CIBERSEGURIDAD PARA DOCENTES

Guía Práctica para la Protección del **Aula Digital**

ISBN: 978-9942-580-57-3

CRÉDITOS

Ciberseguridad para docentes: Guía práctica para la protección del aula digital

Autores

Luis Andrés Hidalgo Bonifaz
andres.hidalgo@upec.edu.ec
https://orcid.org/0000-0003-3635-5877
Universidad Politécnica Estatal del Carchi

Andrea Viviana Razo Cifuentes
arazo.istt@gmail.com
https://orcid.org/0000-0002-1533-2054
Instituto Superior Tecnológico Tungurahua

Darwin Danilo Cañar Yumbolema
dd.canar@uta.edu.ec
https://orcid.org/0000-0002-7040-0785
Universidad Técnica de Ambato

Hernán Patricio Chipantiza Quinatoa
hp.chipantiza@uta.edu.ec
https://orcid.org/0009-0001-7462-0902
Universidad Técnica de Ambato

Gary Daniel Anzules Jordán
Correo: gdanzulesj@ube.com.ec
https://orcid.org/0009-0009-5609-517X
Institución: Universidad Bolivariana del Ecuador

INDEXACIÓN

Dirección y Coordinación Editorial: Sara Díaz Villacís

Revisión de contenido Christian Armendáriz PhD

Revisión pedagógica: Fabrizzio Andrade PhD (c)

Maquetación y Diseño de portada: *Sara Díaz V*

Libro bajo revisión técnica y didáctica de pares

Guayaquil - Ecuador

Abril del 2026

Descarga:

https://liveworkingeditorial.com/product/978-9942-580-57-3/

Enlace del DOI:

https://doi.org/10.63792/978-9942-580-57-3

CÁMARA ECUATORIANA DEL LIBRO

Certificado de autenticidad

ISBN: 978-9942-580-57-3

Google Play Books

ÍNDICE GENERAL

PRÓLOGO

La educación contemporánea se encuentra inmersa en un proceso de transformación sin precedentes, impulsado por la digitalización de los entornos de enseñanza y aprendizaje. La incorporación de tecnologías digitales en el aula ha permitido ampliar el acceso al conocimiento, diversificar las estrategias pedagógicas y fomentar nuevas formas de interacción entre docentes y estudiantes. Sin embargo, este avance tecnológico también ha introducido una serie de desafíos que requieren ser abordados con responsabilidad y rigor, entre los cuales la ciberseguridad ocupa un lugar central.

En la actualidad, el aula ya no se limita a un espacio físico, sino que se extiende hacia entornos virtuales donde se gestionan grandes volúmenes de información personal, académica y social. Esta nueva realidad implica que docentes y estudiantes interactúan constantemente con plataformas digitales, aplicaciones y sistemas que, si bien facilitan

el aprendizaje, también incrementan la exposición a riesgos asociados a la seguridad de la información. En este contexto, la ciberseguridad se convierte en un elemento fundamental para garantizar la protección de los datos y la integridad de los procesos educativos.

La relevancia de la ciberseguridad en el ámbito educativo radica en la vulnerabilidad inherente de los entornos digitales, donde la información puede ser objeto de ataques, manipulaciones o usos indebidos. Los estudiantes, especialmente en etapas formativas, constituyen un grupo particularmente sensible frente a estas amenazas, ya que muchas veces carecen de las competencias necesarias para identificar riesgos y adoptar medidas de protección. Esta situación evidencia la necesidad de integrar la ciberseguridad como un componente esencial en la formación educativa, promoviendo el desarrollo de habilidades que permitan a los usuarios desenvolverse de manera segura en el entorno digital (Herrera et al., 2025).

En este escenario, el docente asume un rol protagónico como mediador entre la tecnología y el aprendizaje, convirtiéndose en un agente clave para la prevención de riesgos digitales. Su función no se limita a la enseñanza de contenidos académicos, sino que se extiende hacia la formación de ciudadanos digitales responsables, capaces de utilizar la tecnología de manera ética y segura. Este nuevo rol exige el desarrollo de competencias digitales avanzadas, así como una comprensión profunda de los riesgos asociados al uso de herramientas tecnológicas (Guillén, 2025).

La presente obra surge como una respuesta a la necesidad de proporcionar a los docentes una guía práctica que les permita enfrentar los desafíos de la ciberseguridad en el aula digital. A través de un enfoque integral, este libro aborda los fundamentos de la ciberseguridad, la protección de datos, la seguridad en herramientas digitales y la implementación de estrategias y protocolos que permitan garantizar la seguridad de los entornos

educativos. Este enfoque no solo se centra en los aspectos técnicos, sino que también considera las dimensiones pedagógicas y éticas que configuran la práctica educativa en la era digital.

Uno de los aportes más relevantes de este libro es su capacidad para integrar el conocimiento teórico con la práctica docente, ofreciendo herramientas concretas que pueden ser aplicadas en el aula. En este sentido, la obra se orienta a la formación de docentes capaces de identificar riesgos, implementar medidas de protección y promover una cultura de seguridad en el uso de la tecnología. Este enfoque resulta especialmente pertinente en un contexto donde la digitalización de la educación avanza a un ritmo acelerado, generando nuevas oportunidades, pero también nuevos desafíos.

La protección de datos constituye uno de los ejes centrales de la ciberseguridad en educación, ya que los entornos digitales implican la gestión de información sensible que debe ser resguardada de manera adecuada. La filtración de datos, el acceso no

autorizado y el uso indebido de la información representan riesgos que pueden afectar tanto a los estudiantes como a las instituciones educativas. En este sentido, la implementación de políticas de protección de datos y la adopción de buenas prácticas en el manejo de la información se convierten en elementos fundamentales para garantizar la seguridad de los sistemas educativos (Orellana & Moran, 2025).

Asimismo, la seguridad en herramientas digitales educativas constituye un aspecto clave para la protección de los entornos de aprendizaje. Las plataformas educativas, las aplicaciones de comunicación y las herramientas de inteligencia artificial deben ser utilizadas de manera segura, considerando las posibles vulnerabilidades que pueden presentar. La configuración adecuada de estas herramientas, la gestión de accesos y la actualización constante de los sistemas son medidas esenciales para reducir los riesgos asociados a su uso (Ramos et al., 2025).

La obra también destaca la importancia de la formación en ciberseguridad como un elemento transversal en la educación, promoviendo el desarrollo de competencias digitales que permitan a los estudiantes actuar de manera responsable en entornos virtuales. Esta formación no solo contribuye a la prevención de riesgos, sino que también fortalece la ciudadanía digital, fomentando valores como la ética, la responsabilidad y el respeto en el uso de la tecnología (Solano et al., 2025).

En este sentido, la educación en ciberseguridad se presenta como una herramienta clave para enfrentar los desafíos de la sociedad digital, donde la información se ha convertido en uno de los recursos más valiosos. La capacidad de proteger esta información y de utilizarla de manera responsable constituye una competencia fundamental para los ciudadanos del siglo XXI, lo que resalta la importancia de integrar la ciberseguridad en el proceso educativo (Gonzalez et al., 2025).

Otro aspecto relevante abordado en este libro es la necesidad de construir una cultura de ciberseguridad en las instituciones educativas, que permita promover prácticas seguras y fortalecer la confianza en el uso de la tecnología. Esta cultura se construye a partir de la participación activa de todos los actores educativos, incluyendo docentes, estudiantes y directivos, quienes deben asumir la seguridad digital como una responsabilidad compartida (Casa, 2025).

La implementación de estrategias de ciberseguridad docente constituye un elemento clave para garantizar la protección de los entornos educativos. Estas estrategias incluyen la formación en competencias digitales, la implementación de protocolos de seguridad y la gestión de incidentes, lo que permite prevenir riesgos y actuar de manera oportuna ante posibles amenazas. Este enfoque integral contribuye a la construcción de entornos de aprendizaje seguros y sostenibles (Vega, 2026).

Finalmente, este libro se presenta como una herramienta de reflexión y acción para los docentes, invitándolos a repensar su rol en la educación digital y a asumir la ciberseguridad como un componente esencial de su práctica profesional. La protección del aula digital no es solo una cuestión técnica, sino un compromiso ético que implica garantizar la seguridad y el bienestar de los estudiantes en un entorno cada vez más complejo.

En un mundo donde la tecnología avanza a un ritmo vertiginoso, la educación debe adaptarse a los cambios y preparar a los estudiantes para enfrentar los desafíos del entorno digital. La ciberseguridad se configura como un elemento clave en este proceso, permitiendo garantizar la protección de la información y la integridad de los procesos educativos. Este libro constituye un aporte significativo en este ámbito, ofreciendo herramientas y conocimientos que contribuyen a la construcción de una educación más segura, responsable y acorde a las demandas del siglo XXI.

INTRODUCCIÓN

La acelerada transformación digital de la educación en el siglo XXI ha redefinido los escenarios de enseñanza y aprendizaje, generando nuevas oportunidades para el acceso al conocimiento, la interacción pedagógica y la innovación didáctica. La incorporación de herramientas tecnológicas, plataformas virtuales y sistemas inteligentes ha permitido ampliar las posibilidades educativas más allá del aula tradicional, consolidando entornos digitales dinámicos, flexibles y centrados en el estudiante. Sin embargo, este proceso de digitalización también ha traído consigo una creciente exposición a riesgos asociados a la seguridad de la información, la privacidad de los usuarios y la integridad de los sistemas educativos, lo que posiciona a la ciberseguridad como un eje fundamental en la educación contemporánea.

En este contexto, la ciberseguridad en el ámbito educativo no puede ser concebida únicamente como

una dimensión técnica, sino como un componente integral del proceso formativo que involucra aspectos pedagógicos, éticos y sociales. La protección de los entornos digitales educativos requiere la articulación de estrategias que permitan prevenir amenazas, gestionar riesgos y garantizar el uso seguro de la tecnología por parte de docentes y estudiantes. La ausencia de estas estrategias puede derivar en situaciones de vulnerabilidad que afectan no solo la información académica, sino también el bienestar de los actores educativos (Ramos et al., 2025).

