Computación y ciberseguridad: protección de aplicaciones académicas en la formación digital

Computing and cybersecurity: protection of academic applications in digital training

Ricardo Manuel Candanedo Yau[1]
[1]Universidad de Panamá, ricardo.candanedo@up.ac.pa, https://orcid.org/0009-0002-5017-9830, Panamá

Información del Artículo

Trazabilidad:

Recibido 27-02-2026
Revisado 05-03-2026
Aceptado 01-04-2026

Palabras Clave:

Aplicaciones informáticas
Ciberseguridad
Educación digital
Protección de datos
Seguridad de la información

RESUMEN

El estudio analizó la relación entre la computación y la ciberseguridad en la protección de aplicaciones informáticas en plataformas de formación digital. Se identificaron vulnerabilidades frecuentes en sistemas educativos, tales como accesos no autorizados, debilidades en los mecanismos de autenticación y exposición de datos sensibles. La investigación adoptó un enfoque descriptivo, sustentado en la revisión documental y el análisis de casos en contextos educativos, lo que permitió evaluar los mecanismos de seguridad de la información implementados en sistemas de gestión del aprendizaje. Los resultados evidenciaron que la aplicación de protocolos de seguridad, el cifrado de datos y las políticas de control de acceso contribuyeron significativamente a la mitigación de riesgos cibernéticos. Asimismo, se destacó la importancia del desarrollo de competencias digitales seguras en estudiantes y docentes. Se concluyó que la integración de estrategias de ciberseguridad en el diseño y uso de aplicaciones académicas fortaleció la protección de la información, lo que promovió plataformas digitales más confiables y resilientes.

Keywords:

Cybersecurity
Computer applications
Data protection
Digital education
Information security

ABSTRACT

The study analyzed the relationship between computing and cybersecurity in the protection of computer applications within digital learning platforms. Common vulnerabilities in educational systems were identified, including unauthorized access, weaknesses in authentication mechanisms, and exposure of sensitive data. The research adopted a descriptive approach based on document review and case analysis in educational contexts, enabling the evaluation of information security mechanisms implemented in learning management systems. The results showed that the implementation of security protocols, data encryption, and access control policies significantly contributed to mitigating cyber risks. Furthermore, the importance of developing secure digital competencies among students and teachers was highlighted. It was concluded that integrating cybersecurity strategies into the design and use of academic applications strengthened information protection, promoting more reliable and resilient digital platforms.

INTRODUCCIÓN

En el marco digital contemporáneo, la computación se consolidó como un eje estructural en la configuración de los procesos educativos, al posibilitar el desarrollo, la implementación y la expansión de aplicaciones académicas orientadas a la enseñanza, el aprendizaje y la gestión institucional. La incorporación de sistemas de gestión del aprendizaje, plataformas de evaluación en línea y plataformas colaborativas virtuales permitió ampliar el acceso al conocimiento, flexibilizar las modalidades educativas y optimizar la interacción entre docentes, estudiantes y administradores. Este avance, sostenido por la evolución de las tecnologías de la información y la comunicación, redefinió las dinámicas formativas y

favoreció la consolidación de ecosistemas educativos digitales cada vez más interconectados, dinámicos y dependientes de infraestructuras tecnológicas complejas (UNESCO, 2021; Guillén-Gámez et al., 2024).

No obstante, el crecimiento acelerado de estas plataformas de formación digital estuvo acompañado por un incremento significativo de los riesgos asociados a la seguridad de la información. La interconectividad, el almacenamiento masivo de datos y la exposición constante a redes abiertas ampliaron la superficie de ataque de las aplicaciones académicas, situando a la ciberseguridad como un componente crítico para la sostenibilidad de los procesos educativos digitales (ENISA, 2021; Karthikeyan, 2024). En este contexto, las instituciones educativas enfrentaron amenazas diversas, tales como ataques de denegación de servicio, accesos no autorizados, suplantación de identidad, vulneración de credenciales y filtración de datos sensibles, comprometiendo la confidencialidad, integridad y disponibilidad de la información (World Economic Forum, 2020; Chaudhuri & Shoemaker, 2025).

Desde una perspectiva sistémica, la protección de aplicaciones académicas trascendió la implementación de soluciones tecnológicas aisladas para constituirse en un proceso integral que articuló políticas institucionales, estándares internacionales de seguridad, gestión de riesgos y prácticas de uso responsable (ISO/IEC, 2022; Kumar et al., 2024). La ciberseguridad, en este sentido, se integró como un componente transversal que vinculó la dimensión técnica con la dimensión formativa, al reconocer que la seguridad no depende exclusivamente de herramientas como el cifrado de datos, los sistemas de autenticación o los controles de acceso, sino también de la conducta y el nivel de preparación de los usuarios (Armas & Taherdoost, 2025; Sarker, 2021). Esta visión integral resultó fundamental en contextos educativos donde la diversidad de perfiles tecnológicos y la heterogeneidad de competencias digitales incidieron directamente en la exposición a vulnerabilidades.

En el ámbito educativo, la relación entre computación y ciberseguridad adquirió una relevancia particular al incorporarse como parte del desarrollo de competencias digitales. La formación contemporánea demandó no solo el dominio instrumental de plataformas y aplicaciones, sino también la comprensión de los riesgos asociados a su uso, la adopción de prácticas seguras y la construcción de una cultura de protección de la información (Mukherjee et al., 2024; Swartz & Nayak, 2024). En consecuencia, la educación digital se orientó progresivamente hacia un enfoque que integró la seguridad como elemento formativo, promoviendo en estudiantes y docentes habilidades para identificar amenazas, gestionar credenciales de manera segura y utilizar de forma responsable los recursos tecnológicos disponibles (Ferhataj et al., 2024; Barbosa, 2024).

