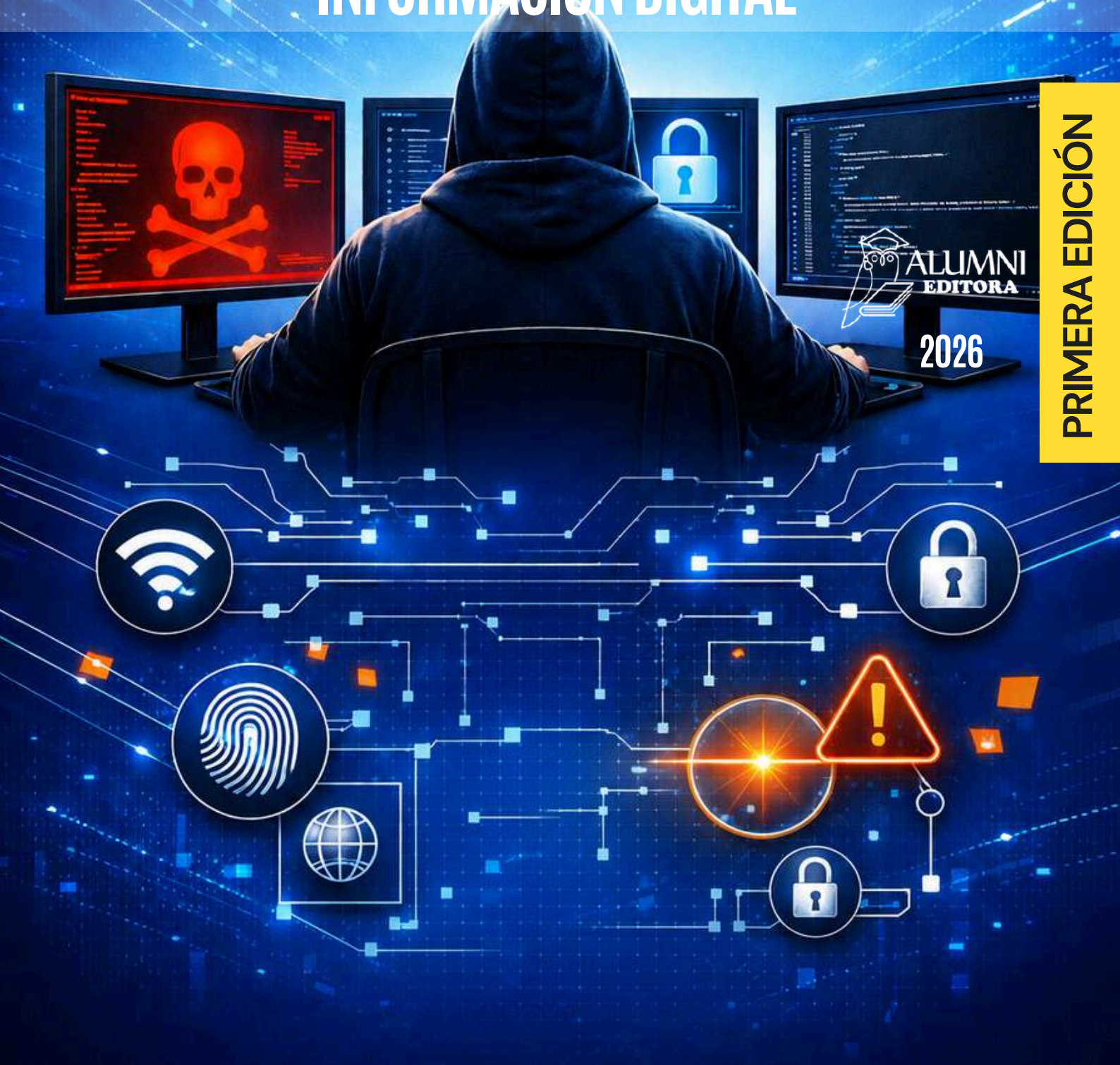
CIBERSEGURIDAD

APLICADA

ESTRATEGIAS PARA LA PROTECCIÓN DE APLICACIONES Y GESTIÓN SEGURA DE LA INFORMACIÓN DIGITAL



ALUMNI EDITORA

2026

PRIMERA EDICIÓN

Ciberseguridad aplicada: Estrategias para la protección de aplicaciones y gestión segura de la información digital

Autores

Ricardo Manuel Candanedo Yau

- Licenciado en Ingenieria de Sistemas Computacionales
- Magister de Gerencia de Sistemas con énfasis en Seguridad Informatica
- Magister en Entornos Virtuales de aprendizaje

https://orcid.org/0009-0002-5017-9830

ricardo.candanedo@up.ac.pa

Ciberseguridad aplicada: Estrategias para la protección de aplicaciones y gestión segura de la información digital

Catalogación Bibliográfica

Autores

- Ricardo Manuel Candanedo Yau

Título	Ciberseguridad aplicada: Estrategias para la protección de aplicaciones y gestión segura de la información digital
Descriptores	Seguridad informática, Evaluación de riesgos, Gestión de la información, Protección de datos, Tecnologías de la información
Dewey	005
Thema	UMT
Publicación	Mayo 2026
Edición	Primera
ISBN	978-9942-7465-5-9
DOI	https://doi.org/10.70625/alumned/30
Editorial	Alumni Editora
Pais - Ciudad	Ecuador - Atuntaqui
Formato	Adobe Acrobat Reader
Páginas	92

Cámara Ecuatoriana del Libro

Todo el contenido de este libro tiene una licencia de Creative Commons Attribution License. Reconocimiento-No Comercial-No Derivados 4.0 Internacional (CC BY-NC-ND 4.0).

El contenido del texto y sus datos en su forma, corrección y confiabilidad son de exclusiva responsabilidad del autor y no representan necesariamente la posición oficial de Alumni Editora. Se permite descargar la obra y compartirla siempre que se den los créditos al autor, pero sin posibilidad de alterarla de ninguna forma ni utilizarla con fines comerciales.

Ciberseguridad aplicada: Estrategias para la protección de aplicaciones y gestión segura de la información digital

Editor en Jefe

Santiago Andrés Otero, PhD., Alumni Editora, Ecuador

Equipo Editorial

- Óscar Gómez Jiménez, PhD., Universidad Internacional de Valencia (VIU), España
- Shashi Kant Gupta, PhD., Eudoxia Research University, Estados Unidos
- Anabell Fondón Ludeña, PhD., Universidad Rey Juan Carlos, España
- Edwin Ricardo Flores Hernández, PhD., Universidad Salvadoreña Alberto Masferrer, El Salvador
- Gopi Devarajan, PhD., SRM Institute of Science and Technology, India
- Flérida Moreno Alcaraz, PhD., Universidad Autónoma de Sinaloa, México
- J. Suresh Kumar, PhD., St. Joseph University, India
- Mauricio Lima Narváez, PhD., Universidad Técnica del Norte, Ecuador
- Héctor Luis López López , PhD., Universidad Autónoma de Sinaloa, México
- Samuel Helena Tumbula, PhD., Universidad Católica de Angola, Angola
- Carlos Bolivar Sarmiento Chugcho, PhD., Universidad Técnica de Machala, Ecuador
- Savier Fernando Acosta Faneite, PhD., Universidad del Zulia, Venezuela
- Mirian Alexandra Valeriano Meneses, PhD., Instituto Superior Tecnológico Liceo Aduanero, Ecuador
- Sivabalan Settu, PhD., CSE SoCI Vignan University Guntur, India
- Lorena Elizabeth Casanova Imbaquingo, MSc., Instituto Universitario Cotacachi, Ecuador
- Gladys Magdalena Paredes, MSc., Ministerio de Educación, Ecuador
- Henri Emmanuel López Gómez, MSc., Universidad Peruana Los Andes, Perú

El contenido del texto y sus datos en su forma, corrección y confiabilidad son de exclusiva responsabilidad del autor y no representan necesariamente la posición oficial de Alumni Editora. Se permite descargar la obra y compartirla siempre que se den los créditos al autor, pero sin posibilidad de alterarla de ninguna forma ni utilizarla con fines comerciales.

Peer Review Process

Revisión de Pares

Este libro ha sido evaluado mediante un proceso de revisión por pares externos bajo el formato de doble ciego. En consecuencia, la investigación presentada en esta obra cuenta con el respaldo de expertos en la materia, quienes han emitido un juicio imparcial basado en criterios científicos, garantizando así la solidez académica del contenido.

Peer Review

This book has undergone a peer review process by external academics using a double-blind system. Consequently, the research presented in this work has the endorsement of subject matter experts, who have provided an impartial assessment based on scientific criteria, ensuring the academic rigor of the content.

Declaración del Editor

Declaración del Editor

Alumni Editora declara para todos los efectos legales, que:

Esta publicación implica únicamente una cesión temporal de los derechos de autor y de publicación, sin que ello constituya responsabilidad solidaria en la creación de los manuscritos publicados en conformidad con la Ley de Propiedad Intelectual y las normativas legales aplicables.

Autoriza y fomenta que los autores firmen acuerdos con repositorios institucionales con el fin exclusivo de difundir la obra, siempre que se reconozca adecuadamente la autoría y la edición, y que no existan fines comerciales involucrados.

Todos los libros electrónicos publicados son de acceso abierto y, por lo tanto, no se venden en el sitio web de Alumni Editora, ni en plataformas asociadas, de comercio electrónico u otros medios virtuales o físicos, eximiéndose de la transferencia de derechos de autor a los autores.

Todos los miembros del consejo editorial cuentan con el grado académico de cuarto nivel y están vinculados a instituciones de educación superior, conforme a las recomendaciones de las entidades de evaluación académica nacionales e internacionales para la obtención de estándares de calidad editorial.

Alumni Editora no transfiere, comercializa, ni autoriza el uso de los nombres, correos electrónicos u otros datos personales de los autores para fines distintos a la difusión de esta obra.

Declaración del Autor

Declaración del Autor

El autor de la obra declara: 1. No poseer ningún interés comercial que pueda representar un conflicto de interés en relación con el presente documento publicado; 2. Asegura haber participado activamente en la elaboración del manuscrito, específicamente en la concepción del estudio, la obtención de datos y/o su análisis e interpretación; la redacción o revisión del documento para garantizar su relevancia intelectual y la aprobación final del manuscrito antes de su envío; 3. Certifica que el contenido publicado está libre de datos o resultados fraudulentos; 4. Confirma que todas las citas y referencias de datos e interpretaciones de investigaciones previas son correctas; 5. Reconoce haber declarado todas las fuentes de financiamiento recibidas para la investigación; 6. Autoriza la publicación de la obra, que incluye su inclusión en catálogos, asignación de ISBN, DOI, otros índices, diseño visual, portada, maquetación interior, y su posterior difusión según lo dispuesto por Alumni Editora.

Prólogo

La transformación digital ha redefinido profundamente la manera en que las organizaciones, las instituciones educativas y la sociedad gestionan la información y desarrollan sus procesos tecnológicos. En este escenario, la ciberseguridad ha dejado de ser un aspecto exclusivamente técnico para convertirse en un componente estratégico indispensable para la protección de aplicaciones, la continuidad operativa y la preservación de la confianza digital.

La creciente interconexión de sistemas, el uso masivo de plataformas digitales y la expansión de los servicios en línea han generado nuevas oportunidades para el acceso al conocimiento y la innovación. Sin embargo, también han incrementado los riesgos asociados a amenazas cibernéticas, vulnerabilidades tecnológicas y ataques dirigidos a comprometer la confidencialidad, integridad y disponibilidad de la información. Esta realidad exige una visión integral que combine tecnología, gestión de riesgos, cultura digital y formación permanente.

La presente obra, *Ciberseguridad Aplicada: Estrategias para la Protección de Aplicaciones y Gestión Segura de la Información Digital*, constituye un aporte significativo al análisis de los desafíos contemporáneos relacionados con la seguridad informática y la protección de los activos digitales. A través de un enfoque académico y aplicado, el libro desarrolla fundamentos conceptuales, marcos normativos internacionales y estrategias prácticas orientadas al fortalecimiento de la seguridad en entornos digitales complejos.

Uno de los principales méritos de esta obra radica en su capacidad para integrar la dimensión tecnológica con la dimensión educativa y organizacional, reconociendo que la ciberseguridad no depende únicamente de herramientas técnicas, sino también del comportamiento humano, la conciencia digital y la construcción de una cultura institucional orientada a la prevención y la resiliencia.

A lo largo de sus capítulos, el lector encontrará una reflexión crítica sobre la relación entre computación, ciberseguridad y protección de la información, así como propuestas metodológicas y modelos orientados al fortalecimiento de plataformas digitales seguros y sostenibles. De esta manera, el texto se convierte en una referencia valiosa para investigadores, docentes, estudiantes, profesionales del área tecnológica y responsables de la gestión de la información.

Prólogo

En un mundo donde los datos constituyen uno de los recursos más valiosos, obras como esta contribuyen significativamente a la formación de ciudadanos digitales conscientes, capaces de enfrentar los desafíos de la transformación tecnológica con responsabilidad, ética y compromiso con la seguridad de la información.

Tabla de contenido

Tabla de contenido

Tabla de contenido

Tabla de contenido

Introducción

La sociedad contemporánea experimenta una transformación acelerada impulsada por el desarrollo de las tecnologías digitales, la conectividad global y la expansión de plataformas informáticas en prácticamente todos los ámbitos de la vida humana. Este proceso ha modificado las dinámicas de comunicación, producción, aprendizaje y gestión de la información, generando nuevas oportunidades para el desarrollo social, económico y educativo. No obstante, también ha dado origen a desafíos complejos relacionados con la protección de datos, la privacidad y la seguridad de los sistemas digitales.

De modo que la ciberseguridad aplicada surge como un campo estratégico orientado a prevenir, detectar y mitigar riesgos asociados al uso de tecnologías de la información. La creciente sofisticación de las amenazas cibernéticas, el incremento de vulnerabilidades en aplicaciones y plataformas digitales, así como la dependencia de infraestructuras tecnológicas críticas, evidencian la necesidad de fortalecer mecanismos de protección capaces de garantizar la continuidad operativa y la integridad de la información.

La presente obra aborda la ciberseguridad desde una perspectiva integral, articulando fundamentos teóricos, enfoques metodológicos y estrategias prácticas orientadas a la protección de aplicaciones y a la gestión segura de la información digital. A partir de un enfoque interdisciplinario, se analizan los principales riesgos y desafíos que enfrentan las organizaciones e instituciones en el entorno digital contemporáneo, destacando la importancia de adoptar modelos de seguridad basados en estándares internacionales, buenas prácticas y procesos de formación continua.

Asimismo, el libro examina la relación existente entre ciberseguridad, computación y cultura digital, enfatizando que la protección de la información no depende exclusivamente de soluciones tecnológicas, sino también del fortalecimiento de competencias digitales, la concienciación de los usuarios y la construcción de entornos organizacionales resilientes.

La estructura de la obra ha sido diseñada de manera progresiva y sistemática. En los primeros capítulos se desarrollan los fundamentos conceptuales y teóricos relacionados con la ciberseguridad, la computación y la protección digital. Posteriormente, se presentan los aspectos metodológicos de la investigación y el análisis de los resultados obtenidos. Finalmente, se incluyen conclusiones,

recomendaciones y una propuesta orientada al fortalecimiento de la seguridad digital en plataformas tecnológicas y educativas.

En consecuencia, este libro pretende constituirse en una herramienta de referencia para investigadores, profesionales, docentes y estudiantes interesados en comprender los desafíos actuales de la seguridad informática y en promover estrategias orientadas a la protección de aplicaciones, la gestión segura de la información y el desarrollo de una cultura digital.

CAPÍTULO I

Introducción

ALUMNI EDITORA

La acelerada evolución de las tecnologías digitales transformó de manera significativa los procesos educativos en todos los niveles de formación, configurando nuevos escenarios de interacción, acceso al conocimiento y construcción del aprendizaje (García-Peñalvo et al., 2021; Marín & Cabero-Almenara, 2022). Este fenómeno se vio impulsado por la expansión de internet, el desarrollo de plataformas digitales y la incorporación de herramientas tecnológicas que permitieron superar las barreras tradicionales del tiempo y el espacio en la educación (Nguyen et al., 2022). En consecuencia, las plataformas de formación adoptaron modelos más dinámicos, flexibles y centrados en el estudiante, favoreciendo el aprendizaje autónomo y colaborativo (Bowen et al., 2022).

En este contexto de transformación, la digitalización de los procesos educativos implicó no solo beneficios evidentes en términos de accesibilidad y eficiencia, sino también la exposición a un conjunto creciente de riesgos asociados al uso intensivo de tecnologías de la información (Camacho & Fernández-Alemán, 2022; Mishra et al., 2023). La gestión de grandes volúmenes de datos, la interconectividad de sistemas y la dependencia de infraestructuras digitales generaron nuevas preocupaciones relacionadas con la protección de la información, la privacidad de los usuarios y la integridad de los sistemas (Dlamini et al., 2022).

A partir de esta realidad, la ciberseguridad emergió como un componente esencial para el funcionamiento adecuado de las plataformas digitales, adquiriendo una relevancia particular en el ámbito educativo (Bada & Nurse, 2023; Alzahrani & Alghamdi, 2022). La necesidad de proteger la información académica, los datos personales y los recursos institucionales demandó la incorporación de estrategias, políticas y prácticas orientadas a la prevención de riesgos y a la mitigación de amenazas en el ciberespacio (Sabillon et al., 2022; González-Granadillo et al., 2022).

Asimismo, la computación desempeñó un papel central en la configuración de estas plataformas, al proporcionar las bases tecnológicas sobre las cuales se desarrollan las plataformas educativas y los sistemas de gestión de la información (García-Peñalvo et al., 2021). La interacción entre ciberseguridad y computación permitió no solo fortalecer los mecanismos de protección, sino

también promover una comprensión más integral de los desafíos asociados a la transformación digital en la educación (Kamal et al., 2023).