Los antecedentes de la ciberseguridad en educación evidencian una evolución progresiva desde enfoques centrados en la protección de sistemas informáticos hacia perspectivas más amplias que incluyen la formación de competencias digitales seguras. En un inicio, la seguridad digital en instituciones educativas se limitaba a la implementación de medidas técnicas, como antivirus y sistemas de protección de redes. No obstante, el incremento de amenazas como el phishing, el

malware y el ciberacoso ha demostrado que estas medidas son insuficientes si no se acompañan de procesos educativos orientados a la prevención y al uso responsable de la tecnología (Montilla & Omar, 2025).

En la actualidad, la creciente integración de plataformas digitales en el aula ha generado la necesidad de repensar la seguridad desde un enfoque educativo, donde el docente desempeña un papel clave en la formación de estudiantes capaces de desenvolverse de manera segura en entornos virtuales. Esta evolución ha sido impulsada por el reconocimiento de que el factor humano constituye uno de los principales puntos de vulnerabilidad en los sistemas de ciberseguridad, lo que hace indispensable fortalecer las competencias digitales de los usuarios (Herrera et al., 2025).

La justificación de esta obra se sustenta en la necesidad de proporcionar a los docentes herramientas conceptuales y prácticas que les permitan enfrentar los desafíos de la ciberseguridad

en el aula digital. En un contexto donde la tecnología se ha convertido en un elemento central del proceso educativo, resulta imprescindible que los docentes desarrollen habilidades para identificar riesgos, implementar medidas de protección y promover una cultura de seguridad en el uso de la tecnología. Este libro busca contribuir a este propósito, ofreciendo una guía que integra conocimientos teóricos y estrategias aplicadas para la protección del entorno educativo digital.

Desde una perspectiva teórica, la obra aporta a la comprensión de la ciberseguridad como un fenómeno multidimensional que involucra la interacción entre tecnología, educación y sociedad. Este enfoque permite analizar los riesgos digitales desde una perspectiva integral, considerando no solo los aspectos técnicos, sino también las implicaciones pedagógicas y éticas del uso de la tecnología en el aula. Asimismo, la obra contribuye a la consolidación de la ciberseguridad como un campo de estudio relevante en la educación, promoviendo el desarrollo

de nuevas líneas de investigación en este ámbito (Bustos & Lizardo, 2025).

En el ámbito práctico, el libro ofrece estrategias y herramientas que pueden ser implementadas por los docentes en su práctica cotidiana, facilitando la gestión de la seguridad en el aula digital. Estas estrategias incluyen la configuración segura de herramientas digitales, la implementación de protocolos de seguridad y la formación de los estudiantes en el uso responsable de la tecnología. De esta manera, la obra busca contribuir a la mejora de la calidad educativa, garantizando entornos de aprendizaje más seguros y confiables.

El objetivo general de este libro es analizar la ciberseguridad en el contexto educativo y proponer estrategias prácticas que permitan a los docentes proteger el aula digital y promover el uso seguro de las herramientas tecnológicas. A partir de este objetivo general, se plantean como objetivos específicos: comprender los fundamentos de la ciberseguridad en el ámbito educativo; identificar los

principales riesgos asociados al uso de tecnologías digitales en el aula; analizar las medidas de protección de datos y privacidad en entornos virtuales; y diseñar estrategias y protocolos que permitan garantizar la seguridad de los sistemas educativos digitales.

El objeto de estudio de esta obra es la ciberseguridad en el aula digital, entendida como el conjunto de prácticas, políticas y estrategias orientadas a la protección de los entornos educativos digitales frente a amenazas y riesgos asociados al uso de la tecnología. Este objeto de estudio se aborda desde una perspectiva interdisciplinaria que integra conocimientos de educación, tecnología y seguridad de la información, lo que permite comprender la complejidad del fenómeno y proponer soluciones integrales.

Por su parte, el sujeto de estudio está constituido por los docentes, quienes desempeñan un papel fundamental en la gestión de la ciberseguridad en el aula. La elección de este sujeto responde a la

necesidad de fortalecer las competencias digitales del profesorado, considerando su influencia en la formación de los estudiantes y en la implementación de estrategias de seguridad. Asimismo, se reconoce la participación indirecta de los estudiantes como actores clave en el proceso educativo, quienes también deben desarrollar habilidades para el uso seguro de la tecnología.

La estructura del libro ha sido diseñada para abordar de manera progresiva los diferentes aspectos de la ciberseguridad en el ámbito educativo. En el primer capítulo se presentan los fundamentos de la ciberseguridad en el entorno educativo, analizando los principales riesgos y amenazas digitales. El segundo capítulo se centra en la protección de datos y la privacidad en el aula digital, abordando la gestión de la información y las medidas de seguridad necesarias para su protección. El tercer capítulo analiza la seguridad en herramientas digitales educativas, identificando vulnerabilidades y proponiendo estrategias para su mitigación.

Finalmente, el cuarto capítulo aborda las estrategias y protocolos de ciberseguridad docente, ofreciendo un enfoque práctico para la gestión de la seguridad en el aula.

La relevancia de esta obra radica en su contribución a la formación de docentes preparados para enfrentar los desafíos de la educación digital, promoviendo el desarrollo de competencias que permitan garantizar la seguridad de los entornos educativos. En un mundo donde la tecnología desempeña un papel cada vez más importante, la ciberseguridad se convierte en un elemento esencial para la construcción de una educación de calidad, capaz de responder a las demandas de la sociedad contemporánea.

En síntesis, la presente obra se configura como una guía integral para la protección del aula digital, orientada a la formación de docentes comprometidos con la seguridad y el uso responsable de la tecnología. A través de un enfoque teórico-práctico, el libro busca contribuir a la construcción de entornos

educativos seguros, inclusivos y sostenibles, donde la tecnología sea utilizada como una herramienta para el aprendizaje y no como un factor de riesgo. De esta manera, se promueve una educación que no solo forme en conocimientos, sino también en valores y competencias necesarias para desenvolverse en la sociedad digital del siglo XXI (Vega, 2026).

CAPÍTULO 1

FUNDAMENTOS DE CIBERSEGURIDAD EN EL ENTORNO EDUCATIVO

La ciberseguridad en el ámbito educativo es esencial para proteger la información, los entornos digitales y a todos los actores que participan en el proceso de enseñanza y aprendizaje. Comprender sus fundamentos permite a los docentes promover un uso seguro, responsable y ético de la tecnología en el aula digital.

1.1 ¿QUÉ ES LA CIBERSEGURIDAD?

La ciberseguridad se define como el conjunto de prácticas, tecnologías y procesos diseñados para proteger sistemas, redes, dispositivos y datos de accesos no autorizados, ataques, daños o usos indebidos.

En el contexto educativo, su finalidad es garantizar la confidencialidad, integridad y disponibilidad de la información y los recursos digitales utilizados en la enseñanza.

Confidencialidad
Proteger la información para que solo sea accesible a quienes están autorizados.

Integridad
Asegurar que la información no sea alterada de manera no autorizada.

Disponibilidad
Garantizar que la información y los sistemas estén disponibles cuando sean necesarios.

Fuente: Adaptado de Vega (2026).

1.2 IMPORTANCIA DE LA CIBERSEGURIDAD EN EDUCACIÓN

- Protege a los estudiantes y docentes frente a amenazas digitales que pueden afectar su seguridad y privacidad.
- Salvaguarda la información académica, administrativa y personal de la comunidad educativa.
- Garantiza la continuidad de los procesos educativos evitando interrupciones causadas por ataques o fallos de seguridad.
- Fomenta una cultura de uso responsable, ético y seguro de la tecnología en el entorno educativo.

Fuente: Casa (2025); Ramos et al. (2025).

1.3 COMPONENTES DE LA CIBERSEGURIDAD

Personas
Los usuarios son el primer factor de seguridad. Su formación y conciencia son fundamentales.

Procesos
Políticas, normas y procedimientos que orientan el uso seguro de la tecnología.

Tecnología
Herramientas y sistemas diseñados para prevenir, detectar y responder a amenazas.

Información
Datos y contenidos que deben ser protegidos para garantizar su confidencialidad, integridad y disponibilidad.

Fuente: Adaptado de Herrera et al. (2025).

1.4 PRINCIPIOS DE LA CIBERSEGURIDAD EDUCATIVA

- **Prevención:** anticiparse a los riesgos y aplicar medidas para evitar incidentes.
- **Detección:** identificar amenazas o comportamientos anómalos de manera oportuna.
- **Respuesta:** actuar rápidamente ante incidentes para minimizar su impacto.
- **Recuperación:** restaurar los sistemas y aprender de los incidentes para mejorar continuamente.
- **Responsabilidad compartida:** todos los actores educativos deben contribuir a la seguridad digital.

Fuente: Solano et al. (2025); Gonzalez et al. (2025).

1.5 RIESGOS Y AMENAZAS COMUNES EN EL ENTORNO EDUCATIVO

PHISHING
Intentos de engañar a los usuarios para que revelen información confidencial a través de correos o mensajes fraudulentos.

MALWARE
Software malicioso diseñado para dañar sistemas, robar información o interrumpir servicios.

RANSOMWARE
Ataques que bloquean el acceso a la información y exigen un pago para recuperarla.

ACCESO NO AUTORIZADO
Ingreso indebido a sistemas o cuentas para obtener, modificar o eliminar información.

CIBERACOSO
Uso de medios digitales para intimidar, humillar o afectar emocionalmente a estudiantes o docentes.

PÉRDIDA DE INFORMACIÓN
Eliminación, fuga o divulgación accidental de datos por descuido o falta de protección.

REFLEXIÓN DOCENTE ¿Qué prácticas de seguridad digital implemento en mi aula? ¿Cómo puedo fortalecer la conciencia de mis estudiantes frente a los riesgos digitales?

Fuente general de la unidad: Montilla & Omar (2025); Bustos & Lizardo (2025); Casa (2025); Vega (2026).