A pesar de los avances en el diseño de arquitecturas seguras y en la adopción de marcos normativos internacionales, persistieron limitaciones significativas en la implementación efectiva de medidas de ciberseguridad en aplicaciones académicas. Estas limitaciones se evidenciaron con mayor intensidad en contextos donde los recursos tecnológicos resultaron insuficientes o las políticas institucionales carecieron de actualización (Gulyamov et al., 2024; Zafar et al., 2024). Se identificó una brecha en la formación en ciberseguridad tanto en docentes como en estudiantes, lo que incrementó la vulnerabilidad frente a amenazas emergentes y prácticas inadecuadas en el uso de plataformas de formación digital (Rodríguez-Correa et al., 2025; Lazarov et al., 2025). Esta situación puso de manifiesto la necesidad de abordar la seguridad desde un enfoque integral que considere tanto los aspectos técnicos como los formativos y organizacionales.

En este escenario, la investigación se orientó a examinar la interrelación entre la computación y la ciberseguridad en la protección de aplicaciones académicas dentro de los procesos de formación digital. Se procuró analizar las principales vulnerabilidades presentes en dichas aplicaciones, así como evaluar la efectividad de los mecanismos de seguridad implementados en contextos educativos. De igual manera, se consideró fundamental explorar el papel de la formación en competencias digitales seguras como un factor determinante en la mitigación de riesgos cibernéticos y en el fortalecimiento de la resiliencia de las plataformas de formación digital.

En coherencia con este planteamiento, la investigación se guio por la siguiente pregunta: *¿de qué manera la integración de estrategias de ciberseguridad en la computación influyó en la protección de aplicaciones académicas en los procesos de formación digital?*

En correspondencia con esta interrogante, el objetivo general consistió en analizar la influencia de la ciberseguridad en la protección de aplicaciones académicas en plataformas de formación digital, con el propósito de fortalecer la seguridad de la información y la confiabilidad de los sistemas educativos. De este objetivo se derivaron objetivos específicos orientados a identificar las principales vulnerabilidades presentes en las aplicaciones académicas utilizadas en contextos educativos, evaluar la efectividad de los mecanismos de seguridad implementados en dichas aplicaciones y examinar el papel de la formación en competencias digitales seguras como estrategia para la prevención y mitigación de riesgos cibernéticos.

En síntesis, la investigación se fundamentó en la necesidad de articular la computación y la ciberseguridad como un eje estratégico en la educación digital contemporánea, reconociendo que la protección de las aplicaciones académicas dependió tanto de la implementación de soluciones tecnológicas robustas como

del fortalecimiento de las competencias digitales de los usuarios y de la consolidación de políticas institucionales coherentes. Este enfoque permitió aportar una visión integral orientada a la mejora de la seguridad en las plataformas de formación digital y al desarrollo de una cultura de prevención frente a las amenazas cibernéticas, contribuyendo así a la construcción de sistemas educativos más seguros, confiables y resilientes.

En este contexto, el presente estudio aporta evidencia empírica relevante sobre la relación entre la computación y la ciberseguridad en la protección de aplicaciones académicas en plataformas de formación digital, contribuyendo a la comprensión de los factores que inciden en la seguridad de la información en el ámbito educativo. A partir del análisis de los resultados obtenidos, se busca no solo describir la situación actual, sino también generar conocimiento aplicable que permita fortalecer las estrategias de protección en aplicaciones académicas, considerando la interacción entre los componentes tecnológicos, humanos e institucionales.

MATERIALES Y MÉTODOS

La investigación se desarrolló bajo un enfoque metodológico cuantitativo con alcance descriptivo y analítico, orientado a examinar la relación entre la computación y la ciberseguridad en la protección de aplicaciones académicas en plataformas de formación digital. Este enfoque permitió abordar el fenómeno desde una perspectiva objetiva, centrada en la medición y el análisis de variables asociadas a la seguridad de la información y al uso de aplicaciones educativas. Con este planteamiento, se adoptó un diseño no experimental de corte transversal, en el cual las variables no fueron manipuladas deliberadamente, sino observadas en su contexto natural durante un periodo determinado, lo que facilitó la comprensión de las condiciones reales de operación de las aplicaciones académicas y de los mecanismos de seguridad implementados en escenarios educativos.

El estudio se sustentó en una estrategia metodológica que integró diversas técnicas de recolección de datos, con el propósito de obtener una visión amplia y consistente del fenómeno analizado. En primer lugar, se realizó una revisión documental exhaustiva que incluyó artículos científicos indexados, informes técnicos especializados y normativas internacionales relacionadas con la ciberseguridad y la protección de la información en plataformas de formación digital educativas. Este proceso permitió establecer un marco teórico sólido y actualizado, así como identificar criterios y estándares de referencia para el análisis de las aplicaciones académicas. La selección de las fuentes se basó en criterios de pertinencia temática, actualidad y rigor científico, priorizando publicaciones reconocidas en el ámbito de la computación y la seguridad informática.