Desde esta perspectiva, la formación en competencias digitales seguras se consolidó como una necesidad prioritaria, orientada a capacitar a los usuarios para identificar riesgos, adoptar prácticas responsables y participar de manera consciente en las plataformas digitales (Amankwa, 2021; Hu, 2024). Esta perspectiva integradora reconoce que la seguridad de la información no depende únicamente de soluciones tecnológicas, sino también del comportamiento humano y de la cultura organizacional (Kennison & Chan-Tin, 2020; Bongiovanni, 2022).

Desde esta perspectiva, la presente obra se situó en la intersección entre la ciberseguridad, la computación y los procesos de formación, abordando de manera integral los desafíos y oportunidades que surgen en las plataformas educativas contemporáneos (Hashim & Hassan, 2023; Achuthan et al., 2024). A partir de un enfoque analítico y aplicado, se buscó comprender cómo la integración de estos elementos contribuye a la protección de la información y al fortalecimiento de la calidad educativa en contextos digitales.

A pesar del crecimiento sostenido de investigaciones en el ámbito de la ciberseguridad aplicada a plataformas educativos, persiste una brecha significativa en la integración efectiva de marcos normativos internacionales, como NIST e ISO/IEC 27001, con modelos pedagógicos adaptados a contextos latinoamericanos. En particular, se evidencia una limitada articulación entre los enfoques técnicos de protección de la información y las estrategias formativas orientadas al desarrollo de competencias digitales seguras en los usuarios. Esta situación pone de manifiesto la necesidad de propuestas integradoras que no solo consideren la dimensión tecnológica, sino también los factores humanos, organizacionales y educativos que inciden en la seguridad de las aplicaciones y sistemas digitales.

1.1 Contextualización del problema

En los últimos años, el desarrollo de las tecnologías digitales ha generado transformaciones profundas en los procesos educativos en todos los niveles de formación (Nguyen et al., 2022), redefiniendo las formas de acceso, producción y difusión del conocimiento. La incorporación de plataformas virtuales,

herramientas colaborativas, dispositivos móviles y servicios en la nube amplió significativamente las oportunidades de aprendizaje (Camacho & Fernández-Alemán, 2022), permitiendo la creación de plataformas flexibles, interactivos y ubicuos. Sin embargo, este proceso de transformación también introdujo nuevos riesgos asociados a la seguridad de la información, la privacidad de los datos (Sharma & Dash, 2023) y la integridad de los sistemas digitales.

En las plataformas educativas contemporáneos, la creciente dependencia de infraestructuras tecnológicas evidenció vulnerabilidades que pueden comprometer tanto la información institucional como los datos personales (Abomhara & Køien, 2022) de estudiantes, docentes y administrativos. La exposición a amenazas como accesos no autorizados, pérdida de información, ataques informáticos y prácticas inadecuadas en el manejo de datos ha puesto de manifiesto la necesidad de integrar la ciberseguridad como un componente esencial (Jang-Jaccard & Nepal, 2022) dentro de los procesos de formación.

En este escenario, la relación entre ciberseguridad y computación adquiere una relevancia estratégica, ya que no solo implica la protección de los sistemas tecnológicos, sino también la formación de individuos capaces de desenvolverse de manera segura, crítica y responsable en el ciberespacio. La educación digital, por tanto, no puede limitarse al desarrollo de competencias técnicas, sino que debe incorporar una dimensión ética y preventiva orientada a la protección de la información.

1.2 Planteamiento del problema y pregunta de investigación

A pesar de la creciente integración de tecnologías digitales en los procesos educativos, se evidenció una brecha significativa en la adopción de prácticas seguras y en el nivel de conocimiento sobre ciberseguridad (Alzahrani & Alghamdi, 2022) dentro de las comunidades académicas. Esta situación generó escenarios de vulnerabilidad que afectan la confianza en las plataformas virtuales (Bada & Nurse, 2023) de aprendizaje y comprometen la protección de la información.

En muchos contextos educativos, la implementación de herramientas tecnológicas no ha estado acompañada de estrategias formativas orientadas a la seguridad digital (Ahmed et al., 2024), lo que ha limitado la capacidad de los usuarios para identificar riesgos, prevenir incidentes y actuar de manera

adecuada ante posibles amenazas. Esta problemática plantea la necesidad de analizar de forma integral la relación entre ciberseguridad, computación y formación digital.

En consecuencia, la investigación se orientó a responder la siguiente pregunta: ¿Cómo influye la integración de la ciberseguridad y la computación en la protección de la información digital dentro de los procesos de formación en plataformas educativas contemporáneos?

1.3 Propósito y objetivos de la investigación

La obra tuvo como propósito analizar la relación entre la ciberseguridad, la computación y la protección digital (Hashim & Hassan, 2023) en los procesos de formación, con el fin de contribuir al fortalecimiento de plataformas educativas seguros y resilientes.

En coherencia con este propósito, se planteó como objetivo general comprender de qué manera la incorporación de principios y prácticas de ciberseguridad influye en la protección de la información (Becerril-Arreola & Sosa-Sosa, 2023) y en el desarrollo de competencias digitales seguras en contextos educativos.

De forma específica, el estudio se orientó a examinar los fundamentos teóricos de la ciberseguridad y la computación en el ámbito educativo, identificar las principales amenazas y vulnerabilidades presentes en las plataformas de formación digital, analizar el nivel de conocimiento y las prácticas de seguridad de los usuarios en una comunidad académica, y proponer lineamientos orientados a fortalecer la protección de la información en dichos contextos.

1.4 Justificación e importancia del estudio

La relevancia de esta obra se sustenta en la necesidad creciente de garantizar la seguridad de la información en plataformas educativas (Sharma & Dash, 2023) altamente digitalizados. La protección de los datos no solo constituye un requisito técnico, sino también un principio fundamental para la confianza, la ética y la sostenibilidad de los procesos educativos.

El estudio aportó una visión integral que articula la dimensión tecnológica y formativa (Da Veiga & Martins, 2023), destacando la importancia de promover una cultura de ciberseguridad que trascienda el uso instrumental de las

tecnologías. Por consiguiente, la investigación adquiere pertinencia tanto a nivel académico como institucional, al ofrecer elementos que pueden ser utilizados para el diseño de políticas, estrategias y programas de formación en seguridad digital.

Asimismo, la obra contribuye al campo del conocimiento al integrar enfoques teóricos y prácticos que permiten comprender la ciberseguridad no solo como una disciplina técnica, sino como un componente transversal en la educación contemporánea.

1.5 Alcance y estructura de la obra

Se estructuró en capítulos que abordan fundamentos, metodología, resultados y conclusiones (González-Granadillo et al., 2022). En primer lugar, se presentan los fundamentos conceptuales relacionados con la ciberseguridad, la computación y la protección de la información en contextos educativos. Posteriormente, se describe el enfoque metodológico adoptado, así como las técnicas e instrumentos utilizados para la recolección y análisis de los datos.

En los capítulos siguientes, se exponen los resultados obtenidos, acompañados de un análisis crítico que permite interpretar los hallazgos a la luz del marco teórico. Finalmente, se presentan las conclusiones y recomendaciones derivadas del estudio, así como una propuesta orientada al fortalecimiento de la protección digital en los procesos de formación.

1.6 Aporte y proyección

La obra pretendió contribuir al desarrollo de competencias digitales seguras (Amankwa, 2021), fomentando el uso responsable de las tecnologías y promoviendo plataformas resilientes (Kour et al., 2024) frente a los desafíos de la plataforma digital. De este modo, se consolidó como un referente para la comprensión de la ciberseguridad aplicada en la educación, ofreciendo una base conceptual y práctica para futuras investigaciones y propuestas de intervención.

De esta manera, el estudio proyecta la necesidad de continuar fortaleciendo la integración de la ciberseguridad en los procesos formativos, reconociendo su papel como elemento clave en la protección de la información y en la formación de ciudadanos digitales conscientes y responsables.

CAPÍTULO II

Marco teórico

ALUMNI EDITORA

El desarrollo del marco teórico constituye un elemento fundamental en toda investigación científica, ya que permite sustentar conceptualmente el estudio a partir de la revisión, análisis e integración de conocimientos previos (Yadav & Rao, 2023) relacionados con el fenómeno investigado. En el contexto de la presente obra, este apartado adquiere especial relevancia debido a la naturaleza interdisciplinaria del tema, el cual articula la ciberseguridad, la computación y la protección de la información digital en los procesos de formación en plataformas educativos. Asimismo, iniciativas internacionales orientadas a la educación en ciberseguridad han reforzado la necesidad de consolidar marcos formativos sólidos en este ámbito (ENISA, 2022).

La transformación digital ha generado nuevos riesgos de seguridad (Mishra et al., 2023) y, paralelamente, la educación ha experimentado en las últimas décadas la incorporación masiva de tecnologías de la información y la comunicación, lo que ha dado lugar a nuevos escenarios de aprendizaje mediados por plataformas virtuales, sistemas de gestión educativa y herramientas colaborativas en línea. Este proceso, si bien ha ampliado las oportunidades de acceso al conocimiento, también ha introducido riesgos asociados a la seguridad de la información, la privacidad de los datos y la integridad de los sistemas digitales, especialmente en contextos de trabajo remoto y virtualización acelerada (Furnell & Shah, 2022; Lallie et al., 2023).

En consecuencia, el marco teórico se orienta al análisis de los principales enfoques, teorías y conceptos que permiten comprender la ciberseguridad como un componente esencial en la construcción de plataformas educativas seguros. Asimismo, se examinan los fundamentos de la computación como base tecnológica de los procesos digitales, junto con los principios relacionados con la protección de la información en contextos formativos.

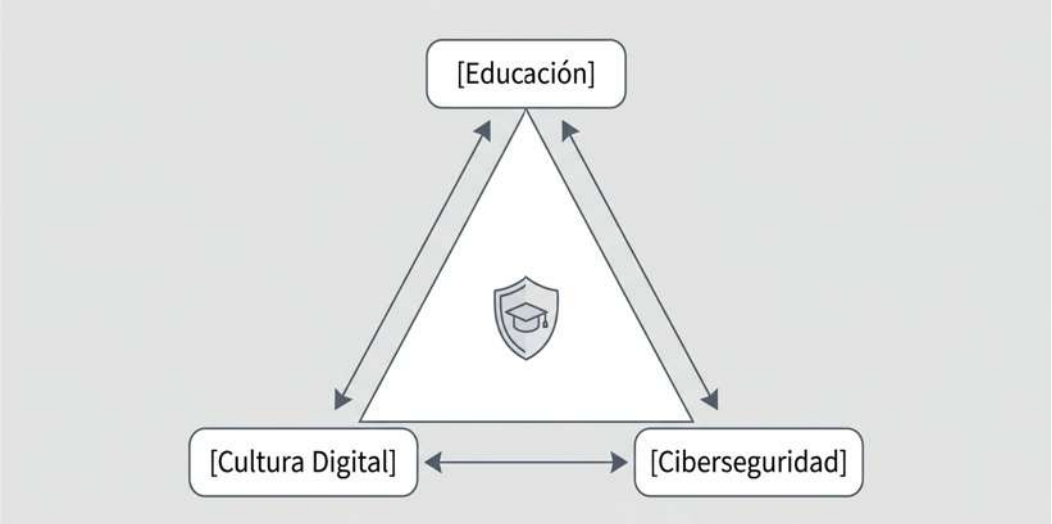
De igual manera, este capítulo integra aportes provenientes de estándares internacionales, modelos de gestión de la seguridad y enfoques contemporáneos que abordan la protección de activos digitales en plataformas organizacionales y educativos. La revisión de estos elementos permite contextualizar el problema de investigación y establecer un marco de referencia sólido que orienta el desarrollo del estudio y la interpretación de sus resultados.

A partir de esta base conceptual, se presentan los fundamentos teóricos de la ciberseguridad como punto de partida para comprender la importancia de la protección digital en los procesos de formación y su impacto en la construcción de una cultura de seguridad en la educación contemporánea.

Para comprender el alcance de la seguridad de la información en el ámbito escolar, es imperativo analizarla no como un elemento aislado, sino como el resultado de la convergencia de tres ejes fundamentales. La literatura especializada sugiere que la protección de datos y sistemas en la academia depende de un equilibrio dinámico entre la pedagogía, el comportamiento del usuario y las medidas técnicas de defensa.

En consecuencia, he propuesto una figura conceptual que ilustra la interdependencia entre la Educación, la Ciberseguridad y la Cultura Digital. Este esquema visualiza cómo la interacción entre estos tres vértices fundamenta una plataforma educativa resiliente, ver figura 1.

Figura 1. Relación entre educación, ciberseguridad y cultura digital



Como se observa en la figura 1, el modelo conceptual adopta la forma de un triángulo para representar que los tres ejes fundamentales —Educación, Ciberseguridad y Cultura Digital— poseen un peso equivalente y deben interactuar de forma equitativa.

El flujo de la relación opera en dos niveles. En el vértice superior, la Educación actúa como el catalizador principal. Sin un proceso pedagógico

estructurado, es imposible generar una alfabetización digital significativa en la comunidad educativa.

Por un lado, la intersección entre Educación y Cultura Digital fomenta la comprensión de los derechos y responsabilidades dentro de una plataforma interconectada, promoviendo un comportamiento ético y reflexivo al navegar. Por otro lado, la interacción entre Educación y Ciberseguridad proporciona las habilidades técnicas y operativas necesarias para identificar, prevenir y responder ante amenazas técnicas y sociales.

Finalmente, el modelo conceptual ilustra que, si bien la Ciberseguridad proporciona las herramientas técnicas y operativas de protección, estas solo alcanzan su máximo potencial cuando están profundamente integradas en una Cultura Digital robusta. La relación transversal entre ambos vértices garantiza que el uso de la tecnología sea, simultáneamente, seguro y ético.

En conjunto, el triángulo conceptual demuestra que la protección efectiva en plataformas académicos no es una responsabilidad puramente técnica, sino un desafío socio pedagógico integral. El equilibrio dinámico entre estos tres vértices constituye la base para una plataforma educativa resiliente y seguro.

2.1 Ciberseguridad: fundamentos conceptuales

La ciberseguridad se ha consolidado como un campo multidisciplinario (Abomhara & Køien, 2022) orientado a la protección de sistemas, redes digitales e información frente a amenazas internas y externas (Dlamini et al., 2022). Este campo abarca la prevención, detección y respuesta ante incidentes de seguridad (Jang-Jaccard & Nepal, 2022) y surge como respuesta a la creciente digitalización de los procesos organizacionales y sociales, lo que ha generado la necesidad de establecer mecanismos de defensa que garanticen la continuidad operativa y la protección de los activos informacionales.

Mientras Bada y Nurse (2023) enfatizan la concienciación del usuario como eje central para la mitigación de riesgos en ciberseguridad, Da Veiga y Martins (2023) destacan la importancia de consolidar una cultura organizacional de seguridad como elemento estructural para la protección de la información. En esta misma línea, Mishra et al. (2023) subrayan los desafíos específicos que enfrentan las plataformas de aprendizaje en línea, particularmente en relación con la protección de datos y la integridad de las plataformas digitales. Estas

perspectivas evidencian que la ciberseguridad no puede abordarse únicamente desde un enfoque técnico, sino que requiere una integración multidimensional que articule factores humanos, tecnológicos y organizacionales.

Asimismo, la evolución de las metodologías de evaluación de riesgos ha permitido fortalecer la gestión estratégica de la ciberseguridad mediante enfoques automatizados y estructurados (Angelini et al., 2022; Nour Eldin et al., 2026). En consecuencia, la ciberseguridad no se limita a la implementación de herramientas tecnológicas, sino que integra enfoques estratégicos, normativos y humanos que permiten abordar los riesgos de manera sistémica.

Desde una perspectiva conceptual, la ciberseguridad abarca la identificación, prevención, detección y respuesta ante incidentes que puedan comprometer la confidencialidad, integridad y disponibilidad de la información. Este enfoque integral implica la adopción de políticas de seguridad, la gestión de riesgos, el cumplimiento de estándares internacionales y la formación de los usuarios como actores clave en la protección de los sistemas.

En el contexto de la protección de aplicaciones, la ciberseguridad adquiere un papel fundamental al garantizar que el software desarrollado e implementado cumpla con criterios de seguridad desde su diseño. La incorporación de prácticas como el desarrollo seguro, la validación de entradas, el control de accesos y la gestión de vulnerabilidades permite reducir la exposición a ataques y fortalecer la resiliencia de los sistemas.

En el ámbito educativo, la ciberseguridad trasciende el componente técnico para convertirse en un elemento formativo esencial. La interacción constante de estudiantes y docentes con plataformas digitales evidencia la necesidad de desarrollar competencias orientadas al uso seguro de la tecnología. De este modo, la ciberseguridad se posiciona como un pilar en la construcción de plataformas digitales confiables, donde la protección de la información y la continuidad de los procesos formativos constituyen prioridades estratégicas.

Asimismo, la gestión de riesgos se integra de manera transversal como un proceso fundamental para identificar, analizar y mitigar amenazas potenciales, permitiendo una toma de decisiones informada en la protección de los sistemas y la información digital.

2.2 Computación y plataformas digitales de aprendizaje

La computación, entendida como el conjunto de procesos y tecnologías que permiten el tratamiento automatizado de la información, desempeña un papel central en la transformación de los sistemas educativos contemporáneos. Esta posibilita el desarrollo de plataformas digitales interactivas (García-Peñalvo et al., 2021), aunque también introduce riesgos asociados a la seguridad (Camacho & Fernández-Alemán, 2022).

Estas plataformas han evolucionado mediante la incorporación de modelos de seguridad cada vez más complejos, incluyendo la integración de estándares como NIST e ISO en infraestructuras digitales modernas (Febrilian Tanjung et al., 2024), lo que evidencia la necesidad de alinear la computación con prácticas robustas de ciberseguridad. Esta evolución ha facilitado la creación de plataformas digitales de aprendizaje caracterizados por la interactividad, la accesibilidad y la adaptación a diversas necesidades formativas.

