enseñanza de ciberseguridad en contextos universitarios multidisciplinarios.

Gráfico 2

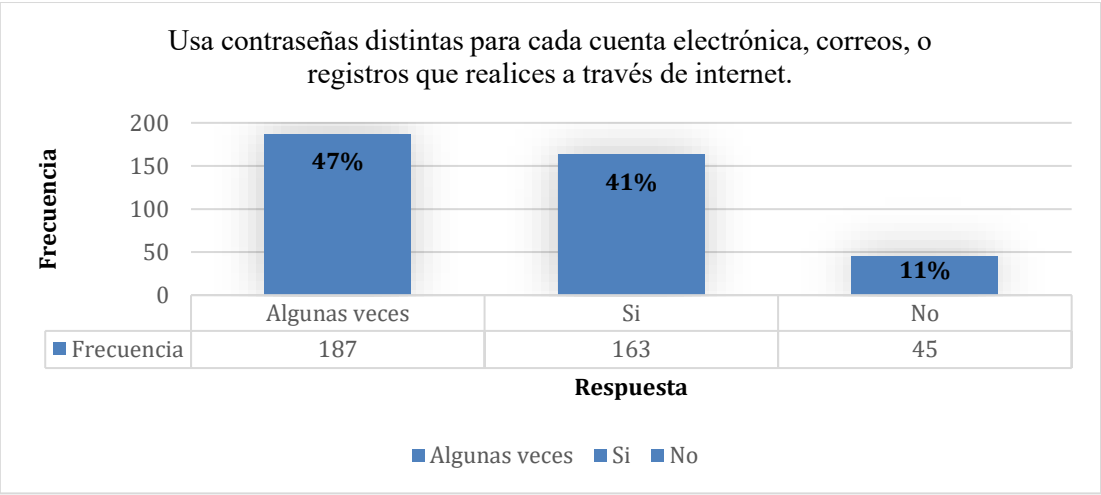
Modalidad de estudio de los participantes



El 48% de los estudiantes cursa programas en modalidad virtual y el 46% en modalidad presencial, con un 6% en modalidad híbrida. Esta distribución equilibrada implica que cualquier estrategia pedagógica en ciberseguridad debe ser funcional en ambos contextos, considerando que la modalidad condiciona el nivel de autonomía digital del estudiante y su grado de exposición a riesgos en entornos no supervisados.

Gráfico 4

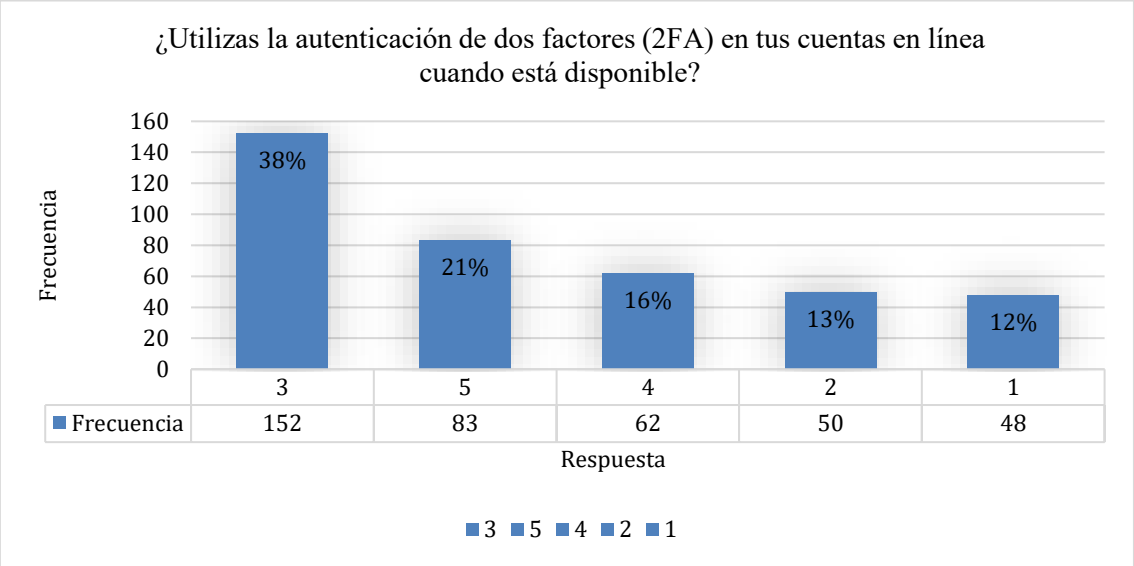
Frecuencia del uso de contraseñas distintas por cuenta