De manera complementaria, se llevó a cabo un análisis técnico de aplicaciones académicas utilizadas en contextos de educación superior, con el fin de identificar vulnerabilidades y evaluar los mecanismos de protección implementados. Este análisis se centró en aspectos críticos de la seguridad, tales como los sistemas de autenticación, la gestión de credenciales, las políticas de control de acceso, el uso de protocolos seguros para la transmisión de datos y la implementación de mecanismos de cifrado. Se consideraron elementos relacionados con la gestión de sesiones, la protección frente a ataques comunes y la configuración general de seguridad de las plataformas. La evaluación técnica se realizó a partir de criterios previamente definidos, alineados con buenas prácticas internacionales en materia de ciberseguridad, lo que permitió garantizar la consistencia y comparabilidad de los resultados obtenidos.

La población objeto de estudio estuvo conformada por usuarios de aplicaciones académicas en instituciones de educación superior, incluyendo estudiantes, docentes y personal administrativo que interactúan de manera habitual con sistemas de gestión del aprendizaje y otras herramientas digitales institucionales. La muestra se seleccionó mediante un muestreo no probabilístico de tipo intencional, considerando como criterio principal la experiencia en el uso de plataformas de formación digital. Esta selección permitió acceder a participantes con conocimiento práctico sobre el funcionamiento de las plataformas, lo que favoreció la obtención de información relevante en relación con la percepción de seguridad, las prácticas de uso y el nivel de formación en ciberseguridad.

Para la recolección de datos se diseñó un cuestionario estructurado con preguntas cerradas, orientado a medir variables relacionadas con la seguridad percibida, la frecuencia de incidentes de seguridad, el uso de mecanismos de protección y el nivel de competencias digitales seguras. El instrumento fue elaborado a partir de la operacionalización de las variables de estudio, asegurando la correspondencia entre los ítems y los objetivos de la investigación. La validez de contenido se garantizó mediante el juicio de expertos en las áreas de computación y seguridad informática, quienes evaluaron la pertinencia, claridad y coherencia de los ítems propuestos. Posteriormente, se realizó una prueba piloto con un grupo reducido de participantes con características similares a la población objetivo, lo que permitió identificar posibles ambigüedades y

realizar los ajustes necesarios para mejorar la confiabilidad del instrumento antes de su aplicación definitiva.

Adicionalmente, se empleó una guía de análisis técnico diseñada específicamente para evaluar las condiciones de seguridad de las aplicaciones académicas seleccionadas. Esta guía permitió sistematizar la revisión de los componentes de seguridad, facilitando la identificación de fortalezas y debilidades en la implementación de medidas de protección. La información obtenida a través de este análisis se contrastó con los datos recolectados mediante el cuestionario, lo que permitió establecer relaciones entre la percepción de los usuarios y las condiciones reales de seguridad de las plataformas evaluadas.

El procesamiento y análisis de los datos se llevó a cabo mediante técnicas estadísticas descriptivas, apoyadas en el uso de herramientas informáticas especializadas para la organización, codificación y análisis de la información. Se calcularon frecuencias absolutas y relativas, así como medidas de tendencia central, lo que permitió describir el comportamiento de las variables en función de los objetivos planteados. Se realizó un análisis comparativo entre los resultados obtenidos del cuestionario y los hallazgos del análisis técnico, con el propósito de identificar coincidencias y discrepancias que permitieran profundizar en la comprensión del fenómeno estudiado.

En relación con los aspectos éticos, la investigación se desarrolló conforme a principios de confidencialidad, anonimato y uso responsable de la información. Los participantes fueron informados previamente sobre los objetivos del estudio, la naturaleza de su participación y el tratamiento de los datos, tras lo cual se obtuvo su consentimiento informado. Se garantizó que la información recolectada fuera utilizada exclusivamente con fines académicos y que no se comprometiera la identidad de los participantes ni la seguridad de las instituciones involucradas. Se mantuvo el rigor metodológico y la integridad científica durante todas las fases del proceso investigativo.

En conjunto, la metodología empleada permitió abordar de manera integral la problemática de la ciberseguridad en aplicaciones académicas, articulando el análisis teórico, la evaluación técnica y la percepción de los usuarios. Este enfoque favoreció la obtención de resultados consistentes y contextualizados, aportando evidencia relevante para la comprensión de los desafíos asociados a la protección de aplicaciones educativas en plataformas de formación digital.

RESULTADOS Y DISCUSIÓN

Los resultados obtenidos permitieron analizar de manera integral la relación entre la ciberseguridad y la protección de aplicaciones académicas en plataformas de formación digital, considerando tanto la percepción de los usuarios como la evaluación técnica de las plataformas. Este enfoque facilitó la comprensión del fenómeno desde una doble perspectiva, en la que convergen la experiencia de uso y las condiciones reales de seguridad implementadas. A continuación, se presentan los hallazgos organizados en tablas, acompañados de su respectiva interpretación, con el propósito de evidenciar patrones, tendencias y relaciones significativas en función de los objetivos planteados.

En primer lugar, se examinó el nivel de percepción de seguridad en las aplicaciones académicas por parte de los usuarios, tomando en cuenta su interacción cotidiana con los sistemas digitales institucionales.

Tabla 1: Nivel de percepción de seguridad en aplicaciones académicas

Nivel de percepción	Frecuencia	Porcentaje (%)	Categoría de usuario
Alto	45	30%	Docentes
Medio	60	40%	Estudiantes
Bajo	30	20%	Administrativos
Muy bajo	15	10%	Mixto

Nota. Datos obtenidos del cuestionario aplicado a usuarios de aplicaciones académicas. *Fuente: Elaboración propia*.