Sustentados en plataformas virtuales, sistemas de gestión del aprendizaje y servicios en la nube, estas plataformas permiten integrar recursos multimedia, herramientas de comunicación y mecanismos de evaluación en línea, configurando espacios educativos dinámicos que favorecen la construcción colaborativa del conocimiento y la personalización del aprendizaje.

No obstante, la creciente dependencia de la computación también introduce desafíos relacionados con la seguridad de las aplicaciones y la protección de la información digital. La interconexión de sistemas, la transmisión constante de datos y el almacenamiento en infraestructuras distribuidas incrementan la exposición a amenazas, lo que hace imprescindible la incorporación de medidas de ciberseguridad en todos los niveles de la arquitectura tecnológica.

En este contexto, la relación entre computación y ciberseguridad se vuelve inseparable, ya que el funcionamiento adecuado de las plataformas digitales depende tanto de la eficiencia tecnológica como de la capacidad de garantizar la protección de la información. Esta integración permite optimizar los procesos educativos y fortalecer la confianza de los usuarios en el uso de plataformas digitales.

2.3 Tríada de la seguridad de la información

La seguridad de la información se fundamenta en la tríada compuesta por confidencialidad, integridad y disponibilidad (ISO/IEC, 2022a; National Institute of Standards and Technology, 2020), que constituye el eje conceptual para el diseño de sistemas seguros. Estos principios orientan la implementación de controles y mecanismos destinados a proteger los activos informacionales frente a diversas amenazas, y su aplicación se ve reforzada por modelos de evaluación de madurez que facilitan su medición y mejora continua (Sulistyowati et al., 2020).

La confidencialidad se enfoca en restringir el acceso a la información únicamente a usuarios autorizados mediante mecanismos como la autenticación, la encriptación y el control de privilegios, lo cual resulta esencial en plataformas educativas donde se gestionan datos personales y académicos sensibles.

La integridad garantiza que la información se mantenga completa, exacta y libre de alteraciones no autorizadas, asegurando la fiabilidad de contenidos, evaluaciones y registros académicos en los sistemas educativos.

Por su parte, la disponibilidad asegura que los sistemas y la información estén accesibles cuando se requieran, lo que adquiere especial relevancia en plataformas digitales de aprendizaje, donde la interrupción de los servicios puede afectar significativamente la continuidad educativa.

El equilibrio entre estos tres principios constituye la base para la gestión segura de la información digital, permitiendo el diseño de estrategias de protección integrales.

2.4 Seguridad en las plataformas educativas digitales

La seguridad en las plataformas educativas digitales implica la implementación de un conjunto articulado de medidas orientadas a proteger tanto a los usuarios como a la información que circula en las plataformas académicas. Este enfoque integral abarca dimensiones tecnológicas, organizacionales y humanas que permiten abordar la seguridad desde una perspectiva holística.

Las amenazas en estas plataformas incluyen malware, phishing y accesos no autorizados (Kumar & Somani, 2022), las cuales se manifiestan a través de software malicioso, suplantación de identidad, vulnerabilidades en aplicaciones

y otros vectores de ataque. Estas situaciones evidencian la necesidad de establecer políticas institucionales claras que regulen el uso de los recursos tecnológicos y definan procedimientos para la gestión de incidentes.

Estas problemáticas también se presentan en diversos sectores que dependen de sistemas digitales, lo que demuestra la transversalidad de la ciberseguridad en distintos contextos (Mantha & García, 2021).

La protección de aplicaciones educativas constituye un elemento crítico, ya que estas representan el principal medio de interacción entre los usuarios y los sistemas. La implementación de controles de seguridad, auditorías periódicas y actualizaciones constantes permite reducir vulnerabilidades y fortalecer la confianza en las plataformas digitales.

Asimismo, la formación continua de la comunidad educativa se posiciona como un factor determinante en la prevención de incidentes. La concienciación sobre buenas prácticas, el reconocimiento de amenazas y el uso responsable de la tecnología contribuyen a la construcción de plataformas más seguros. Desde esta perspectiva, la realización de auditorías de seguridad permitió evaluar periódicamente el estado de los sistemas, identificar vulnerabilidades y verificar el cumplimiento de las políticas establecidas, fortaleciendo la capacidad de respuesta ante incidentes.

2.5 Ingeniería social y riesgos digitales

La ingeniería social se configura como una de las principales amenazas en el ámbito de la ciberseguridad, al basarse en la manipulación psicológica del comportamiento humano para obtener acceso a información sensible o sistemas protegidos (Kumar & Somani, 2022). A diferencia de los ataques técnicos, este enfoque explota factores como la confianza, la urgencia y la curiosidad.

En este contexto, la comunicación en ciberseguridad desempeña un papel clave en la percepción del riesgo y en la respuesta de los usuarios ante amenazas (Murad & Khan, 2025), especialmente en plataformas educativas donde la interacción digital es constante.

En estas plataformas, la ingeniería social se manifiesta mediante correos electrónicos fraudulentos, mensajes engañosos y sitios web falsificados que simulan plataformas institucionales con el fin de inducir a los usuarios a revelar credenciales o ejecutar acciones que comprometan la seguridad.

La mitigación de estos riesgos requiere el fortalecimiento de las competencias digitales y la implementación de estrategias de concienciación que permitan identificar patrones de ataque, consolidando la educación en ciberseguridad como una herramienta clave para reducir la efectividad de estas técnicas.

2.6 Cultura digital y ética en la ciberseguridad

La cultura digital representa el conjunto de valores, conocimientos y prácticas que orientan el uso de la tecnología en la sociedad contemporánea, promoviendo un uso responsable de la misma (Bongiovanni, 2022). Este enfoque se ve fortalecido por iniciativas internacionales que impulsan la educación en ciberseguridad y la formación de ciudadanos digitales responsables (ENISA, 2022).

En el ámbito educativo, su desarrollo implica la formación de individuos capaces de interactuar de manera crítica y responsable en plataformas digitales.

La ética en la ciberseguridad se vincula estrechamente con esta cultura, promoviendo el respeto por la privacidad, la protección de los datos y el uso adecuado de los recursos tecnológicos. La adopción de principios éticos permite prevenir conductas que comprometan la seguridad de la información y fortalece la confianza en los sistemas digitales.

Las instituciones educativas desempeñan un papel clave en la construcción de esta cultura mediante la integración de contenidos de ciberseguridad en los programas de formación y la promoción de prácticas orientadas a la protección de la información. Este enfoque contribuyó a la formación de ciudadanos digitales conscientes, capaces de enfrentar los desafíos de la plataforma tecnológica.

2.7 Protección digital en los procesos de formación en plataformas de formación digital

La protección digital en los procesos de formación se concibe como un enfoque integral que articula dimensiones técnicas, pedagógicas y éticas (Sharma & Dash, 2023) para garantizar la seguridad de la información en plataformas educativos. Este enfoque se refuerza con la adopción de marcos integrados de

seguridad y estándares internacionales en sistemas complejos (Febrilian Tanjung et al., 2024).

Desde la dimensión técnica, se requiere la implementación de sistemas seguros, actualizados y capaces de responder a incidentes. En el ámbito pedagógico, se promueve la incorporación de contenidos de ciberseguridad en los procesos formativos. En el plano ético, se enfatiza el respeto por los derechos digitales y la responsabilidad en el uso de la tecnología.

Este enfoque permite consolidar plataformas de aprendizaje protegidos, donde la tecnología se utiliza de manera segura y eficiente, contribuyendo al desarrollo de competencias necesarias para la participación en la sociedad digital.

Asimismo, el cumplimiento de normativas y estándares de seguridad se constituye como un elemento clave para garantizar la protección de la información y fortalecer la confianza en las plataformas digitales de formación.

2.8 Relación entre ciberseguridad, computación y educación

La relación entre ciberseguridad, computación y educación se configura como un eje fundamental en la transformación de los procesos formativos, al establecer una interacción clave para el desarrollo de plataformas seguros (Achuthan et al., 2024). Además, el avance de tecnologías emergentes y su integración en la ciberseguridad requiere nuevas estrategias educativas y de gestión del conocimiento (Murad & Khan, 2025).

La computación proporciona las herramientas tecnológicas necesarias para el desarrollo de plataformas digitales, mientras que la ciberseguridad garantiza la protección de estos sistemas. La educación, por su parte, actúa como el espacio en el que se desarrollan las competencias necesarias para el uso seguro de la tecnología.

Esta interacción permite integrar el conocimiento técnico con la formación ética y preventiva, fortaleciendo la capacidad de los usuarios para enfrentar los desafíos de la plataforma digital.

El fortalecimiento de esta relación contribuyó a la construcción de plataformas educativas seguros, inclusivos y sostenibles, en los cuales la tecnología se consolidó como un medio para el aprendizaje y el desarrollo social. De esta manera, la ciberseguridad aplicada se posicionó como un elemento

estratégico para la protección de aplicaciones y la gestión segura de la información digital en los procesos de formación contemporáneos.

2.9 Normativas, estándares y marcos de referencia en ciberseguridad

La ciberseguridad aplicada, particularmente en la protección de aplicaciones y la gestión de la información digital, se sustenta en normativas, estándares y marcos de referencia internacionales que orientan la implementación de buenas prácticas y garantizan un enfoque sistemático en la gestión de la seguridad. Estos instrumentos proporcionaron lineamientos estructurados que permiten a las organizaciones identificar riesgos, establecer controles adecuados y evaluar continuamente la eficacia de sus estrategias de protección.

Entre los principales referentes se encuentran ISO 27001 (ISO/IEC, 2022a), NIST (2018a, 2018b) y OWASP (2021, 2023), fundamentales para la gestión de riesgos (Alshar'e, 2023; Rahman et al., 2024). Asimismo, la evolución de marcos de evaluación, automatización de riesgos y análisis avanzado ha optimizado la gestión de la seguridad en plataformas digitales complejos (Angelini et al., 2022; Nour Eldin et al., 2026). De igual manera, investigaciones recientes han resaltado la importancia de integrar modelos de madurez y evaluación continua en ciberseguridad (Sulistyowati et al., 2020), así como la adopción de estándares internacionales en sistemas modernos (Febrilian Tanjung et al., 2024).

La familia de normas ISO/IEC 27000 se ha consolidado como uno de los referentes más relevantes en materia de gestión de la seguridad de la información. En particular, la norma ISO/IEC 27001 estableció los requisitos para la implementación de un sistema de gestión de seguridad de la información, basado en un enfoque de mejora continua y en la identificación, análisis y tratamiento de riesgos. Este estándar permitió a las organizaciones estructurar políticas, procedimientos y controles orientados a proteger la confidencialidad, integridad y disponibilidad de la información, alineándose con los objetivos estratégicos institucionales.

De manera complementaria, diversos estudios destacan la importancia de integrar marcos de evaluación de madurez y gestión de riesgos en la ciberseguridad educativa, destacando la utilidad de modelos como NIST CSF, CIS

Control y evaluaciones automatizadas de riesgos (Irawan et al., 2024; Lokare et al., 2025; Angelini et al., 2022). Asimismo, investigaciones emergentes subrayan el impacto de la inteligencia artificial en la ciberseguridad, tanto como herramienta de defensa como nuevo vector de riesgo (Vulpe & Smith, 2024; Li et al., 2025). Por consiguiente, la inversión en ciberseguridad y la gestión de la reputación digital se consolidan como factores estratégicos en organizaciones educativas modernas (Rattanapong & Brown, 2025; Wojak et al., 2025), lo que evidencia la necesidad de continuar fortaleciendo la investigación y la innovación en este campo.

Asimismo, el marco de ciberseguridad del Instituto Nacional de Estándares y Tecnología proporcionó una guía flexible para la gestión de riesgos, organizada en funciones clave como identificar, proteger, detectar, responder y recuperar. Este enfoque facilitó la adopción de prácticas de seguridad adaptadas a distintos contextos organizacionales, incluyendo plataformas educativas, donde la protección de la información y la continuidad de los servicios resultan esenciales.

En el ámbito específico de la protección de aplicaciones, el proyecto abierto de seguridad de aplicaciones web se posicionó como un referente fundamental. Sus lineamientos permitieron identificar las vulnerabilidades más comunes en aplicaciones, tales como fallos de autenticación, inyecciones de código y exposición de datos sensibles, promoviendo el desarrollo de software seguro desde las etapas iniciales del ciclo de vida.

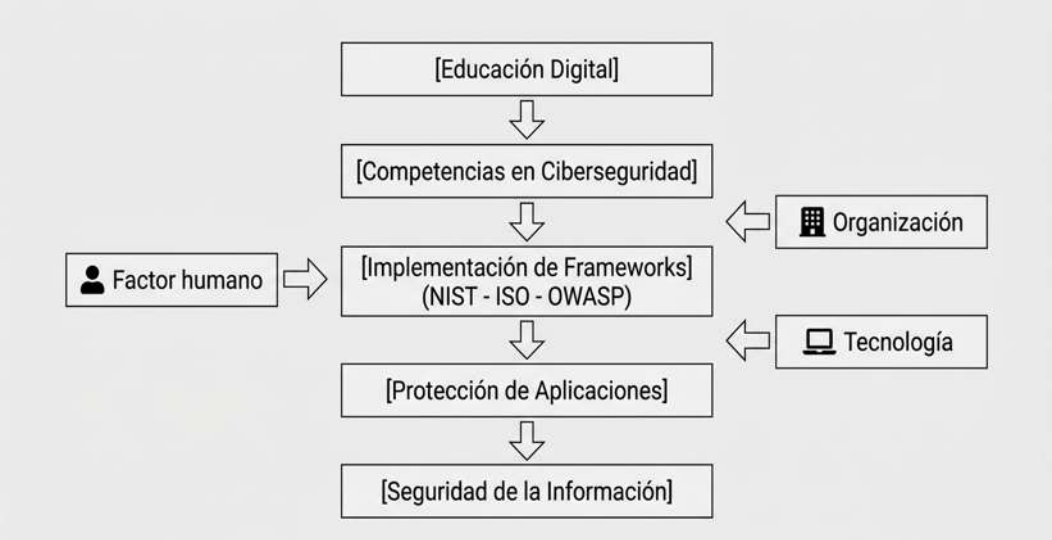
La integración de estos marcos de referencia contribuyó a fortalecer la ciberseguridad aplicada, al proporcionar una base sólida para la toma de decisiones, la implementación de controles efectivos y la construcción de plataformas digitales seguros. En el contexto educativo, su adopción permitió no solo proteger los sistemas y la información, sino también fomentar una cultura institucional orientada a la seguridad, la prevención y la gestión responsable de los riesgos digitales.

2.10 Elementos visuales y diagramas de modelo

Tras analizar la literatura, queda claro que la ciberseguridad educativa no puede abordarse con parches técnicos aislados. Se requiere una visión de conjunto que una la formación de las personas con las normativas técnicas. Para

resolver esta desconexión, he diseñado el modelo integral que se presenta a continuación. Este esquema visualiza cómo interactúan la pedagogía, los marcos de trabajo internacionales y la protección de datos para crear un plataforma escolar seguro, véase figura 2.

Figura 2. Modelo integrador de ciberseguridad para plataformas educativos



Como muestra la figura 2, el modelo propone una ruta lógica y descendente. La base de todo es la Educación Digital. Sin una buena alfabetización digital, es imposible construir Competencias en Ciberseguridad reales en la comunidad educativa. Una vez que las personas están preparadas, la institución puede avanzar hacia la parte técnica: la Implementación de Frameworks reconocidos como NIST, ISO y OWASP.

La aplicación de estos estándares internacionales decanta directamente en la Protección de Aplicaciones críticas (como los portales de notas o plataformas de aprendizaje), lo que finalmente nos lleva a la meta final: garantizar la Seguridad de la Información sensible de toda la institución.

Este flujo central no funciona solo; está sostenido por tres pilares transversales que interactúan en cada etapa. Primero, el Factor Humano, que es el motor del cambio cultural. Segundo, la Organización, que aporta el liderazgo, las políticas y los recursos necesarios. Y tercero, la Tecnología, que provee las herramientas técnicas para materializar la defensa. En conjunto, el modelo ofrece una guía clara para pasar de una postura reactiva a una proactiva en la seguridad escolar.

En el ámbito de la ciberseguridad, la implementación de marcos de referencia constituye un elemento fundamental para la gestión efectiva de riesgos y la protección de la información en plataformas digitales. Diversas organizaciones internacionales han desarrollado frameworks que permiten estructurar estrategias de seguridad adaptadas a diferentes contextos, particularmente en el ámbito educativo. De este modo, resulta pertinente analizar comparativamente los principales marcos utilizados, con el fin de identificar sus enfoques, ventajas y limitaciones, y así determinar su aplicabilidad en la protección de aplicaciones y sistemas en plataformas académicos, véase tabla 1.

Tabla 1. Comparación de frameworks de ciberseguridad

Framework	Enfoque principal	Ventajas principales	Limitaciones
NIST CSF	Gestión de riesgos en ciberseguridad	Flexible, adaptable a diferentes contextos	Complejidad en implementación
ISO/IEC 27001	Sistema de gestión de seguridad (SGSI)	Estandarización internacional, certificable	Costos elevados y procesos formales
OWASP	Seguridad en aplicaciones web	Enfoque práctico y técnico	Alcance limitado a aplicaciones web

Como se observa en la tabla 1, cada framework presenta características particulares que responden a distintos enfoques de la ciberseguridad. El NIST CSF destaca por su flexibilidad y capacidad de adaptación a diversos contextos organizacionales, lo que lo convierte en una herramienta ampliamente utilizada en la gestión de riesgos. Por su parte, la norma ISO/IEC 27001 ofrece un enfoque estructurado y certificable, orientado a la implementación de sistemas de gestión de seguridad de la información, aunque implica mayores costos y niveles de formalización. En contraste, OWASP se centra específicamente en la seguridad de aplicaciones web, proporcionando lineamientos prácticos para la

identificación y mitigación de vulnerabilidades, aunque con un alcance más limitado. En conjunto, estos marcos evidencian la necesidad de un enfoque integrador que permita aprovechar sus fortalezas para fortalecer la ciberseguridad en plataformas educativos.