CAPÍTULO 1: Fundamentos de la ciberseguridad en el entorno educativo

1.1 Introducción a la ciberseguridad en educación

En la actualidad, la digitalización de los entornos educativos ha generado una transformación significativa en los procesos de enseñanza y aprendizaje, permitiendo el acceso a recursos tecnológicos, plataformas virtuales y herramientas digitales que potencian la experiencia educativa. Sin embargo, este avance también ha traído consigo nuevos riesgos asociados a la seguridad de la información, la privacidad de los datos y la exposición de estudiantes y docentes a amenazas digitales. En este contexto, la ciberseguridad se posiciona como un componente fundamental para garantizar la protección de los entornos educativos digitales y promover un uso seguro de la tecnología en el aula.

La ciberseguridad en educación no debe entenderse únicamente como un conjunto de

medidas técnicas orientadas a proteger sistemas informáticos, sino como un enfoque integral que involucra aspectos pedagógicos, sociales y éticos. En este sentido, la formación en ciberseguridad se convierte en una necesidad para los docentes, quienes desempeñan un papel clave en la prevención de riesgos digitales y en la promoción de una cultura de seguridad en el uso de las tecnologías (Herrera et al., 2025).

El crecimiento del uso de plataformas educativas, redes sociales y herramientas digitales ha incrementado la exposición de los estudiantes a riesgos como el ciberacoso, el robo de información y la manipulación de datos. Estas amenazas no solo afectan la seguridad de la información, sino también el bienestar emocional y social de los estudiantes, lo que evidencia la necesidad de integrar la ciberseguridad como un eje transversal en los procesos educativos (Casa, 2025).

1.2 Conceptos fundamentales de ciberseguridad

La ciberseguridad puede definirse como el conjunto de prácticas, políticas y tecnologías destinadas a proteger sistemas, redes y datos frente a accesos no autorizados, ataques digitales y posibles vulnerabilidades. En el ámbito educativo, este concepto adquiere una dimensión particular, ya que involucra la protección de información sensible relacionada con estudiantes, docentes e instituciones educativas.

Uno de los principios fundamentales de la ciberseguridad es la confidencialidad, que se refiere a la protección de la información para evitar que sea accedida por personas no autorizadas. En el contexto educativo, esto implica garantizar que los datos personales de los estudiantes, como calificaciones, información médica o datos familiares, sean protegidos adecuadamente (Orellana & Moran, 2025).

Otro principio clave es la integridad de la información, que asegura que los datos no sean alterados de manera indebida. En el aula digital, esto es especialmente relevante en procesos de evaluación, donde la manipulación de datos puede afectar la validez de los resultados académicos. Asimismo, la disponibilidad de la información constituye un elemento esencial, ya que garantiza que los sistemas educativos funcionen de manera continua y que los usuarios puedan acceder a los recursos cuando lo necesiten (Ramos et al., 2025).

Estos principios conforman la base de la ciberseguridad y permiten comprender la importancia de implementar medidas que protejan los entornos educativos digitales. La falta de conocimiento sobre estos aspectos puede generar vulnerabilidades que ponen en riesgo tanto a los estudiantes como a las instituciones educativas.

1.3 Riesgos digitales en el aula contemporánea

El uso de tecnologías digitales en la educación ha incrementado la exposición a diversos riesgos que pueden afectar la seguridad de los entornos educativos. Entre estos riesgos se encuentran las amenazas relacionadas con el acceso no autorizado a la información, la difusión de contenido inapropiado y la manipulación de datos.

Uno de los riesgos más comunes es el phishing, una técnica de ingeniería social que busca engañar a los usuarios para obtener información confidencial, como contraseñas o datos personales. En el contexto educativo, los estudiantes y docentes pueden ser víctimas de este tipo de ataques a través de correos electrónicos o mensajes fraudulentos que simulan provenir de instituciones oficiales (Montilla & Omar, 2025).

Otro riesgo importante es el malware, que incluye programas maliciosos diseñados para dañar sistemas

informáticos o robar información. Estos programas pueden infiltrarse en los dispositivos a través de descargas no seguras, enlaces sospechosos o aplicaciones fraudulentas, comprometiendo la seguridad de la información almacenada (Medina, 2025).

Asimismo, el ciberacoso constituye una de las principales problemáticas en los entornos educativos digitales, afectando el bienestar emocional de los estudiantes y generando un impacto negativo en su proceso de aprendizaje. Este fenómeno se ve agravado por el uso de redes sociales y plataformas digitales, donde la interacción constante puede dar lugar a situaciones de violencia digital (Tolaba, 2025).

1.4 Tipos de amenazas en entornos educativos

Las amenazas digitales en el ámbito educativo pueden clasificarse en diferentes categorías, dependiendo de su naturaleza y de los objetivos que persiguen. Una de las principales categorías es la ingeniería social, que se basa en la manipulación

psicológica de los usuarios para obtener información confidencial. Este tipo de amenaza es especialmente peligroso en entornos educativos, donde los estudiantes pueden carecer de la experiencia necesaria para identificar intentos de fraude (Rodríguez & Jiménez, 2026).

Otra categoría relevante es la de los ataques informáticos, que incluyen acciones como el acceso no autorizado a sistemas, la alteración de datos y la interrupción de servicios. Estos ataques pueden afectar la operatividad de las plataformas educativas y comprometer la seguridad de la información institucional (Vega, 2026).

Por otro lado, las amenazas internas también representan un riesgo significativo, ya que pueden originarse dentro de la propia institución educativa. Estas amenazas pueden estar relacionadas con el uso inadecuado de la tecnología por parte de estudiantes o docentes, así como con la falta de políticas de seguridad adecuadas (Domínguez, 2025).

1.5 Importancia de la alfabetización digital en ciberseguridad

La alfabetización digital se presenta como una herramienta fundamental para la prevención de riesgos en entornos educativos digitales, ya que permite a los usuarios desarrollar habilidades para utilizar la tecnología de manera segura y responsable. En este sentido, la formación en ciberseguridad debe ser parte integral del proceso educativo, promoviendo el desarrollo de competencias que permitan identificar y prevenir amenazas digitales.

El fortalecimiento de las habilidades digitales en estudiantes y docentes contribuye a mejorar la seguridad de los entornos educativos, ya que permite una mayor conciencia sobre los riesgos y las medidas de protección necesarias. La implementación de programas educativos orientados a la ciberseguridad ha demostrado ser efectiva para reducir la vulnerabilidad frente a amenazas digitales y

promover una cultura de seguridad en el uso de la tecnología (Gladys & Milena, 2025).

Asimismo, la alfabetización digital permite fomentar el pensamiento crítico en relación con el uso de la tecnología, lo que resulta esencial para identificar información falsa, evitar fraudes y proteger la privacidad de los datos. En este contexto, el docente desempeña un papel clave como mediador del aprendizaje, orientando a los estudiantes en el desarrollo de competencias digitales seguras (Guillén, 2025).

1.6 El rol del docente en la ciberseguridad del aula digital

En el contexto de la educación digital, el docente asume un papel estratégico en la protección del entorno educativo frente a amenazas cibernéticas. Más allá de su función tradicional como facilitador del aprendizaje, el docente se convierte en un agente clave para la prevención de riesgos digitales, la promoción de buenas prácticas tecnológicas y el

desarrollo de una cultura de ciberseguridad en el aula. Este rol implica no solo el conocimiento de herramientas digitales, sino también la capacidad de orientar a los estudiantes en el uso seguro y responsable de la tecnología.

El docente debe ser capaz de identificar posibles vulnerabilidades en el entorno digital educativo, así como de implementar estrategias que reduzcan los riesgos asociados al uso de plataformas y dispositivos tecnológicos. Esto incluye la gestión adecuada de contraseñas, la supervisión del uso de herramientas digitales y la enseñanza de prácticas seguras en la navegación en internet. En este sentido, la formación docente en ciberseguridad se convierte en un elemento fundamental para garantizar la protección del aula digital (Rodríguez & Jiménez, 2026).

Asimismo, el docente desempeña un papel relevante en la sensibilización de los estudiantes sobre los riesgos digitales, promoviendo el desarrollo de competencias relacionadas con la seguridad de la información. Esto implica fomentar el pensamiento

crítico, la responsabilidad digital y la capacidad de identificar posibles amenazas en el entorno virtual. La educación en ciberseguridad no solo contribuye a la protección de los datos, sino también al desarrollo integral de los estudiantes como ciudadanos digitales responsables (Gonzalez et al., 2025).

Por otro lado, el docente debe actuar como mediador en situaciones de riesgo, interviniendo de manera oportuna ante incidentes como el ciberacoso o el acceso no autorizado a la información. Esta función requiere no solo conocimientos técnicos, sino también habilidades pedagógicas y sociales que permitan gestionar de manera adecuada estas situaciones y brindar apoyo a los estudiantes afectados (Tolaba, 2025).

1.7 Políticas educativas y normativas de ciberseguridad

La implementación de la ciberseguridad en el ámbito educativo requiere el establecimiento de políticas y normativas que regulen el uso de la

tecnología y garanticen la protección de los datos. Estas políticas deben ser diseñadas de manera integral, considerando aspectos técnicos, pedagógicos y legales, con el fin de crear un entorno seguro para todos los actores educativos.

Las políticas digitales en educación deben incluir lineamientos claros sobre el uso de plataformas tecnológicas, la gestión de la información y la protección de la privacidad. Estas normativas permiten establecer responsabilidades y definir protocolos de actuación ante posibles incidentes de seguridad, contribuyendo a la prevención de riesgos y a la mejora de la gestión educativa (Domínguez, 2025).

En este contexto, resulta fundamental que las instituciones educativas desarrollen estrategias de ciberseguridad que incluyan la capacitación de docentes y estudiantes, la implementación de sistemas de protección y la evaluación continua de los riesgos. La adopción de políticas de ciberseguridad no solo protege la información, sino que también

fortalece la confianza en el uso de la tecnología en el aula (Vega, 2026).

Asimismo, la normativa debe contemplar aspectos relacionados con la ciudadanía digital, promoviendo valores como el respeto, la responsabilidad y la ética en el uso de la tecnología. La integración de estos principios en el currículo educativo contribuye a la formación de estudiantes conscientes de los riesgos digitales y capaces de actuar de manera segura en entornos virtuales (Solano et al., 2025).