Los datos muestran que solo el 32% de los encuestados utiliza contraseñas distintas para cada cuenta de forma sistemática, mientras que el 47% lo hace ocasionalmente y el 21% reconoció no hacerlo nunca. Este resultado evidencia un bajo nivel de aplicación de prácticas seguras, incluso entre quienes declaran conocer su importancia, lo que señala una desconexión entre el conocimiento teórico y la conducta práctica en seguridad digital.

Gráfico 5

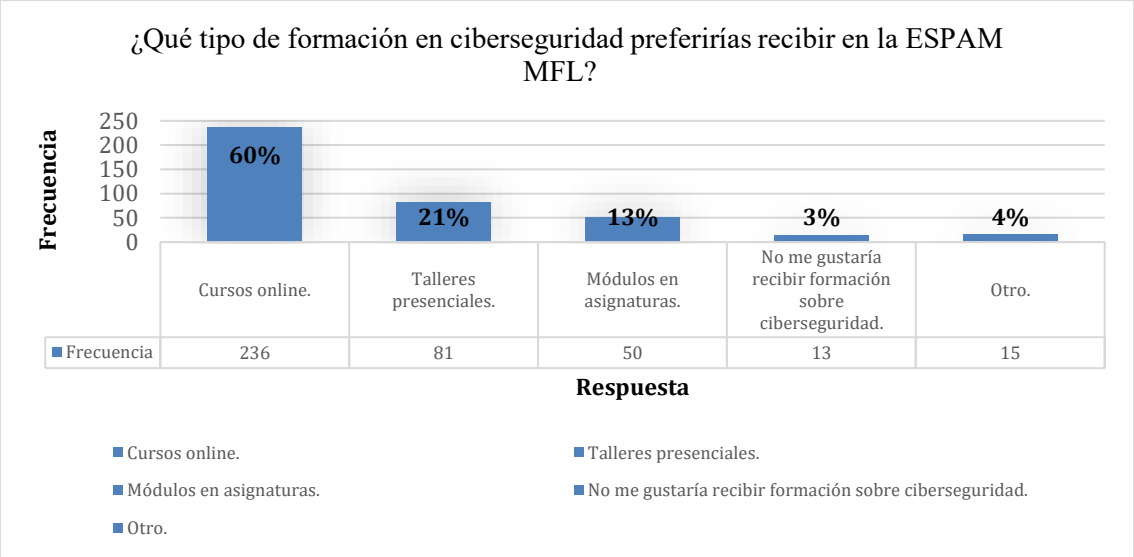
Uso de autenticación de dos factores (2FA) entre los participantes



El 38% de los estudiantes consideró muy importante conocer técnicas de autenticación multifactor, el 21% lo calificó como interesante, el 16% como medianamente importante, el 13% como poco importante y el 12% indicó que no le parece importante. Si bien la mayoría reconoce su relevancia, el 41% restante no la percibe como prioritaria, lo que indica la necesidad de fortalecer la sensibilización sobre su papel en la protección de cuentas e identidades digitales.