2.11 Síntesis del estado del arte

El análisis del estado del arte permite identificar coincidencias, diferencias y vacíos en la literatura especializada en ciberseguridad aplicada a plataformas educativos. En cuanto a las coincidencias, diversos autores destacan la importancia de la formación en competencias digitales seguras, así como la implementación de marcos normativos internacionales para la gestión de riesgos. Por otro lado, las diferencias se centran en el enfoque de aplicación, donde algunos estudios priorizan los aspectos técnicos, mientras que otros enfatizan los factores humanos y organizacionales.

En relación con los vacíos identificados, se evidencia una limitada integración entre los marcos de ciberseguridad y los modelos pedagógicos en contextos educativos, especialmente en regiones en desarrollo. Asimismo, existe una carencia de propuestas metodológicas que articulen de manera sistemática la protección de aplicaciones con procesos de enseñanza-aprendizaje. Estos vacíos justifican la necesidad del presente estudio, orientado a proponer un enfoque integrador que contribuya al fortalecimiento de la ciberseguridad en plataformas educativas digitales.

CAPÍTULO III

Metodología

ALUMNI EDITORA

El presente capítulo describe de manera detallada el diseño metodológico que orienta el desarrollo de la investigación, estableciendo los procedimientos, enfoques y técnicas que permiten abordar de forma sistemática el estudio de la ciberseguridad y la computación aplicadas a la protección de la información digital en los procesos de formación. La metodología constituye el eje operativo de la investigación, ya que define la forma en que se recolecta, procesa y analiza la información necesaria para dar respuesta a la problemática planteada.

En coherencia con los fundamentos teóricos expuestos en el capítulo anterior, el diseño metodológico se estructura a partir de una lógica científica que busca garantizar la validez, confiabilidad y rigor de los resultados obtenidos. En consecuencia, se integran enfoques y procedimientos que permiten analizar la realidad educativa desde una perspectiva empírica, considerando las características propias de las plataformas digitales y las dinámicas de interacción tecnológica que en ellos se desarrollan.

La selección de un enfoque adecuado responde a la necesidad de comprender el fenómeno estudiado desde una dimensión objetiva y medible, permitiendo identificar patrones, tendencias y relaciones entre las variables asociadas a la seguridad de la información y el uso de tecnologías en contextos educativos. Asimismo, la definición del tipo y diseño de investigación, la delimitación de la población y muestra, así como la elección de técnicas e instrumentos de recolección de datos, se fundamentan en criterios metodológicos que aseguran la coherencia interna del estudio.

De esta manera, el capítulo metodológico no solo describe las decisiones técnicas adoptadas, sino que también justifica su pertinencia en función de los objetivos de la investigación y del contexto en el que se desarrolla. A partir de esta estructura, se presenta a continuación el enfoque de la investigación, el cual orienta el proceso de análisis y constituye la base para la obtención de resultados válidos y significativos.

3.1 Enfoque de la investigación

La presente investigación se desarrolló bajo un enfoque cuantitativo, orientado a la recolección, medición y análisis de datos numéricos que permitieran describir, interpretar y explicar las percepciones, conocimientos y

prácticas relacionadas con la ciberseguridad y la computación aplicadas a la protección de la información digital en los procesos de formación en plataformas digitales. Este enfoque respondió a la necesidad de obtener resultados objetivos, verificables y comparables, sustentados en evidencia empírica que permitiera identificar patrones de comportamiento y niveles de apropiación de prácticas seguras dentro del contexto educativo.

El carácter cuantitativo del estudio facilitó la operacionalización de las variables en indicadores medibles, permitiendo evaluar de manera precisa aspectos como el nivel de conocimiento en ciberseguridad, la frecuencia de uso de herramientas tecnológicas y la adopción de medidas de protección de la información. Asimismo, este enfoque posibilitó la aplicación de técnicas estadísticas que contribuyeron a la validación de los resultados y a la generación de inferencias sustentadas en datos.

De manera complementaria, el enfoque asumió un alcance descriptivo, orientado a caracterizar el fenómeno estudiado en su contexto natural, sin intervenir en su desarrollo. Esta perspectiva permitió comprender la realidad educativa en términos de prácticas digitales seguras, identificando fortalezas, debilidades y áreas de mejora en la formación de competencias relacionadas con la seguridad de la información. La integración de estos elementos favoreció una aproximación sistemática y estructurada al problema de investigación, alineada con los objetivos planteados en la obra.

3.2 Justificación

El enfoque metodológico adoptado en este estudio se justifica por la necesidad de analizar de manera sistemática la relación entre variables asociadas a la ciberseguridad y su impacto en la protección de aplicaciones en plataformas educativos. La elección de un enfoque cuantitativo permite obtener datos medibles y comparables, facilitando la identificación de patrones y tendencias relevantes para la toma de decisiones en materia de seguridad digital.

3.3 Limitaciones

Una de las principales limitaciones del estudio radica en la delimitación del contexto de análisis, lo que puede restringir la generalización de los resultados a otras plataformas con características diferentes. Asimismo, la disponibilidad y

calidad de los datos recolectados pueden influir en la precisión de los hallazgos. No obstante, se han implementado procedimientos metodológicos rigurosos para garantizar la validez y confiabilidad de los resultados obtenidos.

3.4 Tipo y diseño de investigación

El estudio se enmarcó en una investigación de tipo descriptiva y correlacional, en la medida en que no solo se orientó a la caracterización de las variables relacionadas con la ciberseguridad y la protección de la información digital en los procesos de formación, sino también al análisis de las relaciones existentes entre dichas variables. La dimensión descriptiva permitió identificar el estado actual del conocimiento, las prácticas y las percepciones de los participantes respecto al uso seguro de las tecnologías digitales, mientras que la dimensión correlacional facilitó el análisis de asociaciones entre factores como el nivel de formación tecnológica y la implementación de medidas de seguridad.

El diseño adoptado fue no experimental, dado que las variables no fueron manipuladas deliberadamente, sino observadas tal como se presentan en la realidad. Este enfoque resultó pertinente para el estudio de fenómenos educativos en plataformas digitales, donde las dinámicas de interacción tecnológica y los comportamientos de los usuarios deben analizarse en su contexto natural para garantizar la validez ecológica de los resultados.

Asimismo, este capítulo se analiza bajo un diseño transversal, ya que la recolección de datos se realizó en un único momento temporal. Este tipo de diseño permitió obtener una fotografía representativa del estado de la ciberseguridad en la plataforma educativa analizado, facilitando la identificación de tendencias y patrones en las prácticas digitales. Aunque este diseño limita el establecimiento de relaciones causales, resulta adecuado para estudios exploratorios y diagnósticos que buscan comprender una realidad específica en un momento determinado.

3.5 Población y muestra

La población objeto de estudio estuvo conformada por estudiantes y docentes pertenecientes a una institución de educación superior, quienes participan activamente en procesos de enseñanza y aprendizaje mediados por tecnologías digitales. Esta población fue seleccionada debido a su constante

interacción con plataformas virtuales, sistemas de gestión del aprendizaje, herramientas colaborativas y recursos en línea, lo que la convierte en un grupo relevante para el análisis de prácticas de ciberseguridad en plataformas educativos.

La muestra fue seleccionada mediante un muestreo no probabilístico de tipo intencional, considerando criterios de inclusión relacionados con la experiencia en el uso de tecnologías digitales, la participación en plataformas virtuales de aprendizaje y la disposición para colaborar con el estudio. Este tipo de muestreo permitió focalizar la investigación en sujetos que poseen características pertinentes para el análisis del fenómeno, garantizando la relevancia de la información recolectada.

Desde una perspectiva metodológica, la selección de la muestra respondió a la necesidad de profundizar en un contexto específico, más que de generalizar los resultados a una población amplia. No obstante, se procuró que la muestra fuera lo suficientemente representativa en términos de diversidad de perfiles académicos, niveles de formación y experiencias tecnológicas, con el fin de enriquecer el análisis y fortalecer la validez de los hallazgos.

Durante todo el proceso se garantizó la participación voluntaria, anónima y confidencial de los sujetos, respetando los principios éticos de la investigación científica y promoviendo un ambiente de confianza que favoreciera la veracidad de las respuestas.

3.6 Técnicas e instrumentos de recolección de datos

La técnica principal de recolección de datos fue la encuesta, seleccionada por su capacidad para obtener información estructurada de un número considerable de participantes en un periodo relativamente corto. Esta técnica resultó especialmente adecuada para el enfoque cuantitativo del estudio, ya que permitió la estandarización de las respuestas y su posterior tratamiento estadístico.

El instrumento utilizado fue un cuestionario estructurado, diseñado a partir de las variables y dimensiones definidas en el marco teórico. Este cuestionario estuvo compuesto por preguntas cerradas y de opción múltiple, orientadas a medir aspectos como el conocimiento en ciberseguridad, el uso de herramientas tecnológicas y las prácticas de protección de la información en

plataformas digitales. La formulación de los ítems se realizó con un lenguaje claro, preciso y accesible, evitando ambigüedades que pudieran afectar la calidad de las respuestas.

El proceso de validación del instrumento incluyó la revisión por expertos en el área de tecnología educativa y ciberseguridad, quienes evaluaron la pertinencia, coherencia y relevancia de cada ítem en relación con los objetivos del estudio. Adicionalmente, se consideró la consistencia interna del cuestionario como un criterio fundamental para garantizar su fiabilidad, lo cual permitió asegurar que los resultados obtenidos reflejaran de manera adecuada las variables analizadas.

3.7 Procedimiento

El desarrollo de la investigación siguió un procedimiento organizado en fases interrelacionadas que garantizaron la coherencia y rigurosidad del proceso metodológico. En una primera fase, se llevó a cabo una revisión bibliográfica exhaustiva que permitió fundamentar teóricamente el estudio, integrando aportes de la ciberseguridad, la computación y la educación digital.

Posteriormente, se diseñó el instrumento de recolección de datos, el cual fue sometido a un proceso de validación para asegurar su calidad metodológica. Una vez validado, el cuestionario fue aplicado a la muestra seleccionada mediante plataformas digitales, facilitando la participación de los sujetos en un plataforma accesible y acorde con la naturaleza del estudio.

Durante la aplicación del instrumento, se proporcionó a los participantes información clara sobre los objetivos de la investigación, garantizando su consentimiento informado y el respeto a su privacidad. Esta etapa fue clave para asegurar la transparencia del proceso y la ética en la recolección de datos.

Una vez obtenida la información, se procedió a su organización, codificación y procesamiento mediante herramientas informáticas especializadas en análisis estadístico. Este proceso permitió transformar los datos en información significativa, facilitando su interpretación y su posterior integración en el análisis de resultados.

3.8 Variables de estudio

Las variables consideradas en la investigación fueron definidas a partir del problema de estudio y del marco teórico, permitiendo estructurar el análisis del fenómeno desde una perspectiva integral. La ciberseguridad fue abordada como un conjunto de conocimientos, actitudes y prácticas orientadas a la protección de los sistemas y la información digital frente a amenazas y riesgos en plataformas tecnológicos.

La computación, por su parte, se entendió como el uso de herramientas tecnológicas en los procesos educativos, incluyendo plataformas virtuales, aplicaciones digitales y recursos en línea que facilitan la enseñanza y el aprendizaje. Esta variable permitió analizar el nivel de integración tecnológica en las plataformas de formación.

Finalmente, la protección de la información digital en los procesos de formación se conceptualizó como la percepción y aplicación de medidas de seguridad por parte de los usuarios, orientadas a garantizar la confidencialidad, integridad y disponibilidad de la información. La interacción entre estas variables permitió explorar la relación entre el uso de la tecnología y la adopción de prácticas seguras, evidenciando la importancia de la formación en ciberseguridad en contextos educativos.

3.9 Consideraciones éticas

La investigación se desarrolló en conformidad con los principios éticos que rigen la producción científica, garantizando el respeto a la dignidad, privacidad y autonomía de los participantes. Se obtuvo el consentimiento informado de cada uno de ellos, asegurando que su participación fuera voluntaria y basada en el conocimiento previo de los objetivos y alcances del estudio.

Se protegió la confidencialidad de la información mediante el anonimato de los datos recolectados, evitando cualquier tipo de identificación personal. Asimismo, se garantizó que la información obtenida sería utilizada exclusivamente con fines académicos y científicos, sin ningún tipo de uso indebido.

El manejo responsable de los datos y el respeto a los derechos de los participantes constituyeron pilares fundamentales en el desarrollo de la investigación, fortaleciendo su validez ética y su credibilidad científica.

3.10 Limitaciones del estudio

A pesar del rigor metodológico aplicado, el estudio presenta ciertas limitaciones que deben ser consideradas en la interpretación de los resultados. Entre ellas se encuentra el tamaño de la muestra y el uso de un muestreo no probabilístico, lo cual limita la generalización de los hallazgos a otros contextos educativos.

Asimismo, el diseño transversal impide establecer relaciones causales entre las variables, restringiendo el análisis a asociaciones observadas en un momento específico. De igual manera, el uso exclusivo de la encuesta como técnica de recolección de datos puede limitar la profundidad del análisis, al no incorporar perspectivas cualitativas que permitan una comprensión más amplia del fenómeno.

No obstante, estas limitaciones no invalidan los resultados obtenidos, sino que delimitan su alcance, ofreciendo una base sólida para futuras investigaciones que profundicen en la temática mediante enfoques complementarios.

3.11 Análisis de datos

El análisis de los datos se realizó mediante técnicas estadísticas descriptivas que permitieron organizar, sintetizar e interpretar la información recolectada. Se utilizaron frecuencias absolutas y relativas, así como porcentajes, para identificar patrones de respuesta y tendencias en las percepciones y prácticas de los participantes.

El procesamiento de los datos se llevó a cabo mediante herramientas informáticas especializadas, lo que permitió garantizar la precisión en los cálculos y la confiabilidad de los resultados. La representación de la información en tablas y gráficos facilitó la visualización de los datos, contribuyendo a una interpretación clara y coherente de los hallazgos.

Este análisis constituyó la base para la discusión de los resultados, permitiendo establecer relaciones entre las variables estudiadas y generar conclusiones fundamentadas en evidencia empírica, en coherencia con los objetivos de la investigación y el enfoque general de la obra.

3.12 Fortalecimiento del diseño metodológico

Con el propósito de fortalecer el rigor científico del estudio, se presentan a continuación algunas consideraciones metodológicas relevantes.

La estructura metodológica del estudio se presenta de manera adecuada y coherente con los objetivos planteados. No obstante, se identifican aspectos susceptibles de mejora que fortalecerían el rigor científico de la investigación.

En primer lugar, se requiere mayor precisión en la descripción del tamaño de la muestra, ya que en algunos apartados esta información no se presenta de forma explícita o consistente. La delimitación clara del número de participantes es fundamental para garantizar la validez de los resultados.

En segundo lugar, se recomienda incorporar procedimientos de validación estadística que respalden la fiabilidad de los instrumentos utilizados, tales como el coeficiente Alfa de Cronbach. La inclusión de este tipo de análisis permitiría evidenciar la consistencia interna de las herramientas de recolección de datos.

Finalmente, es necesario profundizar en la justificación del tipo de muestreo empleado, explicando con mayor detalle los criterios de selección de los participantes y su pertinencia en relación con el enfoque metodológico adoptado.

En conjunto, estos ajustes no comprometen la calidad general del estudio; sin embargo, su incorporación contribuiría significativamente a fortalecer la solidez metodológica del trabajo y a cumplir con los estándares exigidos por editoriales académicas.

CAPÍTULO IV

Resultados

ALUMNI EDITORA

Los resultados presentados evidencian tendencias significativas en relación con las variables analizadas. Este resultado sugiere que existe una relación directa entre la implementación de prácticas de ciberseguridad y el nivel de protección de las aplicaciones en plataformas educativos. Asimismo, se observa que la adopción de medidas preventivas contribuye a la reducción de vulnerabilidades, lo que tiene implicaciones importantes para la gestión de la seguridad de la información.

4.1 Presentación general de los resultados

En el presente capítulo se exponen de manera sistemática los resultados derivados de la aplicación del instrumento de recolección de datos a la muestra seleccionada, con el propósito de analizar las percepciones, conocimientos y prácticas relacionadas con la ciberseguridad, la computación y la protección de la información digital en los procesos de formación en plataformas digitales. El análisis se fundamenta en técnicas estadísticas descriptivas, particularmente mediante el uso de frecuencias absolutas y relativas, así como porcentajes, lo que permite identificar patrones de comportamiento, tendencias y niveles de apropiación de prácticas seguras dentro del contexto educativo.

La organización de los resultados responde a las variables definidas en el diseño metodológico, lo que facilita una interpretación estructurada y coherente del fenómeno estudiado. En este sentido, se presenta evidencia empírica que permite comprender no solo el nivel de conocimiento en ciberseguridad, sino también la forma en que los participantes interactúan con las herramientas tecnológicas y adoptan medidas de protección de la información.

Es importante señalar que los resultados no se limitan a una descripción cuantitativa, sino que se interpretan en función de su relevancia para la construcción de plataformas educativas seguros, permitiendo identificar fortalezas, debilidades y oportunidades de mejora en la formación digital. A partir de esta base, se desarrollan los análisis específicos correspondientes a cada variable de estudio.

4.2 Resultados sobre conocimientos en ciberseguridad

El análisis del nivel de conocimiento en ciberseguridad constituye un elemento central para comprender la capacidad de los participantes para

identificar riesgos y adoptar medidas de protección en plataformas digitales. Desde esta perspectiva, se evaluó el grado de dominio conceptual en temas relacionados con la seguridad de la información, así como el reconocimiento de amenazas digitales y normativas institucionales.

Antes de presentar los resultados, es importante destacar que el conocimiento en ciberseguridad no solo implica la comprensión de conceptos, sino también la capacidad de aplicarlos en situaciones reales, lo cual incide directamente en la prevención de incidentes de seguridad.

A continuación, se presenta la tabla 2, que refleja el nivel general de conocimiento en ciberseguridad.