Previo a la interpretación, los datos de la Tabla 1 evidenciaron una distribución heterogénea en la percepción de seguridad, lo que permitió identificar distintos niveles de confianza en las plataformas de formación digital utilizadas.

Se mostró que el nivel de percepción predominante fue medio, con un 40%, lo que indicó una confianza moderada en las aplicaciones académicas. Este resultado sugirió que, si bien los usuarios reconocieron la existencia de medidas de protección, estas no fueron percibidas como completamente suficientes.

Asimismo, un 30% manifestó un nivel alto de seguridad, lo que evidenció que ciertas aplicaciones académicas lograron transmitir confianza mediante la implementación visible de mecanismos de protección. Sin embargo, el 30% acumulado entre los niveles bajo y muy bajo reflejó una percepción de vulnerabilidad significativa, asociada posiblemente a experiencias previas con incidentes o a un limitado conocimiento en ciberseguridad, lo que afectó la valoración general de la seguridad en las plataformas.
Posteriormente, se analizó la frecuencia de incidentes de seguridad reportados por los usuarios, con el fin de identificar las principales amenazas presentes en las aplicaciones académicas.

Tabla 2: Frecuencia de incidentes de seguridad en aplicaciones académicas

Tipo de incidente	Frecuencia	Porcentaje (%)	Nivel de impacto
Acceso no autorizado	50	33%	Alto
Pérdida de datos	30	20%	Medio
Ataques de phishing	40	27%	Alto
Fallos de autenticación	30	20%	Medio

Nota. Clasificación basada en reportes de usuarios durante el periodo de estudio. *Fuente: Elaboración propia.*

Antes de su interpretación, los datos reflejaron la presencia recurrente de incidentes vinculados principalmente con debilidades en la gestión de accesos y en la interacción de los usuarios con las plataformas.
En relación con lo anterior, la Tabla 2 evidenció que el acceso no autorizado constituyó el incidente más frecuente, con un 33%, seguido por los ataques de phishing con un 27%. Estos resultados señalaron vulnerabilidades tanto en los sistemas de autenticación como en la concienciación de los usuarios frente a amenazas digitales. La pérdida de datos y los fallos de autenticación, aunque con menor proporción, representaron riesgos relevantes que afectaron la integridad y disponibilidad de la información. En conjunto, estos hallazgos confirmaron que las aplicaciones académicas continúan expuestas a amenazas comunes, lo que evidencia la necesidad de fortalecer los mecanismos de seguridad y la formación preventiva de los usuarios.
Seguidamente, se evaluaron los mecanismos de seguridad implementados en las aplicaciones académicas, con el propósito de identificar el nivel de adopción de medidas técnicas de protección.

Tabla 3: Mecanismos de seguridad implementados en aplicaciones académicas

Mecanismo de seguridad	Frecuencia	Porcentaje (%)	Nivel de implementación
Autenticación multifactor	35	23%	Medio
Cifrado de datos	55	37%	Alto
Control de accesos	40	27%	Medio
Monitoreo de actividad	20	13%	Bajo

Nota. Evaluación técnica de aplicaciones educativas analizadas. *Fuente: Elaboración propia.*

De manera previa, los datos permitieron observar diferencias significativas en la implementación de mecanismos de seguridad, lo que evidenció distintos niveles de madurez en la protección de las aplicaciones.
En efecto, la Tabla 3 mostró que el cifrado de datos fue el mecanismo más implementado, con un 37%, lo que indicó un avance importante en la protección de la información durante su transmisión y almacenamiento. Sin embargo, la autenticación multifactor presentó un nivel de adopción relativamente bajo, con un 23%, lo que evidenció una debilidad crítica en la prevención de accesos no autorizados. Asimismo, el monitoreo de actividad registró el nivel más bajo de implementación, lo que limitó la capacidad de detección temprana de incidentes y respuesta ante amenazas. Estos resultados reflejaron la necesidad de fortalecer la implementación de mecanismos avanzados que permitan una protección más integral de las aplicaciones académicas.
En continuidad con el análisis, se exploró el nivel de formación en ciberseguridad de los usuarios, considerando su influencia en la prevención de riesgos en plataformas de formación digital.

Tabla 4: Nivel de formación en ciberseguridad de los usuarios

Nivel de formación	Frecuencia	Porcentaje (%)	Grupo predominante
Alto	25	17%	Docentes
Medio	50	33%	Estudiantes
Bajo	55	37%	Estudiantes
Nulo	20	13%	Administrativos

Nota. Evaluación basada en autopercepción de conocimientos en seguridad digital. *Fuente: Elaboración propia.*

Previo a su análisis, los datos evidenciaron una distribución que reflejó limitaciones en la preparación de los usuarios frente a riesgos cibernéticos.
En este contexto, la Tabla 4 indicó que el nivel de formación predominante fue bajo, con un 37%, seguido de un nivel medio con 33%, lo que evidenció una preparación insuficiente para enfrentar amenazas digitales. La baja proporción de usuarios con formación alta, correspondiente al 17%, reflejó una debilidad en la capacitación formal en ciberseguridad, especialmente en el grupo estudiantil. Este hallazgo puso de manifiesto la necesidad de fortalecer la educación en competencias digitales seguras, dado que el factor humano constituye un elemento determinante en la prevención de incidentes de seguridad.
Finalmente, se analizó la relación entre el nivel de seguridad implementado y la frecuencia de incidentes reportados, con el fin de identificar posibles asociaciones entre estas variables.