1.8 Cultura de ciberseguridad en el entorno educativo

La construcción de una cultura de ciberseguridad en el ámbito educativo implica la adopción de prácticas y valores que promuevan el uso seguro de la tecnología. Esta cultura debe ser fomentada desde las instituciones educativas, involucrando a todos los actores del proceso educativo, incluyendo docentes, estudiantes y familias.

Una cultura de ciberseguridad se caracteriza por la conciencia sobre los riesgos digitales, el conocimiento de las medidas de protección y la adopción de comportamientos responsables en el uso de la tecnología. En este sentido, la educación desempeña un papel fundamental, ya que permite desarrollar competencias que contribuyen a la prevención de amenazas y a la protección de la información (Casa, 2025).

El fortalecimiento de esta cultura requiere la implementación de estrategias educativas que promuevan la sensibilización y la formación en ciberseguridad. Estas estrategias pueden incluir campañas de concienciación, talleres prácticos y actividades educativas orientadas al desarrollo de habilidades digitales seguras. La participación activa de los estudiantes en estas actividades contribuye a la internalización de buenas prácticas y a la construcción de un entorno educativo más seguro (Herrera et al., 2025).

Asimismo, la cultura de ciberseguridad debe estar respaldada por el uso de metodologías innovadoras que faciliten el aprendizaje, como la gamificación y el aprendizaje basado en proyectos. Estas metodologías permiten abordar la ciberseguridad de manera dinámica y participativa, promoviendo el interés y la motivación de los estudiantes (Suárez, 2025).

1.9 Caso aplicado: prevención de riesgos digitales en instituciones educativas

Un ejemplo relevante de la aplicación de la ciberseguridad en el ámbito educativo se observa en la implementación de programas de prevención de riesgos digitales en instituciones educativas. En estos programas, se desarrollan actividades orientadas a la identificación de amenazas, la protección de datos y el uso responsable de la tecnología.

En un caso aplicado en el contexto latinoamericano, se implementó una estrategia educativa basada en el uso de metodologías activas

para la prevención de delitos cibernéticos. Esta estrategia incluyó la utilización de herramientas digitales, actividades colaborativas y simulaciones que permitieron a los estudiantes identificar riesgos y desarrollar habilidades para enfrentarlos. Los resultados evidenciaron una mejora significativa en la conciencia digital y en la capacidad de los estudiantes para identificar amenazas (López et al., 2025).

Asimismo, se han desarrollado plataformas educativas orientadas a la capacitación en ciberseguridad, las cuales permiten a los estudiantes participar en actividades prácticas como competencias tipo CTF (Capture The Flag), donde deben resolver desafíos relacionados con la seguridad informática. Estas experiencias contribuyen al desarrollo de habilidades técnicas y al fortalecimiento de la cultura de ciberseguridad en el entorno educativo (Freccero et al., 2025).

1.10 Integración de la ciberseguridad en el currículo educativo

La integración de la ciberseguridad en el currículo educativo constituye una estrategia clave para garantizar la formación de estudiantes capaces de enfrentar los desafíos del entorno digital. Esta integración debe ser transversal, abarcando diferentes áreas del conocimiento y niveles educativos, con el fin de promover el desarrollo de competencias digitales seguras desde edades tempranas.

El currículo educativo debe incluir contenidos relacionados con la protección de datos, la identificación de amenazas y el uso responsable de la tecnología. Estos contenidos deben ser abordados de manera progresiva, adaptándose al nivel de desarrollo de los estudiantes y utilizando metodologías que faciliten el aprendizaje significativo (Mejía, 2026).

Asimismo, la integración de la ciberseguridad en el currículo permite fortalecer la relación entre educación y tecnología, promoviendo un enfoque interdisciplinario que contribuye al desarrollo de competencias clave para el siglo XXI. En este sentido, la educación en ciberseguridad no solo tiene un enfoque preventivo, sino también formativo, ya que prepara a los estudiantes para desenvolverse de manera segura en entornos digitales.

1.11 Síntesis del capítulo

En síntesis, la ciberseguridad en el entorno educativo se configura como un elemento esencial para garantizar la protección de los datos y la seguridad de los actores educativos en un contexto cada vez más digitalizado. A lo largo de este capítulo se ha evidenciado que la incorporación de tecnologías en la educación, si bien ofrece múltiples beneficios, también implica la aparición de riesgos que deben ser gestionados de manera adecuada.

Se ha destacado la importancia de los conceptos fundamentales de ciberseguridad, así como la identificación de los principales riesgos y amenazas presentes en el aula digital. Asimismo, se ha analizado el rol del docente como agente clave en la prevención de riesgos y en la promoción de una cultura de seguridad, así como la relevancia de las políticas educativas y la integración de la ciberseguridad en el currículo.

Finalmente, los casos analizados demuestran que la implementación de estrategias educativas orientadas a la ciberseguridad contribuye a mejorar la conciencia digital y a fortalecer las competencias de los estudiantes, lo que permite construir entornos educativos más seguros, responsables y preparados para los desafíos del mundo digital.

CAPÍTULO 2

PROTECCIÓN DE DATOS Y PRIVACIDAD EN EL AULA DIGITAL

La protección de datos y la privacidad son pilares fundamentales para garantizar la seguridad de los entornos educativos digitales. Docentes y estudiantes manejan información personal y académica que debe ser resguardada mediante prácticas responsables, políticas claras y el uso ético de la tecnología.

2.1 ¿QUÉ ES LA PROTECCIÓN DE DATOS?

Es el conjunto de medidas, políticas y procedimientos que aseguran el tratamiento adecuado de la información personal, garantizando su confidencialidad, integridad y disponibilidad.

En el contexto educativo, protege los datos de estudiantes, docentes y personal administrativo frente a accesos no autorizados, pérdidas, robos o usos indebidos.

PRINCIPIOS CLAVE

Legalidad	Finalidad	Consentimiento	Seguridad	Transparencia
Los datos deben recopilarse y usarse conforme a la ley.	Los datos se recolectan para fines educativos específicos.	Las personas deben autorizar el uso de sus datos.	Se deben aplicar medidas técnicas y organizativas adecuadas.	Informar de forma clara cómo se usan y protegen los datos.

Fuente: Adaptado de Orellana & Moran (2025).

2.2 TIPOS DE DATOS EN EL AULA DIGITAL

Tipo de dato	Descripción
Datos personales	Nombre, edad, dirección, correo electrónico, documentos de identidad.
Datos académicos	Notas, evaluaciones, historial académico, proyectos y trabajos.
Datos de uso	Información sobre el uso de plataformas, conexiones, tiempo en línea y actividades.
Datos sensibles	Información médica, psicológica o cualquier dato que pueda afectar la integridad del individuo.
Datos institucionales	Documentos administrativos, informes, bases de datos de la institución.

Fuente: Adaptado de Ramos et al. (2025).

2.3 RIESGOS PARA LA PRIVACIDAD EN EL AULA DIGITAL

- **Acceso no autorizado:** personsas sin permiso pueden acceder a información personal y académica.
- **Malware y ataques informáticos:** software malicioso diseñado para robar o dañar información.
- **Phishing:** intento de engañar a los usuarios para obtener datos confidenciales.
- **Almacenamiento inadecuado:** guardar datos en plataformas o dispositivos sin medidas de seguridad.
- **Compartición excesiva:** divulgar información personal en redes sociales o plataformas públicas.

Fuente: Adaptado de Montilla & Omar (2025); Casa (2025).

2.4 BUENAS PRÁCTICAS PARA PROTEGER DATOS Y PRIVACIDAD

- **Usar contraseñas seguras:** combina letras, números y símbolos, y cámbialas periódicamente.
- **Limitar el acceso:** compartir información solo con personas autorizadas y con fines educativos.
- **Realizar copias de seguridad:** guardar la información en lugares seguros y cifrados.
- **Configurar la privacidad:** revisar los ajustes de las plataformas y herramientas digitales.
- **Educar y sensibilizar:** formar a estudiantes y docentes sobre el uso responsable de los datos.
- **Cumplir con la normativa:** respetar las leyes y políticas institucionales de protección de datos.

Fuente: Adaptado de Herrera et al. (2025); Solano et al. (2025).

2.5 MARCO NORMATIVO Y ÉTICO EN LA PROTECCIÓN DE DATOS EDUCATIVOS

La protección de datos en educación está respaldada por normativas nacionales e internacionales que garantizan los derechos de privacidad y el uso ético de la información. Algunas referencias clave:

- Ley de Protección de Datos Personales de cada país.
- Reglamento General de Protección de Datos (GDPR) de la Unión Europea.
- Convención sobre los Derechos del Niño (ONU).
- Políticas institucionales de privacidad y seguridad digital.

El uso ético de los datos implica respetar la dignidad, la autonomía y los derechos de los estudiantes, garantizando que la información se utilice únicamente para fines educativos y con total transparencia.

Fuente: Adaptado de Vega (2026); Gonzalez et al. (2025).

REFLEXIÓN DOCENTE

¿Qué información manejo en mi aula digital? ¿Cómo puedo garantizar que los datos de mis estudiantes estén protegidos? ¿Qué prácticas debo mejorar para respetar su privacidad?

Fuente general de la unidad: Ramos et al. (2025); Herrera et al. (2025); Orellana & Moran (2025); Montilla & Omar (2025); Solano et al. (2025); Casa (2025); Vega (2026).

CAPÍTULO 2: Protección de datos y privacidad en el aula digital

2.1 Introducción a la protección de datos en educación

El desarrollo de entornos educativos digitales ha generado una creciente preocupación por la protección de los datos personales y la privacidad de los usuarios, especialmente en contextos donde estudiantes y docentes interactúan de manera constante con plataformas tecnológicas. La digitalización de la educación ha permitido mejorar el acceso a la información, la comunicación y la gestión del aprendizaje; sin embargo, también ha incrementado la exposición a riesgos relacionados con el manejo inadecuado de datos y la vulneración de la privacidad.