Tabla 2. Nivel general de conocimiento en ciberseguridad

Nivel de conocimiento	Frecuencia	Porcentaje (%)	Interpretación
Alto	18	18%	Dominio sólido
Medio	52	52%	Conocimiento básico
Bajo	30	30%	Conocimiento limitado

Los resultados presentados en la tabla 2 evidencian que la mayoría de los participantes se ubica en un nivel medio de conocimiento, lo que indica que poseen nociones generales sobre ciberseguridad, pero carecen de una comprensión profunda y especializada. Este hallazgo sugiere que, aunque existe una base conceptual inicial, esta no es suficiente para garantizar una protección efectiva frente a amenazas digitales.

Con el fin de profundizar en la comprensión de estos resultados, en la tabla 3 se analiza el nivel de conocimiento específico sobre amenazas digitales, considerando su relevancia en la identificación de riesgos.

Tabla 3. Conocimiento de amenazas digitales

Tipo de amenaza	Frecuencia	Porcentaje (%)	Nivel de conocimiento
Phishing	40	40%	Moderado
Malware	35	35%	Bajo
Ransomware	15	15%	Muy bajo
Suplantación	10	10%	Bajo

La tabla 3 revela una distribución desigual en el conocimiento de amenazas digitales, destacando una mayor familiaridad con el phishing, posiblemente debido a su frecuente aparición en plataformas cotidianos. En contraste, amenazas más complejas como el ransomware presentan un bajo nivel de reconocimiento, lo que incrementa la vulnerabilidad de los usuarios frente a este tipo de ataques.

Finalmente, se analiza el nivel de conocimiento sobre políticas institucionales, elemento clave para la protección de la información en contextos educativos, ver tabla 4.

Tabla 4. Conocimiento de políticas institucionales

Mantiene Conocimiento	Frecuencia	Porcentaje (%)	Interpretación
Sí	28	28%	Conocimiento adecuado
No	72	72%	Desconocimiento

Los datos de la tabla 4 evidencian un alto nivel de desconocimiento de las políticas institucionales, lo cual representa una debilidad crítica en la gestión de la seguridad digital. Esta situación pone de manifiesto la necesidad de fortalecer los mecanismos de difusión y capacitación en normativas de protección de datos dentro de las instituciones educativas.

4.3 Resultados sobre el uso de herramientas computacionales

El análisis del uso de herramientas computacionales permite comprender el grado de integración tecnológica en los procesos de formación y su relación con las prácticas de seguridad digital. Por consiguiente, se evaluó la frecuencia de uso de plataformas digitales, así como las prácticas asociadas a su utilización segura.

En primer lugar, se presenta la tabla 5, que describe las plataformas digitales más utilizadas por los participantes.

Tabla 5. Uso de plataformas digitales

Plataforma utilizada	Frecuencia	Porcentaje (%)	Nivel de uso
LMS	60	60%	Alto
Correo institucional	70	70%	Muy alto
Nube	50	50%	Medio

La tabla 5 evidencia una alta dependencia de herramientas digitales, especialmente del correo institucional, lo que confirma la centralidad de la tecnología en los procesos educativos actuales. No obstante, este uso intensivo también implica mayores riesgos si no se acompaña de prácticas de seguridad adecuadas.

Para analizar este aspecto, se presenta la tabla 6, relacionada con la verificación de seguridad en las plataformas utilizadas.

Tabla 6. Verificación de seguridad en plataformas

Verificación	Frecuencia	Porcentaje (%)	Interpretación
Siempre	25	25%	Adecuado
A veces	45	45%	Riesgo medio
Nunca	30	30%	Alto riesgo

Los resultados en la tabla 6, muestran que una proporción significativa de los usuarios no verifica de manera constante la seguridad de las plataformas, lo que incrementa su exposición a amenazas digitales.

Finalmente, se analiza el uso de copias de seguridad como medida de protección de la información, véase la tabla 7.

Tabla 7. Uso de copias de seguridad

Frecuencia de respaldo	Frecuencia	Porcentaje (%)	Nivel de protección
Frecuente	20	20%	Alto
Ocasional	40	40%	Medio
Nunca	40	40%	Bajo

La tabla 7 evidencia una limitada cultura de respaldo de información, lo cual representa un riesgo significativo ante posibles pérdidas de datos.

4.4 Prácticas de seguridad digital

El análisis de las prácticas de seguridad digital permite evaluar el comportamiento real de los usuarios frente a los riesgos tecnológicos, más allá del conocimiento teórico que poseen. De este modo, se examinan aspectos como el uso de contraseñas, la actualización de dispositivos y la implementación de herramientas de protección.

Se presenta a continuación la tabla 8, relacionada con el tipo de contraseñas utilizadas.

Tabla 8. Tipo de contraseñas utilizadas

Tipo de contraseña	Frecuencia	Porcentaje (%)	Nivel de seguridad
Complejas	30	30%	Alto
Simples	50	50%	Bajo
Repetidas	20	20%	Muy bajo

Los resultados de la tabla 8 evidencian una tendencia hacia el uso de contraseñas inseguras, lo que constituye una de las principales vulnerabilidades en plataformas digitales.

A continuación, en la tabla 9 se analiza la frecuencia de actualización de dispositivos.

Tabla 9. Actualización de dispositivos

Frecuencia	Frecuencia	Porcentaje (%)	Interpretación
Regular	35	35%	Adecuado
Irregular	45	45%	Riesgo medio
Nunca	20	20%	Alto riesgo

Estos resultados de la tabla 9 reflejan prácticas insuficientes que pueden facilitar la explotación de vulnerabilidades.

Finalmente, se presenta la tabla 10 sobre el uso de software antivirus.

Tabla 10. Uso de antivirus

Uso de antivirus	Frecuencia	Porcentaje (%)	Nivel de protección
Permanente	40	40%	Alto
Ocasional	30	30%	Medio
No usa	30	30%	Bajo

Se observa en la tabla 10 que una proporción importante de usuarios no mantiene protección constante, lo que incrementa el riesgo de incidentes de seguridad.

4.5 Resultados sobre protección digital en los procesos de formación

El análisis de la protección digital en los procesos de formación permite comprender la percepción de los usuarios sobre la seguridad en plataformas educativas y su impacto en la experiencia de aprendizaje. Esta dimensión integra elementos cognitivos, actitudinales y conductuales que influyen en la confianza en el uso de tecnologías.

En primer lugar, se presenta la tabla 11, relacionada con la percepción de seguridad digital.

Tabla 11. Percepción de seguridad digital

Percepción	Frecuencia	Porcentaje (%)	Nivel
Alta	30	30%	Confianza
Media	50	50%	Moderada
Baja	20	20%	Inseguridad

Los resultados de la tabla 11 indican que la mayoría de los participantes presenta una percepción moderada de seguridad, lo que sugiere una confianza limitada en las plataformas digitales.

A continuación, en la tabla 12 se analiza el nivel de preparación ante amenazas digitales.

Tabla 12. Preparación ante amenazas

Preparación	Frecuencia	Porcentaje (%)	Interpretación
Preparado	25	25%	Adecuado
Parcial	45	45%	Limitado
No preparado	30	30%	Crítico

La tabla 12 evidencia que una proporción significativa de los participantes no se siente completamente preparada para enfrentar amenazas digitales, lo que refuerza la necesidad de fortalecer la formación en ciberseguridad dentro del ámbito educativo.

4.6 Relación entre ciberseguridad y protección digital en los procesos de formación

El análisis de la relación entre la ciberseguridad y la protección digital en los procesos de formación permite comprender cómo el nivel de conocimiento influye directamente en la confianza, el comportamiento y la adopción de prácticas seguras dentro de las plataformas educativas digitales. En consecuencia, no solo se busca identificar asociaciones entre variables, sino

también interpretar cómo dichas relaciones impactan en la calidad del proceso formativo y en la percepción de seguridad por parte de los usuarios.

Para profundizar en esta relación, se presenta la siguiente tabla que evidencia la correspondencia entre el nivel de conocimiento en ciberseguridad y el grado de confianza en el uso de plataformas digitales, véase tabla 13.

Tabla 13. Relación entre nivel de conocimiento y confianza en plataformas digitales

Nivel de conocimiento	Nivel de confianza	Frecuencia	Porcentaje (%)	Interpretación
Alto	Alto	15	15%	Relación positiva fuerte
Medio	Medio	50	50%	Relación moderada
Bajo	Bajo	35	35%	Relación directa

Los resultados presentados en la tabla 13 evidencian una relación directamente proporcional entre el nivel de conocimiento en ciberseguridad y la confianza en el uso de plataformas digitales. Aquellos participantes con mayor formación muestran una percepción más positiva y segura frente al uso de tecnologías, lo que sugiere que el conocimiento no solo tiene un impacto cognitivo, sino también conductual y emocional.

Con el propósito de profundizar en esta relación, se analiza la incidencia de la formación en ciberseguridad sobre la adopción de prácticas seguras, ver tabla 14.

Tabla 14. Influencia de la formación en ciberseguridad sobre prácticas digitales

Nivel de formación	Prácticas seguras altas	Frecuencia	Porcentaje (%)	Interpretación
Alta	Sí	20	20%	Alta influencia
Media	Parcial	50	50%	Influencia moderada

Baja	No	30	30%	Baja influencia

La tabla 14 confirma que la formación en ciberseguridad incide de manera significativa en la adopción de prácticas seguras. Los participantes con mayor nivel formativo tienden a implementar medidas de protección más consistentes, lo que refuerza la necesidad de integrar programas educativos orientados a la seguridad digital.

4.7 Interpretación global de los resultados

La interpretación global de los resultados permite integrar los hallazgos obtenidos en las diferentes dimensiones analizadas, proporcionando una visión holística del estado de la ciberseguridad en los procesos de formación en plataformas digitales. Este análisis no se limita a la descripción de datos, sino que busca comprender las dinámicas subyacentes que explican los comportamientos observados.

En este contexto, se identifica una brecha significativa entre el conocimiento teórico y la aplicación práctica de medidas de seguridad, lo que sugiere la existencia de factores adicionales que influyen en la conducta digital de los usuarios, tales como la cultura organizacional, la formación recibida y la percepción del riesgo.

Para reforzar esta interpretación, se presenta una tabla 15 que sintetiza las principales debilidades identificadas en el estudio.

Tabla 15. Principales debilidades en ciberseguridad identificadas

Dimensión	Nivel de debilidad	Frecuencia	Porcentaje (%)	Interpretación
Contraseñas	Alta	50	50%	Vulnerabilidad crítica
Actualizaciones	Media	45	45%	Riesgo moderado
Políticas	Alta	72	72%	Falta institucional

La tabla 15 permite identificar que las principales debilidades se concentran en el uso inadecuado de contraseñas y en el desconocimiento de

políticas institucionales, lo cual evidencia una problemática estructural que trasciende el ámbito individual y se relaciona con la gestión institucional de la seguridad.

Este panorama refleja la necesidad de abordar la ciberseguridad desde una perspectiva integral, que combine formación, regulación y cultura organizacional.

4.8 Implicaciones de los resultados para el ámbito educativo

Los resultados obtenidos tienen implicaciones significativas para el diseño de estrategias educativas orientadas al fortalecimiento de la ciberseguridad en plataformas de formación digital. En particular, se evidencia la necesidad de integrar la seguridad de la información como un componente transversal en los procesos educativos, promoviendo no solo el conocimiento teórico, sino también el desarrollo de competencias prácticas.

En este sentido, las instituciones educativas deben asumir un rol activo en la formación de usuarios digitales responsables, capaces de identificar riesgos y adoptar medidas preventivas en su interacción con las tecnologías.

Para profundizar en estas implicaciones, se presenta la siguiente tabla 16:

Tabla 16. Necesidades de formación en ciberseguridad

Área de formación	Nivel de necesidad	Frecuencia	Porcentaje (%)	Interpretación
Protección de datos	Alta	60	60%	Prioridad educativa
Uso seguro de plataformas	Media	25	25%	Necesario
Prevención de ataques	Alta	15	15%	Crítico

La tabla 16 evidencia que la protección de datos y la prevención de ataques constituyen áreas prioritarias en la formación en ciberseguridad, lo que sugiere la necesidad de diseñar programas educativos específicos que aborden estas temáticas de manera estructurada.

Estas implicaciones refuerzan la importancia de desarrollar políticas institucionales que promuevan la seguridad digital como un eje transversal en la educación.

4.9 Interpretación final

El análisis integral de los resultados permite concluir que la ciberseguridad y la computación desempeñan un papel fundamental en la construcción de plataformas de protección digital en los procesos de formación. Si bien se observa un nivel básico de conocimiento en la mayoría de los participantes, persisten debilidades significativas en la aplicación práctica de medidas de seguridad, lo que evidencia una brecha entre la teoría y la práctica.

Desde esta perspectiva, los resultados destacan la necesidad de fortalecer la formación en ciberseguridad, promover una cultura institucional orientada a la protección de la información y desarrollar estrategias educativas que integren la seguridad digital como un componente esencial del proceso formativo. Asimismo, se evidencia que la mejora en los niveles de conocimiento incide positivamente en la confianza y en la adopción de prácticas seguras, lo que contribuye a la construcción de plataformas educativas más seguros, confiables y resilientes frente a las amenazas de la plataforma digital.

Estos resultados no solo evidencian la situación actual, sino que también plantean la necesidad de futuras investigaciones que profundicen en modelos de intervención educativa en ciberseguridad, considerando variables como el contexto institucional, el nivel de formación tecnológica y la evolución de las amenazas digitales.

CAPÍTULO V

Discusión

ALUMNI EDITORA

Los resultados obtenidos en este estudio coinciden con lo planteado por Mishra et al. (2023), quienes identifican la ciberseguridad como un elemento crítico en las plataformas de aprendizaje digital. Sin embargo, difieren parcialmente de Nguyen et al. (2022), quienes abordan el fenómeno desde una perspectiva más general sin profundizar en la integración de marcos normativos. Por consiguiente, los hallazgos del presente estudio aportan una visión más integradora que articula aspectos técnicos, educativos y organizacionales.

En términos de implicaciones, los resultados tienen un impacto significativo en diferentes niveles. Desde el ámbito educativo, se destaca la necesidad de fortalecer la formación en competencias digitales seguras. En el ámbito tecnológico, se evidencia la importancia de implementar marcos de ciberseguridad que garanticen la protección de las aplicaciones. Finalmente, a nivel organizacional, se resalta la necesidad de promover una cultura de seguridad que involucre a todos los actores del sistema educativo.

5.1 Análisis general de los hallazgos

Los resultados obtenidos en la presente investigación permitieron evidenciar, de manera consistente, la relevancia creciente de la ciberseguridad aplicada en la protección de aplicaciones y en la gestión segura de la información digital dentro de los procesos de formación en plataformas digitales. A partir del análisis empírico, se constató que, si bien los participantes demostraron poseer un nivel básico de conocimiento en materia de seguridad informática, este no se traduce de manera efectiva en la adopción de prácticas seguras, lo que pone de manifiesto una brecha significativa entre el conocimiento teórico y su aplicación práctica.

Esta situación adquiere especial relevancia en el contexto educativo, donde el uso intensivo de plataformas digitales, servicios en la nube y herramientas colaborativas incrementa la superficie de exposición a riesgos cibernéticos. La evidencia recopilada muestra que prácticas como el uso de contraseñas débiles, la falta de verificación de la seguridad en plataformas digitales y la ausencia de copias de seguridad son comportamientos recurrentes que comprometen la integridad, confidencialidad y disponibilidad de la información, principios fundamentales de la seguridad de la información.

Desde una perspectiva más amplia, los hallazgos reflejan que la seguridad de las aplicaciones y la gestión de la información digital no pueden ser abordadas únicamente desde un enfoque tecnológico, sino que requieren la integración de factores humanos, organizacionales y normativos. De este modo, el comportamiento del usuario emerge como un elemento crítico dentro del ecosistema de ciberseguridad, coincidiendo con enfoques contemporáneos que destacan la necesidad de fortalecer la cultura de seguridad como eje central de cualquier estrategia de protección digital.

Asimismo, se identificó que la percepción de seguridad por parte de los usuarios está estrechamente vinculada con su nivel de formación, lo que sugiere que la educación en ciberseguridad no solo impacta en las prácticas, sino también en la confianza y en la disposición para utilizar tecnologías digitales en los procesos de aprendizaje. Este aspecto resulta clave para garantizar la sostenibilidad de las plataformas de formación digital en un contexto cada vez más dependiente de la tecnología.

5.2 Relación con investigaciones previas

Los resultados obtenidos en esta investigación se encuentran en consonancia con diversos estudios desarrollados en el ámbito de la ciberseguridad aplicada a la educación, los cuales han señalado de manera reiterada que la incorporación de tecnologías digitales en los procesos formativos no ha sido acompañada, en igual medida, por una formación sólida en seguridad de la información. Esta brecha ha sido identificada como uno de los principales desafíos en la transformación digital educativa.

En particular, investigaciones previas han destacado que el factor humano continúa siendo el eslabón más vulnerable dentro de los sistemas de información, debido principalmente a la falta de conciencia, capacitación y adopción de buenas prácticas en seguridad digital. Este planteamiento se ve reforzado por los resultados del presente estudio, donde se evidencia un uso inadecuado de medidas básicas de protección, lo que incrementa la exposición a amenazas como el phishing, el malware y el acceso no autorizado a sistemas.

Desde el punto de vista normativo y técnico, los hallazgos también pueden ser interpretados a la luz de marcos internacionales como la norma ISO 27001, el marco de ciberseguridad del NIST y las directrices de OWASP para la seguridad

de aplicaciones. Estos referentes coinciden en señalar que la gestión de la seguridad de la información debe basarse en un enfoque integral que incluya la identificación de riesgos, la implementación de controles y la formación continua de los usuarios.

En consecuencia, la baja adopción de prácticas como la actualización de sistemas, el uso de autenticación robusta y la protección de datos evidencia una falta de alineación con los principios establecidos por estos marcos, lo que sugiere la necesidad de incorporar estándares internacionales en los procesos educativos como parte de una estrategia de fortalecimiento de la ciberseguridad.