Tabla 5: Relación entre medidas de seguridad y reducción de incidentes

Nivel de seguridad implementado	Frecuencia	Porcentaje (%)	Incidentes reportados
Alto	40	27%	Bajo
Medio	60	40%	Medio
Bajo	50	33%	Alto

Nota. Relación establecida a partir del análisis comparativo de datos. *Fuente: Elaboración propia.*

Antes de su interpretación, los datos evidenciaron una tendencia clara en la relación entre el nivel de seguridad y la ocurrencia de incidentes.
En consecuencia, la Tabla 5 demostró que las aplicaciones con altos niveles de seguridad presentaron una menor incidencia de problemas, mientras que aquellas con niveles bajos registraron una mayor frecuencia de incidentes. Este comportamiento confirmó la existencia de una relación directa entre la implementación de medidas de ciberseguridad y la reducción de riesgos, lo que validó la importancia de adoptar estrategias de protección robustas y sostenidas en el tiempo. Se evidenció que los niveles intermedios de seguridad generaron resultados moderados, lo que sugiere que la implementación parcial de medidas no resulta suficiente para garantizar una protección efectiva.
En conjunto, los resultados evidenciaron que, aunque se han logrado avances en la implementación de mecanismos de seguridad en aplicaciones académicas, persisten debilidades relevantes tanto en el ámbito técnico como en la formación de los usuarios. La percepción de seguridad moderada, la frecuencia de incidentes asociados a accesos no autorizados y phishing, así como la limitada adopción de medidas avanzadas como la autenticación multifactor, configuran un escenario que requiere una intervención integral. En síntesis, se observó que la protección de las aplicaciones académicas depende de la articulación entre infraestructura tecnológica, políticas de seguridad y formación en competencias digitales, lo que permite fortalecer la resiliencia de las aplicaciones académicas frente a amenazas cibernéticas y garantizar la confiabilidad de los procesos de formación digital.
En la discusión de los resultados, los hallazgos obtenidos permitieron profundizar en la comprensión de la relación entre la computación y la ciberseguridad en la protección de aplicaciones académicas en plataformas de formación digital, evidenciando un escenario caracterizado por avances significativos, pero también por limitaciones estructurales que inciden directamente en la seguridad de la información. La interpretación de los datos se realizó desde una perspectiva crítica e integradora, contrastando los resultados empíricos con los fundamentos teóricos y las tendencias contemporáneas en seguridad informática aplicada

al ámbito educativo (Kumar et al., 2024; Mukherjee et al., 2024; Karthikeyan, 2024; Sarker, 2021), lo que permitió contextualizar los hallazgos y valorar su alcance en términos científicos y prácticos.

En relación con la percepción de seguridad, el predominio de un nivel medio entre los usuarios reflejó una confianza parcial en las aplicaciones académicas, lo cual sugiere que las medidas de protección implementadas han logrado generar cierto grado de credibilidad, pero no han alcanzado un nivel suficiente para consolidar una percepción de seguridad robusta (Barbosa, 2024; Guillén-Gámez et al., 2024). Esta situación pone de manifiesto que la seguridad, además de ser un atributo técnico, constituye una construcción subjetiva influida por la experiencia de uso, la visibilidad de los mecanismos de protección y el nivel de conocimiento de los usuarios. La coexistencia de percepciones divergentes evidenció una heterogeneidad que puede atribuirse a diferencias en la calidad de las plataformas, en la consistencia de las políticas de seguridad y en las competencias digitales de los usuarios (UNESCO, 2021). Desde el punto de vista teórico, estos resultados se alinean con enfoques que sostienen que la confianza en los sistemas digitales depende tanto de la eficacia técnica como de la percepción de control y transparencia en la gestión de la información (Armas & Taherdoost, 2025; Gulyamov et al., 2024).

En cuanto a la frecuencia de incidentes de seguridad, la predominancia de accesos no autorizados y ataques de phishing permitió identificar un patrón claro de vulnerabilidades asociadas a la autenticación y al comportamiento del usuario (Chaudhuri & Shoemaker, 2025; ENISA, 2021). Estos resultados confirmaron que las amenazas más frecuentes en aplicaciones académicas no solo responden a fallas técnicas, sino también a estrategias de ingeniería social que explotan debilidades humanas (Sarker, 2021). La recurrencia de estos incidentes evidenció que la protección de los sistemas no puede limitarse a la implementación de barreras tecnológicas, sino que debe complementarse con procesos de formación y concienciación orientados a fortalecer la capacidad de los usuarios para reconocer y evitar riesgos (Ferhataj et al., 2024; Dupuis et al., 2025). Este hallazgo coincide con la literatura especializada que identifica al factor humano como uno de los componentes más críticos en la gestión de la ciberseguridad, especialmente en plataformas donde la interacción constante incrementa la exposición a amenazas (Zafar et al., 2024; Ramezan et al., 2023).

El análisis de los mecanismos de seguridad implementados permitió identificar una adopción desigual de medidas de protección, lo que refleja distintos niveles de madurez en la gestión de la ciberseguridad dentro de las aplicaciones académicas (Kumar et al., 2024). El predominio del cifrado de datos evidenció una preocupación por garantizar la confidencialidad de la información, lo cual constituye un avance relevante en la protección de los datos durante su transmisión y almacenamiento (ISO/IEC, 2022). Sin embargo, la limitada implementación de mecanismos como la autenticación multifactor y el monitoreo continuo de actividad puso de manifiesto debilidades en la prevención y detección de accesos indebidos (Mukherjee et al., 2024; Karthikeyan, 2024). Esta situación sugiere que las instituciones educativas han priorizado medidas fundamentales, pero aún no han consolidado un enfoque integral basado en la defensa en profundidad, donde múltiples capas de seguridad interactúan de manera coordinada para reducir el riesgo de incidentes (ENISA, 2021). Desde una perspectiva analítica, esta fragmentación en la implementación de medidas limita la efectividad global de los sistemas de protección y expone a las aplicaciones a vulnerabilidades evitables.