Gráfico 6

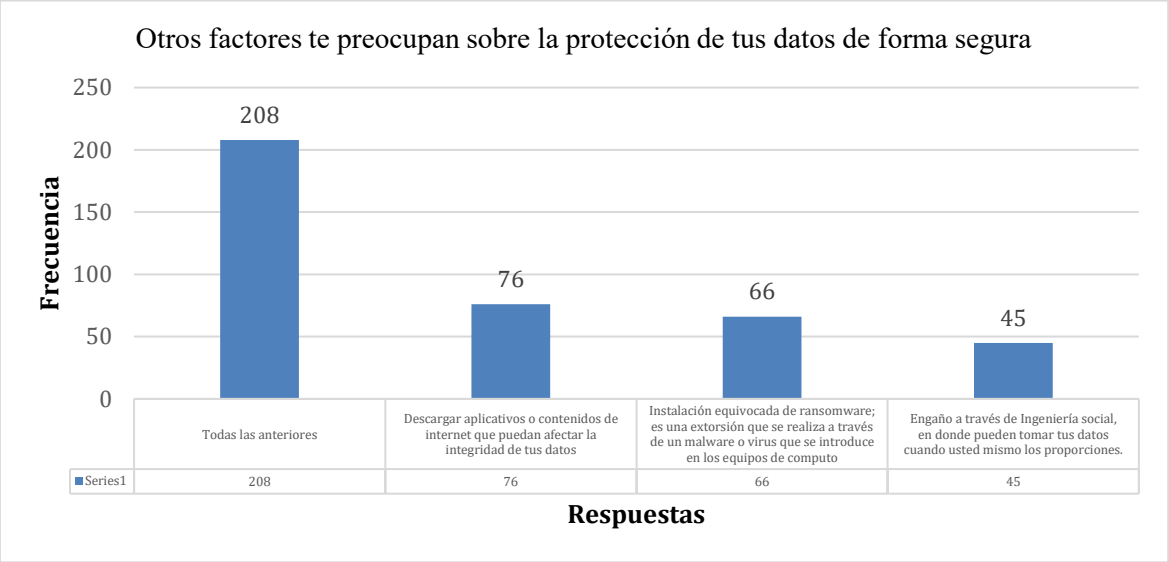
Tipo de formación preferida en ciberseguridad



El 60% de los estudiantes optó por cursos en línea, el 21% prefirió talleres presenciales y el 19% restante se inclinó por módulos integrados en asignaturas. Esta distribución evidencia una preferencia dominante por modalidades flexibles y autogestionadas, aunque la proporción significativa de quienes prefieren la presencialidad o la integración curricular respalda la pertinencia de un enfoque híbrido y transversal.

Gráfico 7

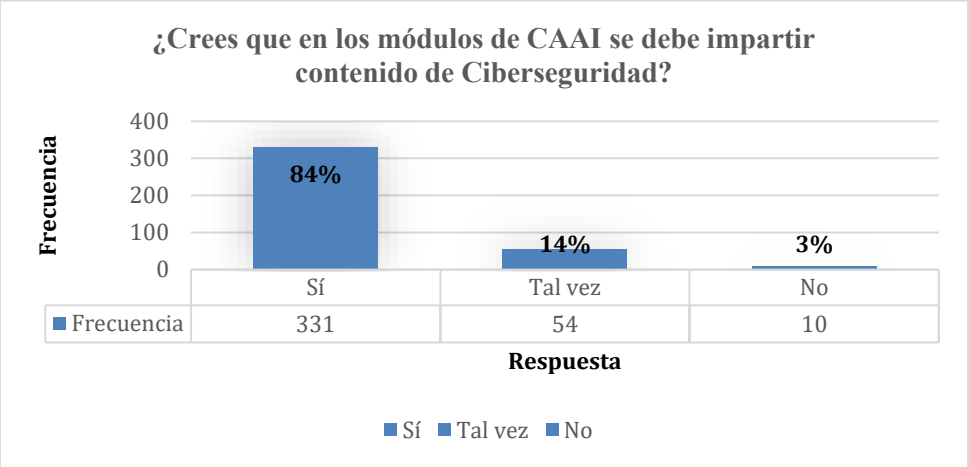
Factores de preocupación sobre la protección de datos personales



Las principales preocupaciones expresadas fueron el robo de información personal, las descargas inseguras y la instalación accidental de malware. Este resultado demuestra que los estudiantes tienen una conciencia creciente sobre la vulnerabilidad de sus datos, aunque sin un conocimiento técnico profundo para prevenir incidentes.

Gráfico 8

Opinión sobre la inclusión de contenidos de ciberseguridad en los módulos académicos



El 84% de los encuestados considera necesario incluir contenidos de ciberseguridad en los módulos académicos de la ESPAM MFL. Este amplio consenso valida la pertinencia del tema dentro del currículo universitario y refleja una demanda estudiantil concreta de formación formal en seguridad digital.