De igual manera, estudios recientes han demostrado que existe una relación directa entre el nivel de alfabetización digital en ciberseguridad y la confianza en el uso de tecnologías, lo cual coincide plenamente con los resultados obtenidos, donde los participantes con mayor conocimiento mostraron una actitud más favorable hacia el uso de plataformas digitales seguros.

5.3 Implicaciones educativas de los resultados

Los hallazgos de la investigación tienen implicaciones profundas para el ámbito educativo, particularmente en lo que respecta a la integración de la ciberseguridad como un componente esencial en los procesos de formación. La evidencia sugiere que la enseñanza de competencias digitales no puede limitarse al uso de herramientas tecnológicas, sino que debe incorporar de manera explícita la formación en seguridad de la información, protección de datos y gestión de riesgos digitales.

En este contexto, la ciberseguridad aplicada debe ser concebida como una competencia transversal, presente en todas las áreas del conocimiento y niveles educativos, con el objetivo de formar ciudadanos digitales capaces de interactuar de manera segura, crítica y responsable en la plataforma tecnológica. Esta perspectiva implica una transformación en los enfoques pedagógicos tradicionales, promoviendo modelos educativos que integren la teoría con la práctica y que fomenten el aprendizaje basado en situaciones reales de riesgo.

Asimismo, las instituciones educativas están llamadas a desempeñar un rol protagónico en la creación de plataformas digitales seguros, lo que implica no solo la implementación de infraestructura tecnológica adecuada, sino también el desarrollo de políticas institucionales claras, alineadas con estándares

internacionales, que regulen el uso de plataformas digitales y la protección de la información.

La capacitación continua de docentes y estudiantes emerge como un elemento clave para garantizar la efectividad de estas estrategias, ya que permite actualizar conocimientos, reforzar buenas prácticas y adaptarse a la evolución constante de las amenazas cibernéticas. En este sentido, la formación en ciberseguridad debe ser entendida como un proceso dinámico y permanente, que acompaña el desarrollo tecnológico y las necesidades de la plataforma educativa.

5.4 Aportes del estudio

La presente investigación aporta de manera significativa al campo de la ciberseguridad aplicada a la educación al integrar, en un mismo marco analítico, los conceptos de protección de aplicaciones, gestión segura de la información digital y procesos de formación en plataformas digitales. Este enfoque integral permite abordar la problemática desde una perspectiva sistémica, considerando la interacción entre factores tecnológicos, humanos y organizacionales.

Uno de los principales aportes radica en la generación de evidencia empírica que permite caracterizar el nivel de conocimiento y las prácticas de ciberseguridad en un contexto educativo específico, lo cual constituye una base sólida para la toma de decisiones en materia de políticas institucionales y diseño de programas formativos. Este tipo de información resulta fundamental para identificar áreas críticas de intervención y priorizar acciones orientadas a la mejora de la seguridad digital.

Adicionalmente, el estudio contribuye a visibilizar la importancia de la protección de aplicaciones dentro del plataforma educativa, un aspecto que, aunque relevante, ha sido tradicionalmente abordado desde una perspectiva técnica y no pedagógica. La incorporación de este enfoque permite ampliar la comprensión de la ciberseguridad como un elemento transversal en los procesos de enseñanza y aprendizaje.

Finalmente, la investigación sienta las bases para el desarrollo de un modelo de protección digital en los procesos de formación, el cual integra principios de gestión de riesgos, buenas prácticas de seguridad y estándares internacionales, constituyéndose en una propuesta innovadora para fortalecer la resiliencia de las plataformas educativas frente a las amenazas del ciberespacio.

5.5 Limitaciones del estudio

A pesar de los aportes realizados, la investigación presenta ciertas limitaciones que deben ser consideradas al momento de interpretar los resultados. En primer lugar, el tamaño de la muestra, aunque suficiente para el análisis descriptivo, puede limitar la generalización de los hallazgos a otros contextos educativos con características diferentes.

Asimismo, el uso de un enfoque cuantitativo basado en encuestas implica una dependencia de la percepción y autodeclaración de los participantes, lo que puede introducir sesgos en la información recopilada. La ausencia de técnicas cualitativas, como entrevistas o grupos focales, limita la profundidad del análisis en términos de comprensión de las motivaciones, actitudes y experiencias de los usuarios frente a la ciberseguridad.

Otra limitación relevante está relacionada con el carácter transversal del estudio, el cual permite analizar la situación en un momento específico, pero no posibilita establecer relaciones causales ni observar la evolución de las prácticas de seguridad a lo largo del tiempo. Este aspecto resulta especialmente importante en el ámbito de la ciberseguridad, donde las amenazas y tecnologías evolucionan de manera constante.

No obstante, estas limitaciones no desvirtúan la validez de los resultados, sino que deben ser entendidas como oportunidades para el desarrollo de investigaciones futuras que profundicen y amplíen el conocimiento en este campo.

5.6 Proyecciones para investigaciones futuras

Los resultados obtenidos abren diversas líneas de investigación que pueden contribuir al fortalecimiento del conocimiento en ciberseguridad aplicada a los procesos de formación. Desde esta perspectiva, resulta pertinente desarrollar estudios que incorporen enfoques metodológicos mixtos, combinando técnicas cuantitativas y cualitativas, con el fin de obtener una comprensión más integral de las prácticas y percepciones de los usuarios.

Asimismo, se recomienda ampliar el alcance de las investigaciones a diferentes contextos educativos, incluyendo instituciones de distintos niveles y características, lo que permitiría identificar patrones comunes y particularidades

en la gestión de la seguridad digital. Esta ampliación facilitaría la construcción de modelos más robustos y generalizables.

Otra línea de investigación relevante consiste en evaluar el impacto de programas de capacitación en ciberseguridad sobre las prácticas de los usuarios, lo que permitiría medir la efectividad de las intervenciones educativas y ajustar las estrategias formativas en función de los resultados obtenidos.

De igual manera, resulta fundamental profundizar en el estudio de la seguridad de aplicaciones en plataformas educativos, considerando aspectos como el desarrollo seguro de software, la protección de datos en plataformas digitales y la implementación de controles basados en estándares internacionales como OWASP, lo que contribuiría a fortalecer la protección de la información desde su origen.

5.7 Análisis

La discusión de los resultados permite establecer que la ciberseguridad aplicada, entendida como la protección de aplicaciones y la gestión segura de la información digital, constituye un elemento esencial para el desarrollo de plataformas de formación seguros, confiables y resilientes. Los hallazgos evidencian que, aunque existe un nivel básico de conocimiento en la comunidad académica, persisten debilidades significativas en la aplicación de prácticas de seguridad, lo que pone de manifiesto la necesidad de fortalecer la formación en este ámbito.

La investigación confirma que la seguridad digital no puede ser abordada de manera aislada, sino que requiere un enfoque integral que articule la tecnología, la educación y la gestión institucional. Por consiguiente, la incorporación de estándares internacionales, la formación continua y el desarrollo de políticas institucionales emergen como elementos clave para garantizar la protección de la información en los procesos educativos.

Este capítulo establece un puente sólido entre los resultados obtenidos y las conclusiones del estudio, proporcionando una interpretación crítica que orienta la toma de decisiones y sienta las bases para el desarrollo de propuestas innovadoras en materia de ciberseguridad aplicada a la educación.

De este modo, la consolidación de modelos integrales de ciberseguridad en la educación representa un desafío estratégico que demanda la articulación entre

políticas institucionales, innovación tecnológica y formación continua, orientadas a garantizar la protección sostenible de la información en las plataformas digitales.

CAPÍTULO VI

Conclusiones y recomendaciones

ALUMNI EDITORA

6.1 Conclusiones generales

La presente investigación permitió comprender, desde una perspectiva integral, el papel fundamental que desempeña la ciberseguridad aplicada en la protección de aplicaciones y en la gestión segura de la información digital dentro de los procesos de formación en plataformas digitales. A partir del análisis de los resultados, se evidenció que la transformación digital en el ámbito educativo ha generado un ecosistema altamente interconectado, en el cual el acceso, procesamiento y almacenamiento de la información se realizan de manera constante mediante plataformas tecnológicas, lo que incrementa significativamente la exposición a riesgos cibernéticos.

En este contexto, se concluye que la ciberseguridad no puede ser concebida como un componente aislado o exclusivamente técnico, sino como un eje transversal que articula la tecnología, la educación y la gestión institucional. La protección de aplicaciones utilizadas en las plataformas de aprendizaje, así como la correcta gestión de la información digital, requieren no solo de infraestructuras seguras, sino también de usuarios capacitados, conscientes y comprometidos con el uso responsable de las tecnologías.

Asimismo, los hallazgos permiten afirmar que la seguridad de la información en los procesos de formación depende en gran medida del comportamiento humano, lo que refuerza la idea de que el factor humano constituye tanto el eslabón más vulnerable como el principal agente de defensa dentro del ecosistema digital. La existencia de prácticas inadecuadas, como el uso de contraseñas débiles, la falta de actualización de sistemas o el desconocimiento de políticas institucionales, pone en evidencia la necesidad de fortalecer la cultura de ciberseguridad en todos los niveles del sistema educativo.

De igual manera, se establece que existe una relación directa y significativa entre el nivel de conocimiento en ciberseguridad y la percepción de confianza en el uso de aplicaciones y plataformas digitales. Este aspecto resulta determinante, ya que la confianza influye en la adopción de tecnologías educativas y en la continuidad de los procesos formativos en plataformas digitales. En consecuencia, la formación en ciberseguridad se consolida como un elemento clave para garantizar no solo la protección de la información, sino también la calidad y sostenibilidad del proceso educativo.

Finalmente, se concluye que la integración de principios de ciberseguridad aplicada en la educación constituye una necesidad impostergable en el contexto actual, caracterizado por la constante evolución de las amenazas digitales. La protección de aplicaciones y la gestión segura de la información deben ser incorporadas como pilares fundamentales en la construcción de plataformas de aprendizaje resilientes, capaces de adaptarse a los desafíos del ciberespacio.

6.2 Conclusiones específicas

Del análisis detallado de los resultados se derivan conclusiones específicas que permiten comprender con mayor precisión las dinámicas observadas en relación con la ciberseguridad aplicada en los procesos de formación. En primer lugar, se evidenció que, aunque los participantes reconocen la importancia de la seguridad digital, este reconocimiento no se traduce de manera consistente en prácticas adecuadas de protección de la información, lo que refleja una desconexión entre el conocimiento conceptual y su aplicación práctica.

Se constató que el uso de herramientas computacionales es elevado dentro del plataforma educativa, especialmente en lo referente a plataformas de aprendizaje, servicios de comunicación y almacenamiento en la nube. Sin embargo, este uso intensivo no siempre está acompañado de una comprensión adecuada de los riesgos asociados, lo que incrementa la probabilidad de incidentes de seguridad que pueden afectar tanto a los usuarios como a las instituciones.

Asimismo, se identificó una carencia significativa en la formación estructurada en ciberseguridad, tanto en estudiantes como en docentes, lo que limita la capacidad de respuesta frente a amenazas digitales y dificulta la adopción de medidas preventivas. Esta situación se agrava por la ausencia o insuficiente difusión de políticas institucionales claras en materia de seguridad de la información, lo que genera incertidumbre y prácticas heterogéneas en el uso de las tecnologías.

Otro aspecto relevante es que la protección digital en los procesos de formación no depende exclusivamente de la infraestructura tecnológica, sino que está condicionada por factores culturales, organizacionales y educativos que influyen en el comportamiento de los usuarios. En consecuencia, la gestión segura de la información digital requiere una visión integral que contemple tanto

la implementación de controles técnicos como el fortalecimiento de la conciencia y responsabilidad digital.

Finalmente, se concluye que la protección de aplicaciones en plataformas educativas constituye un componente crítico de la ciberseguridad aplicada, ya que estas herramientas representan el principal medio de interacción entre los actores del proceso formativo. La seguridad de estas aplicaciones debe ser garantizada mediante prácticas de desarrollo seguro, evaluación de vulnerabilidades y cumplimiento de estándares internacionales.

6.3 Recomendaciones educativas

A partir de las conclusiones alcanzadas, se hace evidente la necesidad de transformar los enfoques educativos tradicionales para incorporar de manera efectiva la ciberseguridad aplicada como parte integral de la formación académica. En este sentido, se recomienda que los planes de estudio incluyan contenidos específicos relacionados con la protección de aplicaciones, la gestión segura de la información digital, la privacidad y la ética en el uso de las tecnologías, de manera que los estudiantes desarrollen competencias que les permitan enfrentar los desafíos de la plataforma digital con criterio y responsabilidad.

La formación en ciberseguridad debe trascender el enfoque teórico y orientarse hacia el desarrollo de habilidades prácticas, mediante el uso de metodologías activas que involucren la resolución de problemas, el análisis de casos reales y la simulación de escenarios de riesgo. Este enfoque permitirá a los estudiantes comprender la complejidad de las amenazas digitales y adquirir herramientas para prevenirlas y gestionarlas de manera efectiva.

Asimismo, se recomienda fortalecer la capacitación docente en materia de ciberseguridad aplicada, de modo que los educadores puedan integrar estos conocimientos en sus prácticas pedagógicas y actuar como agentes multiplicadores dentro de la comunidad académica. La actualización constante del profesorado resulta fundamental en un campo caracterizado por su rápida evolución.

De igual manera, es necesario promover una cultura de seguridad digital basada en la sensibilización, la prevención y la responsabilidad compartida, mediante campañas educativas que destaquen la importancia de proteger la

información y utilizar de manera adecuada las aplicaciones tecnológicas en la plataforma educativa.

6.4 Recomendaciones institucionales

Desde el ámbito institucional, se requiere la adopción de un enfoque estratégico que permita garantizar la protección de aplicaciones y la gestión segura de la información digital de manera sostenible. Desde esta perspectiva, resulta fundamental establecer políticas claras, coherentes y alineadas con estándares internacionales de ciberseguridad, que regulen el uso de las plataformas tecnológicas y definan responsabilidades dentro de la organización.

Las instituciones deben implementar mecanismos de seguridad que incluyan controles de acceso, autenticación robusta, monitoreo de actividades y sistemas de respaldo de información, con el objetivo de proteger los activos digitales y asegurar la continuidad de los procesos educativos. La adopción de marcos de referencia como ISO 27001, el marco NIST y las directrices de OWASP puede contribuir significativamente a la estructuración de una gestión eficaz de la seguridad de la información.

Asimismo, es recomendable designar responsables o unidades especializadas en ciberseguridad que se encarguen de la supervisión, evaluación y mejora continua de las prácticas de seguridad digital, así como de la respuesta ante incidentes. La gestión de riesgos debe convertirse en un proceso permanente, que permita identificar vulnerabilidades y anticipar posibles amenazas.

De igual manera, se sugiere realizar auditorías periódicas de seguridad y evaluaciones de vulnerabilidad en las aplicaciones utilizadas en los procesos de formación, con el fin de garantizar su integridad y confiabilidad. Estas acciones permitirán fortalecer la resiliencia institucional frente a los desafíos de la plataforma digital.

6.5 Recomendaciones para futuras investigaciones

Los resultados obtenidos en esta investigación abren nuevas posibilidades para el desarrollo de estudios que profundicen en la comprensión de la ciberseguridad aplicada en contextos educativos. Por consiguiente, se recomienda que futuras investigaciones adopten enfoques metodológicos mixtos

que integren técnicas cuantitativas y cualitativas, lo que permitirá obtener una visión más completa de las percepciones, experiencias y prácticas de los usuarios.

Asimismo, resulta pertinente ampliar el alcance de los estudios a diferentes niveles educativos y contextos institucionales, con el objetivo de identificar patrones comunes y particularidades en la gestión de la seguridad digital. Este tipo de análisis comparativo contribuirá a la construcción de modelos más robustos y adaptables a diversas realidades.

Otra línea de investigación relevante consiste en evaluar el impacto de programas de formación en ciberseguridad sobre el comportamiento de los usuarios y la reducción de incidentes de seguridad, lo que permitirá medir la efectividad de las estrategias educativas implementadas.

Finalmente, se sugiere profundizar en el estudio de la seguridad de aplicaciones en plataformas educativos, abordando aspectos relacionados con el desarrollo seguro, la protección de datos y la implementación de controles basados en estándares internacionales, lo que contribuirá a fortalecer la gestión de la información desde una perspectiva integral.

6.6 Reflexión final

Las conclusiones y recomendaciones presentadas en este capítulo reflejan la necesidad imperante de consolidar la ciberseguridad aplicada como un componente esencial en la protección de aplicaciones y en la gestión segura de la información digital dentro de los procesos de formación. La evidencia obtenida a lo largo de la investigación demuestra que la construcción de plataformas educativas seguros no depende únicamente de la tecnología, sino de la articulación efectiva entre conocimiento, prácticas y políticas institucionales.

De este modo, la ciberseguridad debe ser entendida como un proceso continuo de aprendizaje, adaptación y mejora, que involucra a todos los actores del sistema educativo. La formación en competencias digitales seguras, el fortalecimiento de la cultura de protección de la información y la implementación de estrategias institucionales coherentes constituyen pilares fundamentales para enfrentar los desafíos de la plataforma digital contemporáneo.

El presente estudio aporta un modelo integrador que articula marcos de ciberseguridad, estrategias educativas y prácticas organizacionales para la protección de aplicaciones en plataformas digitales. Este aporte contribuye al

fortalecimiento de la seguridad de la información desde una perspectiva multidimensional, superando enfoques tradicionales centrados exclusivamente en la tecnología.

Este capítulo cierra el proceso investigativo integrando los hallazgos, la discusión y las implicaciones prácticas del estudio, y sienta las bases para la construcción de un modelo de protección digital en los procesos de formación, orientado a garantizar la seguridad, confiabilidad y sostenibilidad de la educación en la era digital.