En este contexto, la protección de datos en el aula digital se convierte en un elemento fundamental para garantizar la seguridad de la información y la confianza en el uso de las tecnologías educativas. La

información generada en los entornos digitales educativos incluye datos sensibles como calificaciones, información personal, registros de comportamiento y actividades académicas, lo que exige la implementación de medidas adecuadas para su resguardo (Medina, 2025).

La preocupación por la privacidad no se limita únicamente a la protección de los datos, sino que también implica la necesidad de garantizar que estos sean utilizados de manera ética y responsable. En este sentido, la educación en ciberseguridad debe abordar no solo los aspectos técnicos, sino también los principios éticos que regulan el uso de la información en entornos digitales (Bustos & Lizardo, 2025).

2.2 Datos personales en el entorno educativo

Los datos personales en el ámbito educativo constituyen uno de los activos más importantes que deben ser protegidos, ya que su uso indebido puede generar consecuencias negativas tanto para los

estudiantes como para las instituciones. Estos datos incluyen información identificativa, académica, socioeconómica y, en algunos casos, datos sensibles relacionados con la salud o la situación familiar.

El manejo de estos datos en entornos digitales implica la recopilación, almacenamiento y procesamiento de información a través de plataformas educativas, lo que aumenta el riesgo de accesos no autorizados y posibles vulneraciones de la privacidad. En este sentido, es fundamental que las instituciones educativas implementen políticas claras sobre el uso y la protección de los datos personales, garantizando su confidencialidad e integridad (Orellana & Moran, 2025).

Asimismo, el uso de tecnologías educativas requiere que los docentes y estudiantes sean conscientes de la importancia de proteger la información personal, evitando compartir datos sensibles en entornos no seguros. La formación en este ámbito permite desarrollar una mayor responsabilidad en el manejo de la información y

reducir la exposición a riesgos digitales (Gonzalez et al., 2025).

Por otro lado, la gestión de datos en el aula digital debe considerar el principio de minimización, es decir, la recopilación únicamente de la información necesaria para el desarrollo de las actividades educativas. Este enfoque contribuye a reducir el riesgo de exposición de datos y a garantizar un uso más responsable de la información.

2.3 Privacidad digital en el aula virtual

La privacidad digital se refiere al derecho de los usuarios a controlar el acceso y uso de su información personal en entornos digitales. En el contexto educativo, este concepto adquiere una relevancia especial, ya que los estudiantes, especialmente los menores de edad, requieren una protección adicional frente a posibles riesgos.

El uso de plataformas virtuales, redes sociales y herramientas digitales en la educación implica la creación de perfiles digitales que pueden ser

utilizados para fines diversos, desde la personalización del aprendizaje hasta la recopilación de datos con fines comerciales. Esta situación plantea la necesidad de establecer límites claros sobre el uso de la información y de garantizar que los datos sean utilizados exclusivamente para fines educativos (Domínguez, 2025).

Asimismo, la privacidad en el aula digital está relacionada con la protección de la identidad de los estudiantes, evitando la exposición innecesaria de información personal. Esto incluye la configuración adecuada de las plataformas educativas, la restricción del acceso a la información y el uso de medidas de seguridad que garanticen la confidencialidad de los datos.

La educación en privacidad digital también implica la formación de los estudiantes en el uso responsable de la tecnología, promoviendo prácticas como la protección de contraseñas, la configuración de la privacidad en redes sociales y la identificación de riesgos asociados al uso de internet. Estas

habilidades son fundamentales para garantizar la seguridad en entornos digitales y para fomentar una ciudadanía digital responsable (Solano et al., 2025).

2.4 Riesgos asociados a la vulneración de datos

La vulneración de datos en entornos educativos puede tener múltiples consecuencias, tanto a nivel individual como institucional. Entre los principales riesgos se encuentran el robo de identidad, el acceso no autorizado a información académica y la difusión de datos personales sin consentimiento.

Uno de los riesgos más relevantes es el acceso indebido a plataformas educativas, lo que puede permitir la manipulación de información académica o la obtención de datos personales de los estudiantes. Este tipo de situaciones puede afectar la confianza en el sistema educativo y generar problemas legales para las instituciones (Ramos et al., 2025).

Asimismo, la filtración de datos puede dar lugar a situaciones de ciberacoso, especialmente cuando la

información personal es utilizada para dañar la reputación de los estudiantes. Este fenómeno tiene un impacto significativo en el bienestar emocional de los estudiantes y puede afectar su rendimiento académico (Tolaba, 2025).

Otro riesgo importante es la comercialización de datos, que puede ocurrir cuando las plataformas digitales utilizan la información de los usuarios con fines comerciales sin su consentimiento. Este aspecto plantea la necesidad de establecer regulaciones claras sobre el uso de los datos y de garantizar la transparencia en el manejo de la información (Vega, 2026).

2.5 Buenas prácticas para la protección de datos

La protección de datos en el aula digital requiere la implementación de buenas prácticas que permitan reducir los riesgos asociados al uso de la tecnología. Estas prácticas deben ser adoptadas tanto por

docentes como por estudiantes, con el fin de garantizar un entorno educativo seguro.

Una de las principales medidas es el uso de contraseñas seguras, que deben ser complejas, únicas y actualizadas de manera periódica. Asimismo, es importante evitar compartir contraseñas y utilizar sistemas de autenticación que refuercen la seguridad de las cuentas (Rodríguez & Jiménez, 2026).

Otra práctica fundamental es la configuración de la privacidad en las plataformas educativas, limitando el acceso a la información y asegurando que solo las personas autorizadas puedan acceder a los datos. Esto incluye la revisión de los permisos de las aplicaciones y la gestión adecuada de los perfiles digitales.

Además, es importante fomentar el uso responsable de la tecnología, evitando compartir información personal en entornos no seguros y promoviendo la conciencia sobre los riesgos digitales. La educación en este ámbito permite

desarrollar hábitos seguros que contribuyen a la protección de la información (Guillén, 2025).

2.6 Protección de datos en plataformas educativas

El uso de plataformas educativas digitales se ha consolidado como una práctica habitual en los procesos de enseñanza-aprendizaje, facilitando la gestión de contenidos, la comunicación entre docentes y estudiantes, y la evaluación académica. Sin embargo, estas plataformas también representan un punto crítico en términos de ciberseguridad, ya que almacenan grandes volúmenes de información sensible que puede ser objeto de ataques o accesos no autorizados.

Las plataformas como sistemas de gestión del aprendizaje (LMS) requieren la implementación de medidas de seguridad robustas que garanticen la protección de los datos. Estas medidas incluyen la encriptación de la información, el control de accesos, la autenticación de usuarios y la supervisión constante

de posibles vulnerabilidades. La falta de controles adecuados puede derivar en filtraciones de datos, comprometiendo la privacidad de los usuarios y la integridad del sistema educativo (Orellana & Moran, 2025).

Asimismo, es fundamental que las instituciones educativas realicen auditorías periódicas de sus sistemas digitales con el fin de identificar posibles debilidades y establecer mecanismos de mejora continua. Estas auditorías permiten evaluar el cumplimiento de las normativas de protección de datos y garantizar que las plataformas utilizadas cumplan con los estándares de seguridad requeridos (Medina, 2025).

Por otro lado, la configuración adecuada de las plataformas educativas es un aspecto clave para la protección de la privacidad. Esto implica la definición de permisos de acceso, la gestión de roles de usuario y la limitación de la visibilidad de la información. La correcta administración de estos elementos

contribuye a reducir los riesgos asociados al uso de entornos digitales en la educación.

2.7 Rol del docente en la protección de la privacidad

El docente desempeña un papel fundamental en la protección de la privacidad en el aula digital, ya que es el responsable de gestionar el uso de las herramientas tecnológicas y de orientar a los estudiantes en el manejo seguro de la información. Este rol implica no solo el conocimiento de las plataformas educativas, sino también la capacidad de implementar prácticas que garanticen la seguridad de los datos.

Una de las principales responsabilidades del docente es asegurar que los estudiantes utilicen las plataformas digitales de manera adecuada, evitando la exposición de información personal y promoviendo el uso de configuraciones de privacidad seguras. Esto incluye la supervisión del uso de herramientas digitales, la orientación sobre el manejo de datos y la

promoción de hábitos seguros en el entorno virtual (Gonzalez et al., 2025).

Asimismo, el docente debe ser capaz de identificar posibles riesgos relacionados con la privacidad y actuar de manera oportuna para prevenir incidentes. Esto implica la detección de comportamientos sospechosos, la gestión de accesos y la implementación de medidas correctivas cuando sea necesario. En este sentido, la formación docente en ciberseguridad es esencial para garantizar una adecuada protección de los datos en el aula digital (Rodríguez & Jiménez, 2026).

Además, el docente cumple una función educativa en la formación de los estudiantes como ciudadanos digitales responsables, promoviendo valores como la ética, el respeto y la responsabilidad en el uso de la tecnología. Esta formación contribuye a fortalecer la cultura de privacidad y a reducir los riesgos asociados al uso de entornos digitales.

2.8 Protocolos institucionales para la protección de datos

La protección de datos en el ámbito educativo requiere la implementación de protocolos institucionales que regulen el uso de la tecnología y establezcan procedimientos claros para la gestión de la información. Estos protocolos deben ser diseñados de manera integral, considerando tanto los aspectos técnicos como los pedagógicos.

Uno de los elementos clave de estos protocolos es la definición de políticas de acceso a la información, que permitan establecer quiénes pueden acceder a los datos y en qué condiciones. Estas políticas deben ser claras y transparentes, garantizando que la información sea utilizada únicamente para fines educativos (Domínguez, 2025).

Asimismo, los protocolos deben incluir procedimientos para la gestión de incidentes de seguridad, estableciendo acciones específicas que deben ser tomadas en caso de vulneración de datos.

Esto incluye la identificación del incidente, la notificación a las autoridades correspondientes y la implementación de medidas correctivas para evitar futuras ocurrencias.