Análisis de los resultados de la encuesta

Con el objetivo de contrastar los hallazgos teóricos con la realidad institucional, se aplicó un instrumento de recolección de datos a una muestra de 395 estudiantes de la Escuela Superior Politécnica Agropecuaria de Manabí (ESPAM MFL). La composición de la muestra evidenciar el carácter multidisciplinario del estudio, con una participación destacada de Marketing Digital 35,3 % y Medicina Veterinaria 20,5 %, además de las carreras de Ingeniería, Administración y Agroindustria. Los datos recopilados Tabla 7 permiten identificar patrones críticos sobre el comportamiento y las expectativas de los estudiantes frente a la seguridad digital.

Tabla 7

Análisis de los resultados de las encuestas

Categoría	Dato relevante
Exposición Digital	48 % conexión > 4 horas/día, lo que implica una alta superficie de ataque.
Higiene Digital	41 % reutiliza contraseñas, brecha crítica en seguridad personal.
Adopción Técnica	Nivel medio (3/5) en uso de 2FA, implementación parcial de medidas preventivas.
Preferencia Educativa	60 % opta por modalidad virtual, lo que evidencia una demanda de flexibilidad y autoaprendizaje.
Aceptación Curricular	84 % a favor de incluir la temática, validando la pertinencia social del estudio.

Los resultados revelan una brecha conductual significativa: aunque el 84% de los estudiantes reconoce la relevancia de la ciberseguridad, una proporción considerable persiste en prácticas de alto riesgo como la reutilización de credenciales. Esta discrepancia entre

conocimiento y acción indica que la enseñanza de ciberseguridad no puede limitarse a la transferencia de conceptos teóricos, sino que debe orientarse hacia el fortalecimiento de la cultura digital y la modificación de hábitos arraigados mediante estrategias pedagógicas experienciales.

Por otra parte, dado que el 48% de los estudiantes participa en modalidades virtuales con tiempos de conexión prolongados, el ecosistema universitario trasciende los límites de un entorno controlado. En este contexto, amenazas como el robo de información y el malware, identificadas como las principales preocupaciones estudiantiles, dejan de ser problemas exclusivamente técnicos para convertirse en riesgos críticos que comprometen la continuidad académica.

En cuanto a las preferencias formativas, el notable interés por la instrucción en línea con un 60% sugiere que las estrategias educativas deben privilegiar modalidades asincrónicas y modulares. No obstante, la significativa proporción de estudiantes que opta por talleres presenciales 21% y módulos integrados 19% respalda la pertinencia de un enfoque híbrido y transversal, capaz de responder a las necesidades de perfiles tan diversos como los de Medicina Veterinaria o Ingeniería. En síntesis, la amplia demanda de formación formal evidencia que la ciberseguridad ha dejado de ser una especialidad exclusivamente técnica para consolidarse como una competencia esencial para la supervivencia profesional en el contexto multidisciplinario actual.

Síntesis comparativa entre la revisión bibliográfica y la encuesta estudiantil

Tabla 8

Síntesis comparativa entre la revisión bibliográfica y la encuesta

Indicador	Resultado Encuesta Estudiantil	Resultado Revisión Bibliográfica
Prácticas de seguridad digital	41 % reutiliza contraseñas; uso parcial de 2FA	La brecha entre conocimiento y práctica es común (Sittitiamjan & Wuttidittachotti, 2025)
Modalidad preferida	60 % prefiere modalidad virtual	Tendencia internacional hacia entornos híbridos y e-learning adaptativo (Vykopal et al., 2023)
Conciencia sobre riesgos	Preocupación por robo de datos y malware	Coincide con estudios sobre vulnerabilidad estudiantil (Dhungana et al., 2023)
Percepción curricular	84 % considera esencial incluir ciberseguridad	Consenso internacional sobre transversalidad curricular (Kumar et al., 2024; Barruga & Palaoag, 2025)
Dimensión interdisciplinaria	Alta diversidad académica en la muestra	Recomendación de integrar humanidades y ética digital (Frusci, 2024)

DISCUSIÓN

Los hallazgos empíricos y teóricos presentan coincidencias sustantivas respecto a la necesidad de transformar la enseñanza de ciberseguridad desde un enfoque transmisivo hacia uno multidisciplinario, conductual y sostenido institucionalmente.

En primer lugar, la brecha entre conocimiento y práctica identificada en la encuesta coincide con lo reportado por Sittitiamjan y Wuttidittachotti (2025), quienes destacan que la conciencia digital no siempre se traduce en hábitos seguros. Este patrón sugiere que los programas formativos deben incorporar estrategias de aprendizaje experiencial y gamificado que promuevan conductas preventivas sostenidas, más allá de la memorización de conceptos. La mera exposición a contenidos de ciberseguridad no es suficiente para modificar comportamientos arraigados; se requiere una pedagogía orientada a la acción.