En lo que respecta a la formación en ciberseguridad, los resultados evidenciaron un nivel predominantemente bajo entre los usuarios, con especial énfasis en el grupo estudiantil, lo que constituye uno de los aspectos más críticos identificados en la investigación (Barbosa, 2024; Spencer, 2024). Este hallazgo pone de relieve que la vulnerabilidad de las aplicaciones académicas no depende únicamente de factores tecnológicos, sino que está estrechamente vinculada al nivel de preparación de quienes interactúan con ellas (Ferhataj et al., 2024). La insuficiente formación limita la capacidad de los usuarios para adoptar prácticas seguras, gestionar adecuadamente sus credenciales y responder de manera efectiva ante posibles amenazas (Swartz & Nayak, 2024). En este sentido, la discusión permite sostener que la ciberseguridad debe integrarse como un componente esencial de la educación digital, trascendiendo el ámbito técnico para convertirse en un elemento formativo que promueva una cultura de seguridad (Armas & Taherdoost, 2025; Tian, 2025). La incorporación de contenidos relacionados con la protección de la información en los programas académicos contribuiría significativamente a reducir la exposición a riesgos y a fortalecer la resiliencia de las plataformas de formación digital (Rodríguez-Correa et al., 2025; Lazarov et al., 2025).

Por otra parte, la relación identificada entre el nivel de seguridad implementado y la reducción de incidentes permitió confirmar que la adopción de medidas robustas tiene un impacto directo en la protección de las aplicaciones académicas (Kumar et al., 2024; Mukherjee et al., 2024). Los resultados evidenciaron que aquellas plataformas con mayores niveles de seguridad presentaron una menor incidencia de problemas, lo que valida la efectividad de estrategias integrales que combinan múltiples mecanismos de protección (ISO/IEC, 2022). Este hallazgo refuerza la importancia de adoptar enfoques sistémicos en la gestión de la ciberseguridad, en los que la implementación de tecnologías avanzadas se complemente con políticas

institucionales claras y procesos de mejora continua (ENISA, 2021). Asimismo, pone de manifiesto que la seguridad debe ser concebida como un proceso dinámico, capaz de adaptarse a la evolución constante de las amenazas y a los cambios en las plataformas tecnológicas (World Economic Forum, 2020).

Desde una perspectiva global, los resultados discutidos evidenciaron que la protección de aplicaciones académicas en plataformas de formación digital constituye un desafío complejo que requiere la articulación de factores tecnológicos, humanos e institucionales (Zafar et al., 2024). La computación, como base del desarrollo de estas aplicaciones, debe incorporar principios de seguridad desde las etapas iniciales de diseño, adoptando enfoques como la seguridad por defecto y la seguridad por diseño (ISO/IEC, 2022). Paralelamente, la ciberseguridad debe integrarse como un eje estratégico en la gestión educativa, orientando la toma de decisiones hacia la implementación de prácticas sostenibles y alineadas con estándares internacionales (ENISA, 2021; UNESCO, 2021).

En este contexto, la investigación permitió identificar la necesidad de avanzar hacia modelos de seguridad proactivos, que prioricen la prevención, el monitoreo continuo y la respuesta temprana ante incidentes (Chaudhuri & Shoemaker, 2025). La discusión también evidenció la importancia de fortalecer la gobernanza de la seguridad en las instituciones educativas, promoviendo la adopción de marcos normativos, la asignación de recursos adecuados y la capacitación permanente de los usuarios (Kumar et al., 2024; Rodríguez-Correa et al., 2025). Este enfoque integral contribuiría a consolidar una cultura organizacional orientada a la protección de la información, en la que la seguridad no sea percibida como una responsabilidad exclusiva del área técnica, sino como un compromiso compartido por toda la comunidad educativa (Armas & Taherdoost, 2025).

En definitiva, los hallazgos analizados permitieron confirmar que la integración efectiva de la ciberseguridad en la computación aplicada a la educación constituye un factor determinante para la protección de las aplicaciones académicas (Mukherjee et al., 2024; Tian, 2025). La discusión evidenció que, aunque se han logrado avances relevantes, persisten desafíos significativos que requieren una respuesta articulada, sostenida y basada en la mejora continua (World Economic Forum, 2020). La consolidación de plataformas de formación digital seguras dependerá de la capacidad de las instituciones para equilibrar la innovación tecnológica con la implementación de estrategias de seguridad robustas y el fortalecimiento de las competencias digitales de los usuarios, garantizando así la confiabilidad, integridad y sostenibilidad de los procesos formativos en la era digital (ENISA, 2021; UNESCO, 2021).

CONCLUSIÓN

La investigación permitió analizar de manera integral la relación entre la computación y la ciberseguridad en la protección de aplicaciones académicas en plataformas de formación digital, evidenciando que la seguridad de la información constituye un componente estructural para garantizar la confiabilidad, continuidad y calidad de los procesos educativos mediados por tecnologías. A partir de los resultados obtenidos, se confirmó que la integración de estrategias de ciberseguridad en el desarrollo, implementación y uso de aplicaciones académicas influyó de manera significativa en la reducción de riesgos y en el fortalecimiento de las plataformas de formación digital, consolidando su papel como un elemento indispensable dentro de la transformación digital educativa.