Otro aspecto relevante es la capacitación de los actores educativos en materia de protección de datos, lo que permite fortalecer la cultura de seguridad y garantizar el cumplimiento de las normativas establecidas. La formación continua en este ámbito es fundamental para adaptarse a los cambios tecnológicos y a los nuevos riesgos digitales (Vega, 2026).

2.9 Caso aplicado: auditoría de ciberseguridad en plataformas educativas

Un caso relevante en la protección de datos en el aula digital es la implementación de auditorías de ciberseguridad en plataformas educativas, con el objetivo de identificar vulnerabilidades y mejorar los sistemas de protección. En este contexto, se realizó un análisis de una plataforma educativa utilizada en

instituciones de educación básica y secundaria, evaluando aspectos como la gestión de accesos, la protección de datos y la configuración de la privacidad.

Los resultados de la auditoría evidenciaron la existencia de vulnerabilidades relacionadas con el uso de contraseñas débiles, la falta de actualización de los sistemas y la configuración inadecuada de los permisos de acceso. A partir de estos hallazgos, se implementaron medidas correctivas que incluyeron la capacitación de los usuarios, la actualización de los sistemas y la mejora de las políticas de seguridad (Orellana & Moran, 2025).

Este caso demuestra la importancia de realizar evaluaciones periódicas de los sistemas educativos digitales, con el fin de garantizar la protección de los datos y mejorar la seguridad de los entornos virtuales. Asimismo, evidencia la necesidad de adoptar un enfoque proactivo en la gestión de la ciberseguridad, anticipándose a posibles riesgos y estableciendo medidas preventivas.

2.10 Educación en privacidad y ciudadanía digital

La educación en privacidad constituye un componente esencial en la formación de los estudiantes, ya que les permite desarrollar habilidades para proteger su información personal y actuar de manera responsable en entornos digitales. Esta formación debe ser integrada en el currículo educativo, promoviendo el desarrollo de competencias relacionadas con la ciudadanía digital.

La ciudadanía digital implica el uso responsable, ético y seguro de la tecnología, así como la comprensión de los derechos y responsabilidades asociados al uso de la información. En este sentido, la educación en privacidad contribuye a formar ciudadanos conscientes de los riesgos digitales y capaces de tomar decisiones informadas en el uso de la tecnología (Solano et al., 2025).

Asimismo, la formación en ciudadanía digital permite abordar problemáticas como el ciberacoso,

la desinformación y el uso indebido de la información, promoviendo valores como el respeto, la empatía y la responsabilidad. Estas competencias son fundamentales para garantizar una convivencia adecuada en entornos digitales y para prevenir situaciones de riesgo.

2.11 Síntesis del capítulo

En síntesis, la protección de datos y la privacidad en el aula digital constituyen elementos fundamentales para garantizar la seguridad de los entornos educativos en la era digital. A lo largo de este capítulo se ha evidenciado la importancia de implementar medidas de seguridad en las plataformas educativas, así como la necesidad de establecer políticas y protocolos que regulen el uso de la información.

Se ha destacado el rol del docente como agente clave en la protección de la privacidad, así como la relevancia de la formación en ciudadanía digital para el desarrollo de competencias que permitan a los

estudiantes actuar de manera segura en entornos digitales. Asimismo, los casos analizados evidencian la importancia de adoptar un enfoque proactivo en la gestión de la ciberseguridad.

Finalmente, la integración de la protección de datos en el currículo educativo se presenta como una estrategia fundamental para garantizar la formación de estudiantes capaces de enfrentar los desafíos del entorno digital, contribuyendo a la construcción de una educación más segura, responsable y acorde a las demandas del siglo XXI.

CAPÍTULO 3

SEGURIDAD EN HERRAMIENTAS DIGITALES EDUCATIVAS

El uso de herramientas digitales en el aula ofrece grandes beneficios, pero también implica riesgos para la información personal, la privacidad y la integridad de los datos. Conocer estas herramientas y aplicar buenas prácticas de seguridad es esencial para garantizar entornos de aprendizaje seguros.

3.1 TIPOS DE HERRAMIENTAS DIGITALES EDUCATIVAS

Las herramientas digitales educativas pueden clasificarse según su función principal:

Comunicación	Gestión del aprendizaje	Creación de contenidos	Almacenamiento en la nube	Evaluación y retroalimentación
Permiten la interacción entre docentes y estudiantes.	Organizan cursos, actividades y recursos.	Facilitan la elaboración de materiales educativos.	Permiten guardar y compartir archivos.	Apoyan la evaluación del aprendizaje.
Ejemplos: Zoom, Microsoft Teams, Google Meet.	Ejemplos: Moodle, Google Classroom, Canvas.	Ejemplos: Canva, Genially, Adobe Express.	Ejemplos: Google Drive, OneDrive, Dropbox.	Ejemplos: Kahoot!, Quizizz, Socrative.

Fuente: Adaptado de Ramos et al. (2025); Vega (2026).

3.2 RIESGOS ASOCIADOS AL USO DE HERRAMIENTAS DIGITALES

El uso inadecuado o la falta de configuraciones de seguridad puede exponer a la comunidad educativa a diversos riesgos:

- **Acceso no autorizado:** terceros pueden ingresar a cuentas, plataformas o documentos sin permiso.
- **Pérdida o filtración de datos:** exposición de información personal o académica.
- **Phishing y fraudes:** intentos de suplantación de identidad para obtener credenciales.
- **Malware y software malicioso:** archivos o enlaces que pueden dañar dispositivos o robar información.
- **Vulneraciones de privacidad:** uso indebido de fotos, videos o datos de estudiantes.

Fuente: Adaptado de Montilla & Omar (2025); Herrera et al. (2025).

3.3 VULNERABILIDADES COMUNES EN HERRAMIENTAS EDUCATIVAS

- Contraseñas débiles o reutilizadas.
- Falta de autenticación en dos pasos.
- Permisos de acceso mal configurados.
- Compartir enlaces sin restricciones.
- Uso de extensiones y complementos no verificadas.
- Versiones desactualizadas de software.
- Desconocimiento de las políticas de privacidad de las plataformas.

Fuente: Adaptado de Freccero et al. (2025); Bustos & Lizardo (2025).

3.4 ESTRATEGIAS PARA USAR HERRAMIENTAS DIGITALES DE FORMA SEGURA

Configurar adecuadamente las plataformas	Usar contraseñas fuertes y únicas	Activar la autenticación en dos pasos	Mantener actualizadas las herramientas	Capacitarse continuamente
Revisar y ajustar permisos, privacidad y opciones de seguridad.	Combinar letras, números y símbolos y cambiarlas periódicamente.	Añade una capa adicional de protección a las cuentas.	Instalar actualizaciones y parches de seguridad.	Actualizar conocimientos sobre seguridad digital y buenas prácticas.

Fuente: Adaptado de Solano et al. (2025); Vega (2026).

3.5 BUENAS PRÁCTICAS DOCENTES EN EL USO DE HERRAMIENTAS DIGITALES

- Verificar la confiabilidad y reputación de las herramientas.
- Leer las políticas de privacidad y términos de uso.
- Evitar compartir información personal o sensible.
- Establecer normas claras de uso para los estudiantes.
- Supervisar las interacciones y actividades en línea.
- Usar canales oficiales de comunicación institucional.
- Realizar copias de seguridad de recursos y contenidos.

Fuente: Adaptado de Casa (2025); Ramos et al. (2025).

3.6 SEGURIDAD EN HERRAMIENTAS ESPECÍFICAS: RECOMENDACIONES

Google Workspace (Classroom, Drive)	• Usar cuentas institucionales. • Revisar permisos de compartir archivos. • No descargar archivos de remitentes desconocidos.
Microsoft Teams	• Configurar reuniones con contraseña. • Restringir ingreso a personas externas. • Moderar chats y permisos de chats.
Zoom	• Activar sala de espera. • Bloquear reuniones una vez iniciadas. • Evitar grabar sin consentimiento.
Moodle	• Mantener el sistema actualizado. • Configurar roles y permisos correctamente. • Hacer copias de seguridad del curso.

Fuente: Adaptado de Domínguez (2025); Vega (2026).

3.7 PROTECCIÓN DE DATOS Y PRIVACIDAD EN HERRAMIENTAS DIGITALES

Recopilar solo los datos necesarios	Informar sobre el uso de los datos	Almacenar de manera segura	Eliminar datos innecesarios	Cumplir con la normativa
Solicitar únicamente la información indispensable para fines educativos.	Comunicar a estudiantes y familias cómo se usará y protegerá su información.	Utilizar plataformas que garanticen cifrado y protección de datos en la nube.	Borrar información cuando ya no sea útil o requerida.	Respetar leyes y políticas de protección de datos (personales, institucionales e internacionales).

Fuente: Adaptado de Orellana & Moran (2025); Vega (2026).

REFLEXIÓN DOCENTE ¿Cómo puedo asegurar que las herramientas digitales que utilizo en mi aula protejan la información, la privacidad y el bienestar de mis estudiantes?

CAPÍTULO 3: Seguridad en herramientas digitales educativas

3.1 Introducción a la seguridad en herramientas digitales educativas

La transformación digital de la educación ha implicado la incorporación intensiva de herramientas tecnológicas que facilitan la enseñanza, el aprendizaje y la gestión académica. Plataformas educativas, aplicaciones colaborativas, sistemas de videoconferencia y herramientas basadas en inteligencia artificial forman parte del ecosistema digital contemporáneo en el que se desarrollan los procesos educativos. Sin embargo, este entorno altamente digitalizado también ha incrementado la exposición a riesgos de ciberseguridad, convirtiendo la protección de estas herramientas en una prioridad estratégica para las instituciones educativas.

La seguridad en herramientas digitales educativas no puede ser entendida únicamente como un conjunto de medidas técnicas destinadas a

proteger sistemas informáticos, sino como un enfoque integral que abarca aspectos tecnológicos, pedagógicos y organizacionales. En este sentido, la ciberseguridad se configura como un componente esencial para garantizar la continuidad de los procesos educativos, la protección de los datos personales y la confianza en el uso de la tecnología (Ramos et al., 2025).