En segundo lugar, la preferencia por la modalidad virtual (60%) evidencia un cambio estructural en los patrones de aprendizaje que se consolidó en el período pospandemia. Vykopal et al. (2023) demuestran que los entornos virtuales adaptativos favorecen la personalización y la retención del conocimiento cuando cuentan con recursos interactivos y acompañamiento docente adecuado. Sin embargo, esta preferencia también implica un riesgo: la mayor autonomía digital de los estudiantes virtuales no siempre va acompañada de mejores prácticas de seguridad, como lo evidencian los datos de higiene digital de esta muestra.

En tercer lugar, el consenso sobre la inclusión curricular (84%) subraya una demanda estudiantil que la literatura respalda ampliamente. Kumar et al. (2024) y Barruga y Palaoag (2025) coinciden en que la ciberseguridad debe tratarse como una competencia transversal, integrada en todos los planes de estudio con independencia de la disciplina. Esto implica que las universidades deben avanzar más allá de asignaturas optativas y promover programas de sensibilización permanentes articulados con el currículo general.

Finalmente, la diversidad disciplinaria observada en la muestra confirma que los enfoques de enseñanza deben ser flexibles y contextualizados según el perfil académico del estudiante. Como propone Frusci (2024), integrar la ética, la sociología y el pensamiento crítico en los programas técnicos amplía la comprensión del impacto social de la ciberseguridad y fortalece la formación ciudadana digital, algo especialmente relevante en carreras como Medicina Veterinaria o Marketing Digital, donde la conexión con la seguridad informática no es evidente a priori pero resulta igualmente necesaria.

En conjunto, los resultados empíricos y teóricos obtenidos confirman que las instituciones de educación superior deben avanzar hacia modelos formativos prácticos, interdisciplinarios y sostenidos por políticas institucionales claras. La ciberseguridad ha dejado de ser una especialidad exclusivamente técnica para convertirse en una competencia transversal imprescindible en cualquier perfil profesional. Garantizar su enseñanza efectiva en entornos multidisciplinarios

exige articular metodologías activas, modalidades flexibles, diagnóstico previo del estudiantado y cooperación con el sector productivo, con el fin de generar competencias digitales sólidas, hábitos seguros sostenidos y una cultura universitaria orientada a la protección responsable de la información en un entorno digital cada vez más complejo e interconectado.

REFERENCIAS

Barruga, M. B., & Palaoag, T. D. (2025). *Cybersecurity strategy for higher education institutions: A thematic analysis on standards and frameworks*. *International Journal of Advanced Multidisciplinary Research*, 38(4S), 299-310. https://doi.org/10.12732/ijam.v38i4s.299

Beltrán Muñoz, A. (2024). *Educar y proteger: análisis de la educación en ciberseguridad para combatir la ciberdelincuencia*. Revista de Educación y Derecho, Educación and Law Review, (30), 1–15.

Beltrán, Alberto; Jiménez-Torres, Manuel G. y Sampayo, Sara. (2023). Métodos y efectos de la educación en ciberseguridad: Una revisión sistemática. Revista Electrónica de Criminología, 07-14. 1-19. https://doi.org/10.30827/rec.7.33194

Derenzin-Martínez, F. G. (2024). *Are Ecuadorian universities prepared for cyberattacks? 593 Digital Publisher CEIT*, *9*(6), artículo e2864. https://doi.org/10.33386/593dp.2024.6.2864

Dhungana, Raj Kumar; Gurung, Lina Dr; and Poudyal, Hem (2023) "Cybersecurity Challenges and Awareness of the Multi-Generational Learners in Nepal," Journal of Cybersecurity Education, Research and Practice: Vol. 2023: No. 2, Article 5. DOI: 10.32727/8.2023.17 DOI: https://doi.org/10.1344/REYD2024.30.44082

Frusci, Joseph (2024) "Integrating Humanities into Cybersecurity Education: Enhancing Ethical, Historical, and Sociopolitical Understanding in Technical Training," Journal of Cybersecurity Education, Research and Practice: Vol. 2024: No. 1, Article 31.DOI: https://doi.org/10.62915/2472-2707.1209

González A., Pereira M., y Lacruhy C., "Hombres y mujeres en el aprendizaje virtual: ¿Opinión diferenciada de la calidad en la formación en línea?", Eduweb, vol. 18, núm. 1, pp. 66–80, 2024, doi: 10.46502/issn.1856-7576/2024.18.01.5.