CAPÍTULO VII

Propuesta de modelo de protección digital en los procesos de formación en plataformas de formación digital

ALUMNI EDITORA

7.1 Fundamentación de la propuesta

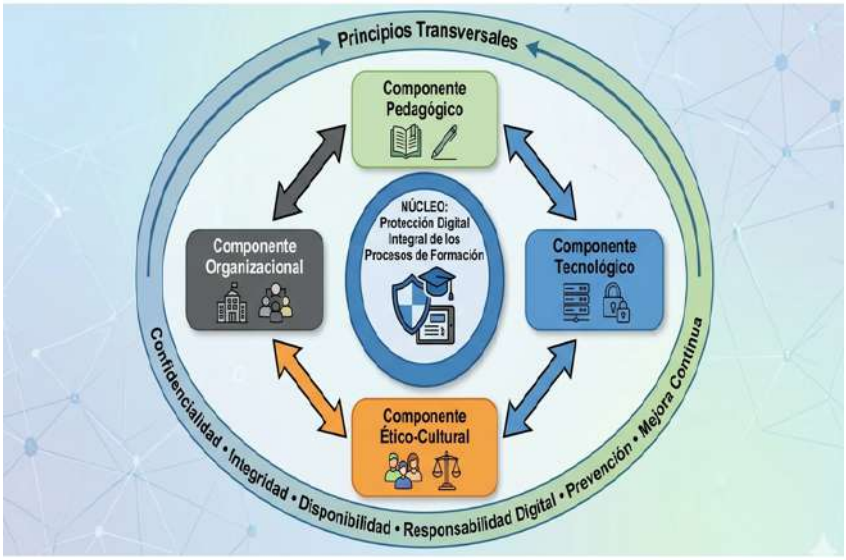
La evolución de las plataformas digitales ha transformado de manera profunda los procesos de formación, dando lugar a escenarios educativos altamente interconectados donde la información circula de forma constante a través de aplicaciones, plataformas virtuales y sistemas de gestión del aprendizaje. Este contexto ha incrementado significativamente la exposición a riesgos asociados a la ciberseguridad, lo que ha generado la necesidad de diseñar modelos estructurados que permitan garantizar la protección de las aplicaciones y la gestión segura de la información digital.

La presente propuesta se fundamenta en la integración de los principios de la ciberseguridad aplicada, la computación y la educación digital, entendiendo que la protección de las plataformas de formación no puede limitarse a la implementación de herramientas tecnológicas, sino que debe incorporar dimensiones pedagógicas, organizacionales y éticas que permitan abordar la problemática de manera integral. En consecuencia, el modelo propuesto reconoce que la seguridad de la información es un proceso dinámico que requiere adaptación constante frente a la evolución de las amenazas digitales.

Desde esta perspectiva, el modelo concibe la ciberseguridad como un eje transversal del proceso educativo, que influye tanto en la calidad del aprendizaje como en la confianza de los usuarios en el uso de las tecnologías. La protección de aplicaciones educativas, la preservación de la integridad de los datos académicos y la garantía de la privacidad de los usuarios se constituyen en elementos esenciales para la sostenibilidad de las plataformas digitales de formación.

De acuerdo con la fundamentación expuesta, el modelo se concibe como un sistema integrado donde la ciberseguridad aplicada actúa como eje transversal. En la figura 3 se presenta la visión general de la propuesta, ilustrando cómo el núcleo del modelo se articula con los cuatro componentes rectores (pedagógico, tecnológico, organizacional y ético-cultural) y se sustenta en principios dinámicos para garantizar la protección integral en los procesos de formación.

Figura 3. Visión general del modelo de protección digital en plataformas de formación



La figura 3 funciona como un mapa heurístico de la propuesta. Lo que observamos no es una simple lista de elementos, sino un ecosistema dinámico e interdependiente. En el centro, el "NÚCLEO" actúa como el sol de este sistema, estableciendo que el objetivo final no es la seguridad por la seguridad misma, sino la protección integral del acto educativo digital.

Rodeando este núcleo, los cuatro componentes rectores (Pedagógico, Tecnológico, Organizacional y Ético-Cultural) no están aislados; las flechas bidireccionales demuestran que un cambio en uno afecta inevitablemente a los otros. Por ejemplo, una nueva herramienta tecnológica (Tecnológico) requiere nuevos protocolos de uso (Organizacional) y nueva capacitación docente (Pedagógico), todo bajo un marco de responsabilidad (Ético-Cultural).

Finalmente, el anillo externo representa la "atmósfera" que hace respirable este modelo. Los principios de Confidencialidad, Integridad y Disponibilidad (la tríada CID), sumados a la Responsabilidad, Prevención y Mejora Continua, no son estáticos; son fuerzas transversales que deben estar presentes en cada acción, decisión y proceso formativo para garantizar la sostenibilidad del modelo en el tiempo frente a un panorama de amenazas en constante evolución.

Asimismo, la propuesta se sustenta en la necesidad de desarrollar competencias digitales seguras en los actores educativos, promoviendo una cultura de prevención, responsabilidad y uso ético de la información. De esta manera, el modelo no solo busca mitigar riesgos, sino también fortalecer las

capacidades de los usuarios para interactuar de manera segura en la plataforma digital, contribuyendo a la formación de ciudadanos digitales críticos y responsables.

7.2 Objetivos del modelo

El modelo de protección digital en los procesos de formación tiene como propósito central articular la ciberseguridad aplicada con la gestión educativa, de manera que se garantice la protección de las aplicaciones y la información digital en plataformas de aprendizaje virtual. En este sentido, el objetivo general se orienta al diseño de un marco integral que permita fortalecer la seguridad de los procesos formativos mediante la incorporación de principios de ciberseguridad y computación.

A partir de este propósito, se plantean objetivos específicos que buscan consolidar una cultura institucional basada en la seguridad digital, promover el desarrollo de competencias en ciberseguridad en estudiantes y docentes, integrar estrategias pedagógicas orientadas al uso seguro de las tecnologías, fortalecer las políticas institucionales de protección de datos y establecer mecanismos de evaluación continua que permitan monitorear y mejorar las prácticas de seguridad en los procesos educativos.

Estos objetivos reflejan una visión sistémica de la ciberseguridad aplicada, en la cual la protección de aplicaciones y la gestión de la información digital se conciben como procesos interdependientes que requieren la participación de todos los actores involucrados en la plataforma educativa.

7.3 Principios del modelo

El modelo propuesto se sustenta en un conjunto de principios que orientan su diseño e implementación, los cuales garantizan su coherencia y pertinencia en el contexto de la educación digital. Entre estos principios, la confidencialidad se establece como un elemento fundamental para la protección de los datos personales y académicos, asegurando que la información sea accesible únicamente para los usuarios autorizados. La integridad, por su parte, garantiza que los datos se mantengan completos, exactos y libres de alteraciones no autorizadas, lo que resulta esencial para la confiabilidad de los procesos educativos.

La disponibilidad se constituye en un principio clave que asegura el acceso oportuno y continuo a los recursos digitales, permitiendo la continuidad de los procesos de enseñanza y aprendizaje. A estos principios clásicos de la seguridad de la información se suma la responsabilidad digital, entendida como la capacidad de los usuarios para utilizar las tecnologías de manera ética y consciente, reconociendo las implicaciones de sus acciones en la plataforma digital.

Asimismo, el modelo incorpora el principio de prevención, orientado a la anticipación de riesgos mediante la formación y la sensibilización, así como el principio de mejora continua, que reconoce la necesidad de actualizar permanentemente las estrategias de seguridad frente a una plataforma tecnológica en constante cambio. Estos principios, en conjunto, proporcionan un marco conceptual sólido para la implementación de la ciberseguridad aplicada en los procesos de formación.

7.4 Componentes del modelo de protección digital en los procesos de formación

El modelo se estructura a partir de cuatro componentes interrelacionados que permiten abordar la ciberseguridad desde una perspectiva integral, articulando dimensiones pedagógicas, tecnológicas, organizacionales y culturales.

Para comprender la operatividad del modelo, es necesario desglosar la composición interna de cada una de sus dimensiones. La figura 4 detalla la estructura de los componentes, especificando los elementos clave, herramientas y subprocesos que conforman las áreas pedagógicas, tecnológica, organizacional y ético-cultural, evidenciando su interrelación sinérgica.

Figura 4. Detalle estructural de los componentes del modelo.

Esta figura 4 realiza un análisis detallado de la estructura operativa del modelo, desglosando la taxonomía visual de cada componente. Esta matriz es fundamental porque traduce la teoría en líneas de acción concretas.

Al observar la columna Pedagógica, vemos que la ciberseguridad deja de ser un tema técnico para convertirse en un contenido curricular y una competencia a evaluar a través de metodologías activas como el ABP. En la columna Tecnológica, se validan las herramientas técnicas necesarias, desde la seguridad de las aplicaciones (AppSec) hasta la encriptación y los backups, que sostienen la infraestructura.

Por su parte, la columna Organizacional establece el " marco normativo institucional" institucional: las políticas de datos (como GDPR), los protocolos de respuesta ante incidentes y la necesaria capacitación del personal. Finalmente, la columna Ético-Cultural aborda el factor humano desde los valores, promoviendo la privacidad, combatiendo el ciberacoso y construyendo una verdadera ciudadanía digital.

El elemento aglutinador es la flecha basal de "Interrelación Sinérgica". Esta nos recuerda que el modelo solo es efectivo si se lee horizontalmente; de nada sirve una tecnología robusta (Columna 2) sin una cultura de uso responsable (Columna 4).

7.4.1 Componente pedagógico

El componente pedagógico se orienta a la integración de la ciberseguridad dentro del proceso educativo, reconociendo que la formación en competencias digitales seguras es un elemento esencial para la protección de la información. Este componente promueve la incorporación de contenidos relacionados con la seguridad digital en los programas académicos, así como el desarrollo de actividades prácticas que permitan a los estudiantes identificar, analizar y mitigar riesgos en plataformas digitales.

La utilización de metodologías activas, como el aprendizaje basado en problemas y el análisis de casos, facilita la comprensión de situaciones reales vinculadas a la ciberseguridad, fortaleciendo la capacidad de los estudiantes para tomar decisiones informadas en contextos de riesgo. Asimismo, la evaluación de competencias digitales seguras se convierte en un mecanismo clave para medir el impacto de la formación y garantizar la adquisición de habilidades necesarias para la protección de aplicaciones y datos.

7.4.2 Componente tecnológico

El componente tecnológico se centra en la infraestructura y las herramientas utilizadas en las plataformas de formación, destacando la importancia de garantizar la seguridad de las aplicaciones educativas y de los sistemas de gestión de la información. Este componente implica la implementación de plataformas seguras, el uso de mecanismos de autenticación robusta, la actualización constante de software y la adopción de medidas de protección contra amenazas como el malware y los accesos no autorizados.

La gestión de copias de seguridad, la encriptación de datos y el monitoreo de actividades son prácticas fundamentales que contribuyen a la protección de la información digital. Asimismo, la aplicación de estándares internacionales de seguridad permite fortalecer la confiabilidad de las aplicaciones utilizadas en los procesos de formación, reduciendo la exposición a vulnerabilidades.

7.4.3 Componente organizacional

El componente organizacional aborda la gestión institucional de la ciberseguridad, destacando la necesidad de establecer políticas claras y procedimientos definidos que regulen el uso de las tecnologías en las plataformas

educativas. Este componente incluye la elaboración de normativas sobre protección de datos, la definición de protocolos de respuesta ante incidentes y la asignación de responsabilidades en materia de seguridad digital.

La capacitación continua del personal docente y administrativo constituye un elemento clave para garantizar la correcta implementación de las políticas de seguridad, así como la promoción de una cultura organizacional orientada a la prevención de riesgos. La gestión de la ciberseguridad, desde esta perspectiva, se concibe como un proceso estratégico que requiere planificación, supervisión y mejora continua.

Este componente se alinea con marcos internacionales como ISO 27001, el NIST Cybersecurity Framework y las directrices de OWASP, fortaleciendo la gestión de la seguridad en plataformas educativos.

7.4.4 Componente ético y cultural

El componente ético y cultural se orienta a la formación de valores y actitudes que promuevan el uso responsable de la tecnología y el respeto por la información digital. Este componente reconoce que la ciberseguridad no depende únicamente de factores técnicos, sino también del comportamiento de los usuarios y de la cultura institucional.

La promoción de la privacidad, la prevención del ciberacoso, la protección de la identidad digital y el fomento de la ciudadanía digital son aspectos fundamentales que contribuyen a la construcción de plataformas de formación seguros y respetuosos. La sensibilización y la educación en valores digitales permiten fortalecer la conciencia sobre los riesgos y responsabilidades asociados al uso de las tecnologías.

7.5 Estrategias para la implementación del modelo

La implementación del modelo requiere la adopción de estrategias que permitan su integración efectiva en los procesos de formación, considerando las particularidades de cada institución educativa. Desde esta perspectiva, se propone el desarrollo de programas de formación en ciberseguridad dirigidos a estudiantes y docentes, así como la elaboración de recursos educativos que promuevan buenas prácticas en el uso de la tecnología.

El uso de simulaciones y ejercicios prácticos orientados a la identificación de amenazas digitales permite fortalecer las competencias de los usuarios y mejorar su capacidad de respuesta ante incidentes de seguridad.

La efectividad de estas estrategias radica en la capacidad del modelo para operacionalizar los conceptos técnicos de seguridad en el día a día educativo. Como se visualiza en la figura 5, la integración de la ciberseguridad aplicada se materializa mediante la triangulación directa entre la protección de aplicaciones, la gestión segura de la información y la capacitación activa de los usuarios (estudiantes y docentes), cerrando la brecha entre la teoría técnica y la práctica formativa.

Figura 5. Modelo de Integración de Ciberseguridad Aplicada.

Esta figura es el corazón "aplicado" del libro, pues visualiza la convergencia de los tres pilares fundamentales que dan título a la obra. Utilizando un diagrama de Venn, la figura 5 demuestra que la ciberseguridad aplicada no reside en un solo punto, sino en la intersección armónica de tres dominios.

El Círculo A (Protección de Aplicaciones) representa la *fortaleza técnica*; el Círculo B (Gestión de la Información) representa el *activo a proteger*; y el Círculo C (Usuarios) representa el *factor humano y educativo*.

El valor analítico del diagrama reside en sus intersecciones. Donde la técnica (A) se encuentra con los datos (B), surge la Infraestructura Segura. Donde

los datos (B) se encuentran con las personas (C), surge el Uso Responsable. Y donde las personas (C) interactúan con la técnica (A), surge la Interacción Segura.

El hexágono dorado central, "CIBERSEGURIDAD APLICADA EN FORMACIÓN DIGITAL", es el punto de equilibrio donde estos tres dominios convergen. Es el estado óptimo donde la tecnología es robusta, la información está gestionada y los usuarios están capacitados, creando una plataforma de aprendizaje verdaderamente confiable.

Asimismo, la creación de espacios de reflexión y diálogo sobre la protección de la información contribuye a la construcción de una cultura de seguridad digital. La articulación entre los diferentes componentes del modelo y su adaptación a las necesidades institucionales resulta fundamental para garantizar su efectividad y sostenibilidad en el tiempo.

7.6 Proceso de implementación del modelo

El proceso de implementación del modelo se concibe como una secuencia sistemática y dinámica que inicia con un diagnóstico del estado actual de la ciberseguridad en la institución, permitiendo identificar fortalezas, debilidades y áreas de mejora. A partir de este diagnóstico, se desarrolla una fase de planificación en la que se definen las estrategias, recursos y acciones necesarias para la implementación del modelo.

La fase de ejecución implica la puesta en práctica de las estrategias diseñadas, integrando la ciberseguridad en los procesos pedagógicos y tecnológicos. Posteriormente, se realiza un seguimiento continuo que permite monitorear el cumplimiento de las acciones y evaluar su impacto en la protección de la información y el uso de las aplicaciones.

Finalmente, la evaluación del modelo permite medir los resultados obtenidos y realizar ajustes que favorezcan su mejora continua, garantizando su adaptación a los cambios en la plataforma digital y a la evolución de las amenazas cibernéticas.

Este proceso no debe visualizarse como una estructura rígida, sino como un ciclo iterativo de gestión del riesgo y mejora continua. En la figura 6 se esquematiza el flujo lógico de implementación, mostrando la secuencialidad y retroalimentación entre las fases de diagnóstico, planificación, ejecución, seguimiento, evaluación y la consecuente mejora del sistema.

Figura 6. Flujo del proceso de implementación del modelo

La figura 6 aborda la dimensión temporal y pragmática del modelo, respondiendo a la pregunta: ¿Cómo llevamos esto a la realidad?

Este diagrama de flujo circular rompe con la visión lineal de la implementación, proponiendo en su lugar un ciclo de vida iterativo basado en la mejora continua.

El proceso comienza, obligatoriamente, con un Diagnóstico (1) honesto de la situación actual, que nos lleva a una Planificación (2) estratégica. La fase de Ejecución (3) es donde los componentes pedagógicos y tecnológicos entran en acción. Sin embargo, el modelo no se detiene ahí. Las fases de Seguimiento (4) y Evaluación (5) son críticas para medir el impacto real y detectar desviaciones.

La flecha que cierra el ciclo hacia la Mejora Continua (6) y reabre el Diagnóstico es el motor de la propuesta. En ciberseguridad, lo que hoy es seguro, mañana puede no serlo. Este flujo cíclico garantiza que la institución educativa se mantenga en un estado de adaptación constante, aprendiendo de sus propios procesos y madurando su postura de seguridad con cada vuelta del ciclo.

7.7 Evaluación del modelo de protección digital en los procesos de formación

La evaluación del modelo constituye un elemento esencial para determinar su efectividad y sostenibilidad, permitiendo identificar los avances alcanzados y las áreas que requieren fortalecimiento. Este proceso debe considerar aspectos relacionados con el nivel de conocimiento en ciberseguridad, las prácticas de

protección de la información, el uso responsable de las plataformas digitales y la incidencia de eventos de seguridad.

Asimismo, la percepción de los usuarios sobre la confiabilidad de las plataformas digitales y la calidad de los procesos educativos representa un indicador relevante para valorar el impacto del modelo. La evaluación continua permite generar información que contribuye a la toma de decisiones y a la mejora permanente de las estrategias de ciberseguridad aplicada, incorporando indicadores cuantitativos y cualitativos que permitan medir la madurez de la ciberseguridad institucional.