El uso generalizado de plataformas digitales ha permitido democratizar el acceso a la educación, pero también ha generado nuevas formas de vulnerabilidad, especialmente en contextos donde los usuarios carecen de formación en seguridad digital. Los estudiantes, particularmente en niveles básicos y medios, se encuentran expuestos a riesgos como el robo de información, el acceso no autorizado a sus cuentas y la manipulación de contenidos educativos. Esta situación evidencia la necesidad de integrar la ciberseguridad como un elemento transversal en el uso de herramientas digitales en el aula (Montilla & Omar, 2025).

Asimismo, la incorporación de tecnologías emergentes como la inteligencia artificial plantea nuevos desafíos en términos de seguridad, debido a la complejidad de los sistemas y al volumen de datos que procesan. La gestión de estos datos requiere la implementación de medidas avanzadas de protección, así como la adopción de prácticas responsables en el uso de la tecnología (Mejía, 2026).

3.2 Clasificación de herramientas digitales en el aula

Las herramientas digitales utilizadas en el ámbito educativo pueden clasificarse en diferentes categorías, dependiendo de su función y de los procesos que facilitan. Esta clasificación permite comprender los riesgos asociados a cada tipo de herramienta y diseñar estrategias específicas para su protección.

En primer lugar, se encuentran los sistemas de gestión del aprendizaje (LMS), que permiten organizar contenidos, gestionar actividades y evaluar

el desempeño de los estudiantes. Estas plataformas constituyen el núcleo de la educación digital, ya que centralizan la información académica y facilitan la interacción entre docentes y estudiantes. Sin embargo, su uso implica la gestión de grandes volúmenes de datos, lo que las convierte en un objetivo atractivo para ataques cibernéticos (Perez & Zapata, 2025).

En segundo lugar, las herramientas de comunicación digital, como las plataformas de videoconferencia y las aplicaciones de mensajería, desempeñan un papel fundamental en la interacción educativa. Estas herramientas permiten la comunicación en tiempo real, pero también presentan riesgos relacionados con la privacidad, como el acceso no autorizado a las sesiones o la interceptación de mensajes (Domínguez, 2025).

En tercer lugar, se encuentran las herramientas de creación de contenido, que permiten a los estudiantes y docentes generar materiales educativos digitales. Estas herramientas incluyen editores de

texto, aplicaciones multimedia y plataformas colaborativas que facilitan la co-creación del conocimiento. Si bien estas herramientas potencian la creatividad, también pueden implicar riesgos relacionados con la propiedad intelectual y la seguridad de la información.

Finalmente, las herramientas basadas en inteligencia artificial representan una categoría emergente que está transformando la educación. Estas herramientas permiten la personalización del aprendizaje, la automatización de procesos y el análisis de datos educativos. No obstante, su uso plantea desafíos en términos de transparencia, ética y protección de datos (Bustos & Lizardo, 2025).

3.3 Principales vulnerabilidades en herramientas educativas

Las herramientas digitales educativas presentan diversas vulnerabilidades que pueden ser explotadas por actores maliciosos para comprometer la seguridad de los sistemas y la información. Estas

vulnerabilidades pueden originarse tanto en aspectos técnicos como en el comportamiento de los usuarios.

Una de las vulnerabilidades más comunes es el uso de credenciales débiles, que facilita el acceso no autorizado a las cuentas de los usuarios. La falta de prácticas adecuadas en la gestión de contraseñas constituye uno de los principales factores de riesgo en la seguridad digital, especialmente en entornos educativos donde los usuarios suelen compartir información sin considerar las implicaciones de seguridad (Rodríguez & Jiménez, 2026).

Otra vulnerabilidad relevante es la configuración inadecuada de las plataformas, que puede permitir el acceso a información sensible por parte de usuarios no autorizados. Este problema se presenta con frecuencia en sistemas donde los permisos de acceso no están correctamente definidos, lo que genera riesgos para la privacidad de los datos (Orellana & Moran, 2025).

Asimismo, la falta de actualización de las herramientas digitales constituye un factor de riesgo

significativo, ya que las versiones obsoletas pueden contener vulnerabilidades que han sido corregidas en versiones posteriores. La actualización constante de los sistemas es una medida fundamental para garantizar la seguridad de las herramientas digitales (Medina, 2025).

Por otro lado, el factor humano representa una de las principales fuentes de vulnerabilidad en los sistemas de ciberseguridad. Los errores de los usuarios, como la apertura de enlaces sospechosos o la descarga de archivos maliciosos, pueden comprometer la seguridad de los sistemas y facilitar la propagación de ataques (Montilla & Omar, 2025).

3.4 Seguridad en plataformas de videoconferencia y comunicación

Las plataformas de videoconferencia y comunicación digital se han convertido en herramientas esenciales en la educación contemporánea, especialmente en contextos de educación virtual y híbrida. Estas herramientas

permiten la interacción en tiempo real, facilitando la enseñanza a distancia y la colaboración entre los actores educativos. Sin embargo, su uso también implica riesgos significativos en términos de ciberseguridad.

Uno de los principales riesgos asociados a estas plataformas es el acceso no autorizado a las sesiones, lo que puede dar lugar a interrupciones, exposición de información y situaciones de vulnerabilidad para los usuarios. Este fenómeno, conocido como "intrusión en videoconferencias", evidencia la necesidad de implementar medidas de seguridad como el uso de contraseñas, la autenticación de usuarios y la restricción del acceso (Domínguez, 2025).

Asimismo, la grabación de sesiones representa un riesgo potencial para la privacidad, especialmente cuando se almacenan datos sensibles sin las medidas de protección adecuadas. La gestión de estas grabaciones debe realizarse de manera responsable, garantizando la confidencialidad de la información y

el cumplimiento de las normativas de protección de datos.

Otro aspecto relevante es la comunicación a través de aplicaciones de mensajería, que puede implicar la exposición de información personal si no se utilizan de manera adecuada. La educación en el uso seguro de estas herramientas es fundamental para prevenir riesgos y garantizar la protección de los usuarios (Gonzalez et al., 2025).

3.5 Riesgos avanzados en herramientas de inteligencia artificial educativa

La incorporación de herramientas de inteligencia artificial en el ámbito educativo ha introducido nuevas posibilidades para la personalización del aprendizaje, la automatización de procesos y la mejora de la toma de decisiones pedagógicas. Sin embargo, estas tecnologías también han generado riesgos avanzados en términos de ciberseguridad, debido a la complejidad de los sistemas y al volumen de datos que manejan.

Uno de los principales riesgos asociados a la inteligencia artificial es la exposición de datos sensibles, ya que estos sistemas requieren grandes cantidades de información para funcionar de manera eficiente. En el contexto educativo, esto implica la recopilación de datos personales, académicos y comportamentales de los estudiantes, lo que aumenta la vulnerabilidad frente a posibles ataques o usos indebidos de la información (Mejía, 2026).

Asimismo, la falta de transparencia en los algoritmos de inteligencia artificial representa un desafío importante, ya que dificulta la comprensión de cómo se procesan los datos y se toman las decisiones. Esta opacidad puede generar riesgos relacionados con la manipulación de la información y la toma de decisiones automatizadas sin supervisión adecuada (Bustos & Lizardo, 2025).

Otro riesgo relevante es la dependencia de sistemas automatizados, que puede limitar la capacidad de los usuarios para identificar errores o anomalías en el funcionamiento de las herramientas.

En este sentido, es fundamental promover un uso crítico de la inteligencia artificial, donde los docentes y estudiantes comprendan las limitaciones de estas tecnologías y puedan utilizarlas de manera responsable.

3.6 Configuración avanzada de seguridad en herramientas educativas

La configuración de seguridad en herramientas digitales educativas debe ir más allá de las prácticas básicas, incorporando medidas avanzadas que permitan proteger los sistemas frente a amenazas sofisticadas. Estas configuraciones incluyen la implementación de protocolos de autenticación, la gestión de accesos y la supervisión constante de la actividad en las plataformas.

Uno de los elementos clave en la configuración avanzada es la autenticación multifactor, que permite reforzar la seguridad de las cuentas mediante la combinación de diferentes métodos de verificación. Esta medida reduce significativamente el riesgo de

accesos no autorizados y constituye una práctica recomendada en entornos educativos digitales (Rodríguez & Jiménez, 2026).

Asimismo, la segmentación de accesos permite limitar la exposición de la información, asignando permisos específicos según el rol de cada usuario. Esta práctica es fundamental para garantizar la confidencialidad de los datos y prevenir el acceso indebido a información sensible (Orellana & Moran, 2025).

Otro aspecto relevante es la implementación de sistemas de monitoreo que permitan detectar comportamientos sospechosos y prevenir posibles ataques. Estos sistemas utilizan herramientas de análisis de datos para identificar patrones anómalos y generar alertas que facilitan la respuesta oportuna ante incidentes de seguridad (Ramos et al., 2025).

3.7 Gestión de riesgos en el uso de herramientas digitales

La gestión de riesgos en herramientas digitales educativas constituye un proceso continuo que permite identificar, evaluar y mitigar las amenazas que pueden afectar la seguridad de los sistemas. Este proceso implica la adopción de estrategias preventivas y correctivas que garanticen la protección de los entornos digitales.

En el ámbito educativo, la gestión de riesgos debe considerar factores como la diversidad de usuarios, la variedad de herramientas utilizadas y la constante evolución de las amenazas digitales. Esto requiere la implementación de políticas de seguridad que regulen el uso de la tecnología y establezcan procedimientos claros para la prevención de incidentes (Vega, 2026).

Asimismo, la gestión de riesgos debe incluir la capacitación de los usuarios, ya que el factor humano constituye uno de los principales puntos de

vulnerabilidad en los sistemas de ciberseguridad. La formación en buenas prácticas digitales permite reducir los errores humanos y fortalecer la seguridad de las herramientas utilizadas en el aula (Herrera et al., 2025).

Por otro lado, la evaluación periódica de los sistemas permite identificar posibles debilidades y establecer medidas de mejora continua. Este enfoque proactivo es fundamental para garantizar la seguridad de los entornos educativos y prevenir incidentes que puedan afectar el desarrollo del proceso educativo.