Uno de los principales aportes del estudio radicó en la identificación de vulnerabilidades persistentes en las aplicaciones académicas, particularmente en los mecanismos de autenticación, la gestión de accesos y la exposición a ataques basados en ingeniería social. Estas debilidades evidenciaron que, a pesar de los avances tecnológicos, subsisten brechas relevantes en la implementación de medidas de seguridad, lo que incrementa la exposición a incidentes que pueden comprometer tanto la integridad de los sistemas como la confidencialidad de la información. En consecuencia, se concluyó que la protección efectiva de las aplicaciones académicas no puede abordarse desde una perspectiva exclusivamente técnica, sino que requiere una visión integral que articule componentes tecnológicos, organizacionales y formativos, orientados a garantizar una protección sostenible y adaptativa frente a amenazas emergentes.

De igual manera, se determinó que la percepción de seguridad de los usuarios no siempre se corresponde con las condiciones reales de las plataformas, lo que pone de manifiesto la existencia de una brecha entre la implementación técnica de los mecanismos de protección y la confianza que estos generan en la comunidad educativa. Este hallazgo permitió concluir que la seguridad no solo debe ser efectiva, sino también perceptible, lo que implica la necesidad de fortalecer la comunicación institucional, la transparencia en las políticas de protección y la sensibilización de los usuarios respecto a las medidas implementadas. En este sentido, la construcción de confianza se posiciona como un factor clave para el uso adecuado y seguro de las aplicaciones académicas.

Otro aspecto relevante derivado de la investigación fue el bajo nivel de formación en ciberseguridad evidenciado en los usuarios, especialmente en los estudiantes, lo que confirmó que la vulnerabilidad de las

plataformas de formación digital no depende únicamente de factores técnicos, sino también del comportamiento humano y del nivel de competencias digitales. Este resultado permitió establecer que la formación en ciberseguridad constituye un elemento estratégico para la prevención de riesgos, ya que contribuye al desarrollo de habilidades orientadas a la identificación de amenazas, la adopción de prácticas seguras y la respuesta oportuna ante incidentes. En consecuencia, se concluyó que la educación en seguridad digital debe integrarse de manera transversal en los procesos formativos, consolidándose como un componente esencial de la alfabetización digital contemporánea.

Los resultados confirmaron que la implementación de medidas de seguridad robustas, tales como el cifrado de datos, el control de accesos y la autenticación multifactor, se asocia con una disminución significativa en la ocurrencia de incidentes de seguridad. Este hallazgo permitió reafirmar que la adopción de estrategias integrales de ciberseguridad no solo mejora la protección de las aplicaciones académicas, sino que también fortalece la resiliencia de los sistemas educativos frente a amenazas cada vez más sofisticadas. En este contexto, la ciberseguridad dejó de ser concebida como un componente complementario para consolidarse como un eje estratégico en la gestión de la educación digital, imprescindible para la sostenibilidad de los procesos formativos.

Desde una perspectiva global, la investigación evidenció que la protección de aplicaciones académicas en plataformas de formación digital depende de la convergencia entre la computación y la ciberseguridad, entendidas como dimensiones interdependientes que deben integrarse desde las fases iniciales de diseño, desarrollo e implementación de las tecnologías educativas. Se concluyó que la consolidación de plataformas de formación digital seguros requiere no solo el fortalecimiento de la infraestructura tecnológica, sino también la implementación de políticas institucionales coherentes, la adopción de estándares internacionales y el desarrollo continuo de competencias digitales seguras en todos los actores del proceso educativo. Este enfoque integral permitió aportar una visión orientada a la mejora de la seguridad de la información, destacando la importancia de la prevención, la gestión de riesgos y la cultura organizacional como elementos clave para la protección de los sistemas educativos digitales.

En síntesis, los hallazgos del estudio permitieron confirmar que la integración efectiva de la ciberseguridad en la computación aplicada a la educación constituye un factor determinante para la protección de las aplicaciones académicas, así como para su construcción confiable, resiliente y sostenible. La investigación aportó evidencia relevante que contribuye al desarrollo de estrategias orientadas a fortalecer la seguridad en el ámbito educativo, reconociendo que los desafíos actuales exigen respuestas articuladas, dinámicas y basadas en la mejora continua.

Finalmente, los resultados de la investigación poseen una clara proyección práctica, ya que ofrecen insumos relevantes para la toma de decisiones en instituciones educativas en materia de ciberseguridad. La aplicabilidad de los hallazgos permite orientar el diseño e implementación de estrategias más efectivas para la protección de la información en aplicaciones académicas, favoreciendo el desarrollo de plataformas de formación digital más seguras, confiables y adaptadas a las exigencias actuales del entorno tecnológico.

En cuanto a las recomendaciones, se considera fundamental que las instituciones educativas fortalezcan la implementación de políticas de ciberseguridad alineadas con estándares internacionales, promoviendo la adopción de mecanismos avanzados de protección como la autenticación multifactor, el monitoreo continuo y la gestión proactiva de vulnerabilidades. Asimismo, resulta imprescindible integrar la ciberseguridad como un componente transversal en los programas de formación, con el propósito de desarrollar competencias digitales seguras en estudiantes, docentes y personal administrativo, favoreciendo una cultura de prevención y uso responsable de las tecnologías. De igual forma, se recomienda establecer procesos sistemáticos de evaluación y actualización de las aplicaciones académicas, que permitan identificar y mitigar riesgos de manera oportuna frente a la evolución de las amenazas cibernéticas. Finalmente, se sugiere promover una cultura organizacional orientada a la seguridad de la información, en la que la protección de los sistemas digitales sea asumida como una responsabilidad compartida, garantizando así aplicaciones académicas más seguras, confiables y preparados para los desafíos de la transformación digital.