7.8 Impacto esperado del modelo

La implementación del modelo de protección digital en los procesos de formación tiene el potencial de generar un impacto significativo en la calidad y seguridad de las plataformas educativas digitales. Se espera que contribuya a la reducción de incidentes de seguridad, al fortalecimiento de la cultura digital y al incremento de la confianza en el uso de las tecnologías para el aprendizaje.

Asimismo, el modelo favorece el desarrollo de competencias digitales responsables, promoviendo la formación de usuarios capaces de gestionar la información de manera segura y de interactuar en la plataforma digital con criterio ético. La mejora en la protección de las aplicaciones y en la gestión de la información digital se traduce en plataformas de aprendizaje más confiables, resilientes y sostenibles.

A modo de síntesis visual de los beneficios derivados de la propuesta, la figura 7 expone la cadena de valor y el impacto esperado del modelo. Se ilustra cómo la correcta articulación de los componentes transversales conduce a resultados tangibles como el fortalecimiento de la cultura digital, la reducción efectiva de riesgos, y el incremento de la confianza y calidad en las plataformas de educación virtual.

Figura 7. Impacto y resultados esperados de la implementación.

La figura 7 funciona como el cierre visual y la síntesis de la promesa de valor del modelo. Utilizando una estructura piramidal ascendente, el diagrama ilustra la cadena de valor que se genera tras la implementación.

La base de la pirámide es el "MODELO OPERATIVO". Sin esta cimentación (la articulación de los 4 componentes), no hay impacto posible. Al aplicar el modelo, el primer nivel de resultados tangibles es de carácter técnico-operativo: la Reducción de Incidentes y la Protección de Datos.

Al sostener estos resultados en el tiempo, accedemos al siguiente nivel, que es un cambio de paradigma: el Fortalecimiento de la Cultura Digital y el desarrollo de competencias reales en los actores educativos.

Finalmente, la cima de la pirámide representa el impacto estratégico y la aspiración última de la propuesta: lograr un estado de CONFIANZA Y CALIDAD EDUCATIVA SUSTENIBLE. Esta pirámide demuestra que la ciberseguridad aplicada no es un gasto o una barrera, sino una inversión directa en la calidad y la reputación de la institución educativa en la era digital.

7.9 Consideraciones finales

El modelo de protección digital en los procesos de formación propuesto en este capítulo representa una respuesta integral a los desafíos de la ciberseguridad en el ámbito educativo, articulando principios, componentes y estrategias en un marco coherente que permite fortalecer la protección de aplicaciones y la gestión segura de la información digital.

Su enfoque multidimensional integra aspectos pedagógicos, tecnológicos, organizacionales y culturales, reconociendo que la ciberseguridad aplicada es un proceso complejo que requiere la participación de todos los actores del sistema educativo. Esta propuesta constituye una herramienta práctica y adaptable que puede ser implementada en diversos contextos institucionales, contribuyendo a la construcción de plataformas de formación seguros, confiables y orientados al desarrollo de competencias digitales en la era de la información, consolidándose como una propuesta replicable y escalable en distintos contextos educativos.

Como líneas futuras de investigación, se recomienda profundizar en la aplicación del modelo propuesto en diferentes contextos educativos, así como explorar el impacto de nuevas tecnologías emergentes, como la inteligencia artificial, en la ciberseguridad. Asimismo, se sugiere desarrollar estudios comparativos que permitan validar y ampliar los hallazgos obtenidos en esta investigación.

.

Referencias

Abomhara, M., & Køien, G. M. (2022). Cyber security and the internet of things: Vulnerabilities, threats, intruders and attacks. Journal of Cybersecurity and Privacy, 2(1), 1–18. https://doi.org/10.3390/jcp2010001

Achuthan, K., Shankar, B., Francis, S. P. J., & Bose, J. C. (2024). Educational trends in artificial intelligence and cybersecurity. Frontiers in Big Data, 7, 1497535. https://doi.org/10.3389/fdata.2024.1497535

Ahmed, A., Rehman, S. U., & Ahmed, S. (2024). Online cybersecurity education review. Frontiers in Computer Science, 6, 1499490. https://doi.org/10.3389/fcomp.2024.1499490

Alshar'e, M. (2023). Cyber security framework selection: Comparison of NIST and ISO27001. Applied Computing Journal, 3(1), 245–255. https://journal.unwira.ac.id/index.php/ACJ/article/view/2153

Alzahrani, A., & Alghamdi, A. (2022). Cybersecurity awareness and practices in educational institutions. International Journal of Advanced Computer Science and Applications, 13(6), 1–10. https://doi.org/10.14569/IJACSA.2022.0130601

Amankwa, E. (2021). Relevance of cybersecurity education at pedagogy levels in schools. Journal of Information Security, 12(3), 233–249. https://doi.org/10.4236/jis.2021.124013

Angelini, M., Bonomi, S., & Palma, A. (2022). A methodology to support automatic cyber risk assessment review. arXiv. https://arxiv.org/abs/2207.03269

Bada, M., & Nurse, J. R. C. (2023). Cybersecurity awareness. Frontiers in Digital Health, 5, 1242264. https://doi.org/10.3389/fdgth.2023.1242264

Becerril-Arreola, R., & Sosa-Sosa, V. J. (2023). Cybersecurity risk management in higher education institutions. IEEE Access, 11, 45678–45689. https://doi.org/10.1109/ACCESS.2023.3267890

Bongiovanni, I. (2022). Cybersecurity culture: A systematic literature review. Computers & Security, 112, 102519. https://doi.org/10.1016/j.cose.2021.102519

Bowen, D., Jaurez, J., Jones, N., Reid, W., & Simpson, C. (2022). Cybersecurity educational resources for K-12. Journal of Cybersecurity Education, Research & Practice, 2022(1), Article 4. https://digitalcommons.kennesaw.edu/jcerp/vol2022/iss1/4

Camacho, J., & Fernández-Alemán, J. L. (2022). Security and privacy in e-learning systems: A systematic mapping study. Computer Standards & Interfaces, 80, 103585. https://doi.org/10.1016/j.csi.2021.103585

Da Veiga, A., & Martins, N. (2023). Improving the information security culture through training and awareness. Information & Computer Security, 31(2), 256–273. https://doi.org/10.1108/ICS-05-2022-0072

Dlamini, M. T., Eloff, J. H. P., & Eloff, M. M. (2022). Information security: The moving target. Computers & Security, 112, 102508. https://doi.org/10.1016/j.cose.2021.102508

European Union Agency for Cybersecurity (ENISA). (2022). Cybersecurity education initiatives. https://www.enisa.europa.eu

Febrilian Tanjung, D., Nurhayati, O. D., & Wibowo, A. (2024). Design information security in electronic-based government systems using NIST CSF 2.0 and ISO/IEC 27001:2022. International Journal of Innovative Science and Research Technology, 9(6), 1432–1439. https://doi.org/10.5281/zenodo.12519126

Furnell, S., & Shah, J. (2022). Home working and cyber security—An outbreak of unpreparedness? Computer Fraud & Security, 2022(1), 6–12. https://doi.org/10.1016/S1361-3723(21)00002-2

García-Peñalvo, F. J., García-Holgado, A., Vázquez-Ingelmo, A., & Conde, M. Á. (2021). Digital transformation in education. Education in the Knowledge Society, 22, Article 25456. https://doi.org/10.14201/eks.25456

González-Granadillo, G., Menesidou, S. A., Papamartzivanos, D., Romeu, R., & Nifakos, S. (2022). Risk-based cybersecurity framework for digital environments. Future Generation Computer Systems, 125, 1–15. https://doi.org/10.1016/j.future.2021.06.012

Hashim, H., & Hassan, R. (2023). Cybersecurity readiness in educational institutions: A conceptual framework. Education and Information Technologies, 28, 14567–14589. https://doi.org/10.1007/s10639-023-11745-2

Hu, Q. (2024). Research on cybersecurity education and student mindset. Applied Mathematics and Nonlinear Sciences, 9(1). https://doi.org/10.2478/amns-2024-1504

International Organization for Standardization (ISO/IEC). (2022a). ISO/IEC 27001: Information security management systems. https://www.iso.org/isoiec-27001-information-security.html

International Organization for Standardization (ISO/IEC). (2022b). ISO/IEC 27002: Information security controls. https://www.iso.org/standard/75652.html

Irawan, H., Muhammad, A. H., & Nasiri, A. (2024). Design of cybersecurity maturity assessment framework using NIST CSF v1.1 and CIS Controls v8. Journal of Informatics and Software Engineering, 5(1), 1–10. https://doi.org/10.52696/jise.v5i1.233

Jang-Jaccard, J., & Nepal, S. (2022). A survey of emerging threats in cybersecurity. Journal of Computer and System Sciences, 80(5), 973–993. https://doi.org/10.1016/j.jcss.2014.02.005

Kamal, M., Sulieman, H., & Al-Ahmadi, S. (2023). Cybersecurity governance in higher education institutions. IEEE Access, 11, 99876–99890. https://doi.org/10.1109/ACCESS.2023.3298765

Kennison, S., & Chan-Tin, E. (2020). Cybersecurity behavior. Frontiers in Psychology, 11, 546546. https://doi.org/10.3389/fpsyg.2020.546546

Kour, R., Jigar, K., & Gupta, S. K. (2024). Cybersecurity in Industry 5.0. Frontiers in Computer Science, 6, 1434436. https://doi.org/10.3389/fcomp.2024.1434436

Kumar, R., & Somani, G. (2022). Social engineering attacks in cybersecurity: A systematic review. Computer Communications, 179, 158–179. https://doi.org/10.1016/j.comcom.2021.09.024

Lallie, H. S., Shepherd, L. A., Wong, J. R., Andriotis, P., Prajapati, A., Nurse, J. R. C., Chang, V., Debattista, K., Rostami, S., Sugden, S., Davies, N., & Rostami, A. (2023). Cybersecurity in the COVID-19 era: A review. Computers & Security, 117, 102735. https://doi.org/10.1016/j.cose.2022.102735

Li, J., Wang, F., & Jones, A. (2025). Cybersecurity education incentives. arXiv. https://arxiv.org/abs/2508.01520

Lokare, A., Bankar, S., & Mhaske, P. (2025). Integrating cybersecurity frameworks into IT security. arXiv. https://arxiv.org/abs/2502.00651

Mantha, B., & Garcia, M. A. (2021). Cybersecurity in construction. Frontiers in Built Environment, 7, 612668. https://doi.org/10.3389/fbuil.2021.612668

Marín, V. I., & Cabero-Almenara, J. (2022). Digital competence in education: A systematic review. Education Sciences, 12(3), 1–15. https://doi.org/10.3390/educsci12030172

Mishra, S., Thakur, S., & Singh, S. (2023). Cybersecurity challenges in online learning platforms. Sustainability, 15(4), 3456. https://doi.org/10.3390/su15043456

Murad, H., & Khan, S. (2025). Cybersecurity communication attitudes. Frontiers in Communication, 10, 1552520. https://doi.org/10.3389/fcomm.2025.1552520

National Institute of Standards and Technology (NIST). (2018a). Framework for improving critical infrastructure cybersecurity (Version 1.1). U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.04162018

National Institute of Standards and Technology (NIST). (2018b). NIST Cybersecurity Framework. https://www.nist.gov/cyberframework

National Institute of Standards and Technology (NIST). (2020). NIST SP 800-53 Rev. 5: Security and privacy controls. U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-53r5

Nguyen, T. T., Malawu, M., & Malawu, B. (2022). Cybersecurity education in universities: A global perspective. Education and Information Technologies, 27, 109–130. https://doi.org/10.1007/s10639-021-10783-y

Nour Eldin, A., Sellami, M., & Gaaloul, W. (2026). Exploring semantic labeling strategies for third-party cybersecurity risk assessment questionnaires. arXiv. https://arxiv.org/abs/2602.10149

Open Web Application Security Project (OWASP). (2021). OWASP Top 10: The ten most critical web application security risks. https://owasp.org/www-project-top-ten/

Open Web Application Security Project (OWASP). (2023). OWASP Application Security Verification Standard (ASVS). https://owasp.org/www-project-application-security-verification-standard/

Rahman, R., Ananta, A., & Surianti, B. (2024). Analisis perbandingan framework keamanan jaringan (NIST CSF, CIS Controls, ISO 27001). Technology Sciences Insights Journal, 1(1), 12–25. https://journal.tsij.or.id/index.php/TSIJ/article/view/15

Rattanapong, P., & Brown, L. (2025). Cybersecurity investment. Frontiers in Risk Management, 2, 1594554. https://doi.org/10.3389/frcmn.2025.1594554

Sabillon, R., Serra-Ruiz, J., & Cavaller, V. (2022). Cybersecurity frameworks evaluation and improvement. Computer Standards & Interfaces, 81, 103600. https://doi.org/10.1016/j.csi.2022.103600

Sharma, R., & Dash, S. (2023). Cybersecurity and data privacy in digital education systems. Journal of Information Security and Applications, 70, 103315. https://doi.org/10.1016/j.jisa.2022.103315

Sulistyowati, D., Handayani, F., & Suryanto, Y. (2020). Comparative analysis of cybersecurity maturity assessment methodology. JOIV: International Journal on Informatics Visualization, 4(4), 225–230. http://joiv.org/index.php/joiv/article/view/482

Vulpe, S., & Smith, J. D. (2024). AI and cybersecurity society. Frontiers in Computer Science, 6, 1462250. https://doi.org/10.3389/fcomp.2024.1462250

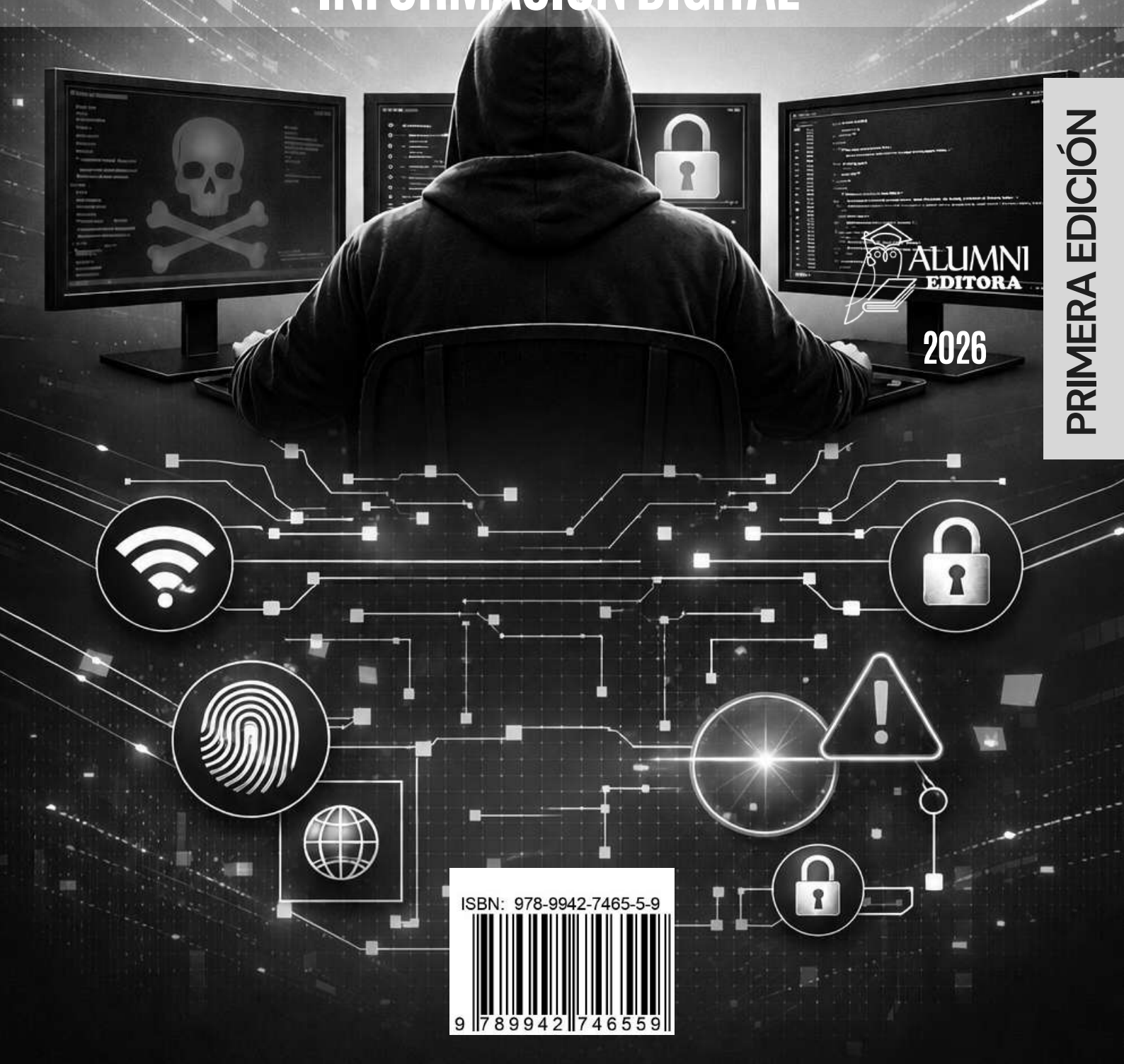
Wojak, G., Janowski, M., & Kopiński, M. (2025). Data protection and corporate reputation management in the digital era. arXiv. https://arxiv.org/abs/2512.15794

Yadav, T., & Rao, A. M. (2023). Technical aspects of cyber security: A systematic mapping study. Journal of Systems and Software, 196, 111552. https://doi.org/10.1016/j.jss.2022.111552

CIBERSEGURIDAD

APLICADA

ESTRATEGIAS PARA LA PROTECCIÓN DE APLICACIONES Y GESTIÓN SEGURA DE LA INFORMACIÓN DIGITAL



ALUMNI EDITORA

2026

PRIMERA EDICIÓN

ISBN: 978-9942-7465-5-9