Hall, A. O., Liu, X. M., & Murphy, D. (2021). Integrating andragogy theory into a multidisciplinary curriculum to achieve a connected program for a doctorate in cybersecurity. *Proceedings of the 2021 IEEE Frontiers in Education Conference (FIE)*, 1–8. https://doi.org/10.1109/FIE49875.2021.9637127.

Irzam, F. Z. M., & Taherdoost, H. (2024, abril 18). *Cybersecurity KPIs in Higher Institutions: A Systematic Review*. En *2024 International Conference on Expert Clouds and Applications (ICOECA)*. IEEE. https://doi.org/10.1109/ICOECA62351.2024.00058

Jain A. y Gupta B., "A survey of phishing attack techniques, defence mechanisms and open research challenges", Enterprise Information Systems, vol. 16, 2021, doi:10.1080/17517575.2021.1896786.

Jiménez Sánchez, V. G., Tipanluisa Masabanda, R. I., & León Espinoza, C. J. (2025). Ciberseguridad en la educación superior: evaluación y estrategias de formación.Technology in *Journal, 4*(2), e94. https://doi.org/10.55204/trj.v4i1.e94

Kryshtanovych, M., Kozlovskiy, Y., Chubinska, N., Huzii, I., & Lukashevska, U. (2021). *Ensuring cybersecurity for higher educational institutions*. En *Proceedings of the 2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T)* (pp. 1–5). IEEE. https://doi.org/10.1109/PICST54195.2021.9772173

Kumar A, Mishra K, Kumar Mahto R, Kumar Mishra B. A Framework for Institution to Enhancing Cybersecurity in Higher Education: A Review. LatIA. 2024; 2:94. https://doi.org/10.62486/latia202494

López, H. L. L., Rodríguez, L. G. Q., & Valenzuela, A. C. C. (2024). Percepción de la ciberseguridad entre estudiantes universitarios en entornos digitales: Un estudio en la Facultad de Informática Mazatlán. *TIES, Revista de Tecnología e Innovación en Educación Superior*, (11), 72-95.

Orosco-Fabian J. (2024). Ciberseguridad en educación superior: una revisión bibliométrica. Revista Digital de Investigación en Docencia Universitaria, 18(2), e1933. https://doi.org/10.19083/ridu.2024.1933

Pinda Román, N. J., & Moya Martínez, L. A. (2024). Ciberseguridad enfocada en el futuro digital de los estudiantes. LATAM Revista Latinoamericana de Ciencias Sociales y Humanidades, 5(2). https://doi.org/10.56712/latam.v5i2.1910

Sittitiamjan, K., & Wuttidittachotti, P. (2025). Bridging the Gap: How Knowledge, Attitudes, and Practices Shape Cybersecurity Awareness in Thai Education. Educational Process: International Journal, 16, e2025236. doi.org/10.22521/edupij.2025.16.236

Trujillo-Torres, J.-M., Rodríguez-Jiménez, C., Alonso-García, S., & Berral-Ortiz, B. (2024). *Revisión sistemática de la literatura sobre la seguridad digital en estudiantes de educación superior*. *Información Tecnológica, 35*(4), 1–12. https://doi.org/10.4067/S0718-07642024000400001

Zafar, Humayun; Hollingsworth, Carole L.; Bandyopadhyay, Tridib; and Randolph, Adriane B. (2024)"Collaborative Pathways to Cybersecurity Excellence: Insights from Industry and Academia in the utheastern US," Journal of Cybersecurity Education, Research and Practice: Vol. 2024: No. 1, Article 23 DOI: https://doi.org/10.62915/2472-2707.1183

Zapata Zurita, J. G. (2024). *Acoso cibernético a universitarios creadores de contenido: análisis y medidas de prevención en Bolivia*. Revista Educación Superior y Sociedad, 36(2), 316–344. https://doi.org/10.54674/ess.v36i2.917