REFERENCIAS

Armas, R. & Taherdoost, H. (2025). Building a cybersecurity culture in higher education: Proposing a cybersecurity awareness paradigm. *Information*, *16*(5), 336. https://doi.org/10.3390/info16050336

Barbosa, J. (2024). Cybersecurity awareness and training in higher education: Student perceptions and needs. *WSEAS Transactions on Advances in Engineering Education*, *21*. https://doi.org/10.37394/232010.2024.21.12

Chaudhuri, A. & Shoemaker, D. (2025). Cyber-attack on schools – steps toward resilience. *EDPACS*, *70*(11), 63–71. https://doi.org/10.1080/07366981.2025.2503627

Dupuis, M., Honomichl, R., Zantua, M. & Ju, J. (2025). Cybersecurity high school innovations: A path for educators to teach cybersecurity courses in their schools. *Journal of the Colloquium for Information Systems Security Education*, *12*(1). https://doi.org/10.53735/cisse.v12i1.198

ENISA. (2021). *Cybersecurity in education*. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/cybersecurity-in-education

Ferhataj, A., Memaj, F., Sahatcija, R. & Ora, A. (2024). Strengthening cybersecurity education for university students: Bridging vulnerabilities and promoting proactive digital safety practices. *Millenium – Journal of Education, Technologies, and Health*. https://doi.org/10.29352/mill0227.41111

Guillén-Gámez, F. D., Tomczyk, Ł., Ruiz-Palmero, J. & Connolly, C. (2024). Digital security in educational contexts: Digital competence and challenges for good practice. *Computers in the Schools*, *41*(3). https://doi.org/10.1080/07380569.2024.2390319

Gulyamov, S., Babaev, J. & Rakhmatov, U. (2024). Building cybersecurity culture in education as imperative for youth to thrive in digital society. *Uzbek Journal of Law and Digital Policy*. https://doi.org/10.59022/ujldp.218

ISO/IEC. (2022). *ISO/IEC 27001: Information security management systems — Requirements*. https://www.iso.org/standard/27001

Karthikeyan, S. P. (2024). Cybersecurity in education: Safeguarding digital learning environments. *International Journal of Engineering and Technology Research*. https://doi.org/10.5281/zenodo.13645990

Kumar, A., Mishra, K., Mahto, R. K. & Mishra, B. K. (2024). A framework for institution to enhancing cybersecurity in higher education: A review. *LatIA*, *2*, 94. https://latia.ageditor.uy/index.php/latia/article/view/94

Lazarov, W., Schafeitel-Tähtinen, T., Squillace, J. & Martinasek, Z. (2025). Lessons learned from using cyber range to teach cybersecurity at different levels of education. *Technology, Knowledge and Learning*. https://doi.org/10.1007/s10758-025-09840-y

Mukherjee, M., Le, N. T., Chow, Y.-W. & Susilo, W. (2024). Strategic approaches to cybersecurity learning: A study of educational models and outcomes. *Information*, *15*(2), 117. https://doi.org/10.3390/info15020117

Ramezan, C. A., Coffy, P. M. & Lemons, J. (2023). Building the operational technology (OT) cybersecurity workforce: What are employers looking for? *Journal of Cybersecurity Education, Research and Practice*. https://doi.org/10.32727/8.2023.31

Rodríguez-Correa, P. A., Valencia-Arias, A., Martínez Rojas, E., Oré León, A., Mellin Rubio, R. H., Vásquez Coronado, M. H. & Jiménez García, J. A. (2025). Information security education: A thematic trend analysis. *F1000Research*. https://doi.org/10.12688/f1000research.159828.2

Sarker, I. H. (2021). Cybersecurity data science: An overview from machine learning perspective. *Journal of Big Data*, *8*, 1–29. https://doi.org/10.1186/s40537-021-00409-y

Spencer, A. (2024). Cyber science education within STEM. *Cybersecurity and Innovative Technology Journal*, *2*(2), 67–78. https://doi.org/10.52889/citj.v2i2.330

Swartz, S. & Nayak, D. (2024). Addressing the need for interculturality in cybersecurity education. *Journal of the Colloquium for Information Systems Security Education*, *11*(1). https://doi.org/10.53735/cisse.v11i1.176

Tian, J. (2025). Integrating artificial intelligence into the cybersecurity curriculum in higher education: A systematic literature review. *Education Sciences*, *15*(11), 1540. https://doi.org/10.3390/educsci15111540

UNESCO. (2021). *ICT competency framework for teachers*. https://unesdoc.unesco.org/ark:/48223/pf0000371024

World Economic Forum. (2020). *The global risks report 2020*. https://www.weforum.org/reports/the-global-risks-report-2020

Zafar, H., Hollingsworth, C. L., Bandyopadhyay, T. & Randolph, A. B. (2024). Collaborative pathways to cybersecurity excellence: Insights from industry and academia in the southeastern US. *Journal of Cybersecurity Education, Research and Practice*. https://doi.org/10.62915/2472-2707.1183