3.8 Caso aplicado 1: vulnerabilidad en LMS y acceso no autorizado

Un caso relevante en el análisis de la seguridad en herramientas digitales educativas se presenta en la identificación de vulnerabilidades en sistemas de gestión del aprendizaje. En este contexto, se detectó que la falta de configuración adecuada de los permisos de acceso permitió que usuarios no

autorizados accedieran a información académica sensible.

La vulnerabilidad se originó en la asignación incorrecta de roles dentro de la plataforma, lo que permitió a ciertos usuarios visualizar y modificar información que no correspondía a su nivel de acceso. Esta situación evidenció la importancia de implementar controles adecuados en la gestión de accesos y de realizar auditorías periódicas para identificar posibles fallas en la configuración (Orellana & Moran, 2025).

A partir de este caso, se implementaron medidas correctivas que incluyeron la redefinición de roles, la capacitación de los administradores del sistema y la mejora de las políticas de seguridad. Estas acciones permitieron reducir significativamente el riesgo de acceso no autorizado y fortalecer la seguridad de la plataforma.

3.9 Caso aplicado 2: simulación de ataque de phishing en el aula

Otro caso relevante en la enseñanza de la ciberseguridad en herramientas digitales es la implementación de simulaciones de ataques de phishing en entornos educativos. Estas simulaciones permiten a los estudiantes experimentar situaciones de riesgo y desarrollar habilidades para identificar y prevenir amenazas.

En este caso, se diseñó una actividad en la que los estudiantes recibían correos electrónicos simulados con características de phishing, como enlaces sospechosos y solicitudes de información confidencial. Los estudiantes debían analizar estos correos y determinar si representaban una amenaza, aplicando los conocimientos adquiridos en ciberseguridad (Freccero et al., 2025).

Los resultados evidenciaron una mejora significativa en la capacidad de los estudiantes para identificar ataques de phishing, así como un

incremento en su conciencia sobre los riesgos digitales. Este caso demuestra la efectividad del aprendizaje basado en la experiencia para la enseñanza de la ciberseguridad.

3.10 Estrategias pedagógicas para la seguridad digital

La implementación de estrategias pedagógicas orientadas a la seguridad digital constituye un elemento fundamental para garantizar el uso seguro de las herramientas digitales en el aula. Estas estrategias deben estar diseñadas para promover el aprendizaje significativo y el desarrollo de competencias digitales.

Una de las estrategias más efectivas es la gamificación, que permite abordar la ciberseguridad de manera dinámica y participativa. A través de juegos y actividades interactivas, los estudiantes pueden aprender conceptos de seguridad digital y desarrollar habilidades prácticas para la protección de la información (Suárez, 2025).

Asimismo, el aprendizaje basado en proyectos permite a los estudiantes trabajar en la resolución de problemas relacionados con la ciberseguridad, aplicando sus conocimientos en contextos reales. Esta metodología fomenta el pensamiento crítico y la colaboración, contribuyendo al desarrollo de competencias digitales avanzadas (López et al., 2025).

3.11 Hacia un modelo integral de seguridad en herramientas educativas

La seguridad en herramientas digitales educativas debe evolucionar hacia un modelo integral que combine aspectos tecnológicos, pedagógicos y organizacionales. Este modelo debe considerar la interacción entre los diferentes actores educativos y promover una cultura de seguridad que permita garantizar la protección de los entornos digitales.

En este sentido, la implementación de estrategias de ciberseguridad debe formar parte de una planificación institucional que incluya la evaluación de

riesgos, la capacitación de los usuarios y la adopción de tecnologías seguras. Este enfoque integral permite abordar los desafíos de la ciberseguridad de manera efectiva y garantizar la sostenibilidad de los sistemas educativos digitales (Vega, 2026).

3.12 Síntesis final del capítulo

En síntesis, la seguridad en herramientas digitales educativas constituye un desafío complejo que requiere la integración de múltiples estrategias para garantizar la protección de los entornos de aprendizaje. A lo largo de este capítulo se ha evidenciado que la ciberseguridad no depende únicamente de la tecnología, sino también del comportamiento de los usuarios y de las políticas institucionales.

Se ha destacado la importancia de la configuración avanzada de seguridad, la gestión de riesgos y la implementación de estrategias pedagógicas que promuevan el uso responsable de la tecnología. Asimismo, los casos analizados

demuestran la relevancia de la formación en ciberseguridad y la necesidad de adoptar enfoques innovadores para su enseñanza.

Finalmente, la construcción de entornos educativos seguros requiere un compromiso conjunto de docentes, estudiantes e instituciones, orientado a la promoción de prácticas responsables y al desarrollo de competencias digitales que permitan enfrentar los desafíos del entorno digital.

CAPÍTULO 4

ESTRATEGIAS Y PROTOCOLOS DE CIBERSEGURIDAD DOCENTE

El docente es un actor clave en la protección del aula digital. Implementar estrategias y protocolos de ciberseguridad permite prevenir riesgos, responder ante incidentes y promover una cultura de uso seguro, responsable y ético de la tecnología educativa.

4.1 ROL DEL DOCENTE EN LA CIBERSEGURIDAD

- **Guía y modelo:** promueve buenas prácticas digitales y el uso responsable de la tecnología.
- **Previene riesgos:** identifica amenazas y actúa para evitar incidentes en el aula digital.
- **Protege la información:** asegura la privacidad y los datos de estudiantes y de la comunidad educativa.
- **Responde ante incidentes:** aplica protocolos para minimizar impactos y recuperar la seguridad.

Fuente: Adaptado de Vega (2026); Ramos et al. (2025).

4.2 ESTRATEGIAS DOCENTES PARA PREVENIR RIESGOS

- **Formación y sensibilización:** capacitar a estudiantes sobre ciberseguridad, privacidad y ciudadanía digital.
- **Uso seguro de herramientas:** configurar correctamente plataformas, contraseñas y permisos de acceso.
- **Normas claras en el aula digital:** establecer reglas de uso de dispositivos, comunicación y comportamiento en línea.
- **Supervisión y acompañamiento:** monitorear actividades digitales y orientar el uso responsable de la tecnología.
- **Actualización constante:** mantener programas, dispositivos y software siempre actualizados.

Fuente: Adaptado de Herrera et al. (2025); Casa (2025).

4.3 PROTOCOLOS DE CIBERSEGURIDAD EN EL AULA DIGITAL

1. **Prevención**
   Implementar medidas para evitar amenazas (filtros, contraseñas seguras, copias de seguridad, políticas de uso).
2. **Detección**
   Identificar comportamientos sospechosos, intentos de acceso no autorizado o contenido inapropiado.
3. **Contención**
   Aislar el problema para evitar su propagación (limitar accesos, bloquear cuentas o dispositivos comprometidos).
4. **Respuesta**
   Actuar según el protocolo: informar, registrar y tomar acciones correctivas.
5. **Recuperación**
   Restaurar sistemas y datos, evaluar lo ocurrido y fortalecer las medidas de seguridad.

Fuente: Adaptado de Orellana & Moran (2025); Vega (2026).

4.4 GESTIÓN DE INCIDENTES DE CIBERSEGURIDAD

Identificación → **Contención** → **Erradicación** → **Recuperación** → **Lecciones aprendidas**

- **Identificación:** Reconocer la amenaza y evaluar su impacto.
- **Contención:** Limitar el daño y evitar que se propague.
- **Erradicación:** Eliminar la causa del incidente o la vulnerabilidad.
- **Recuperación:** Restaurar sistemas y datos a su estado seguro.
- **Lecciones aprendidas:** Analizar el incidente y mejorar los protocolos.

Fuente: Adaptado de Vega (2026); Domínguez (2025).

Buenas prácticas en la gestión de incidentes

- Tener un plan de respuesta documentado y conocido por todos.
- Comunicar de manera inmediata a las autoridades competentes.
- No culpar: enfocarse en resolver y aprender para prevenir futuros eventos.
- Mantener un registro de incidentes para análisis y mejora continua.

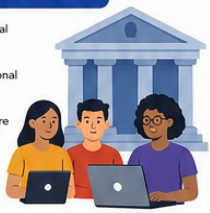
4.5 CASO APLICADO: PROTOCOLO DOCENTE ANTE PHISHING

- **Situación**
  Los estudiantes reciben correos fraudulentos que simulan ser de la institución.
- **Acción docente**
  El docente identifica el intento de phishing y alerta al grupo.
- **Medidas aplicadas**
  Notifica a las autoridades, bloquea enlaces y refuerza la educación sobre phishing.
- **Resultado**
  Se evita el fraude, se protege la información y se fortalece la conciencia digital.

Fuente: Adaptado de Freccero et al. (2025); Vega (2026).

4.6 CULTURA DE CIBERSEGURIDAD EN LA INSTITUCIÓN

- **Compromiso institucional:** integrar la seguridad digital en la misión y políticas de la institución.
- **Participación de todos:** docentes, estudiantes y personal administrativo deben conocer y aplicar las normas.
- **Comunicación efectiva:** difundir información clara sobre riesgos, protocolos y buenas prácticas.
- **Evaluación continua:** revisar y actualizar políticas, capacitaciones y tecnologías.



Fuente: Adaptado de Casa (2025); Ramos et al. (2025).

4.7 HERRAMIENTAS Y RECURSOS RECOMENDADOS

- **Gestores de contraseñas:** Bitwarden, KeePass para crear y almacenar contraseñas seguras.
- **Antivirus y antimalware:** Microsoft Defender, ESET, Kaspersky para proteger dispositivos.
- **Copias de seguridad:** Google Drive, OneDrive, Dropbox para respaldar información crítica.
- **Filtros de correo:** Google Workspace, Microsoft 365 para detectar spam y phishing.
- **VPN:** Para conexiones seguras en redes públicas o externas a la institución.
- **Plataformas seguras:** Moodle, Google Classroom, Microsoft Teams con configuraciones de privacidad adecuadas.
- **Recursos educativos:** INCIBE, ENISA, Cisco Networking Academy para capacitación y materiales gratuitos.

Fuente: Adaptado de Solano et al. (2025); Orellana & Moran (2025); Ramos et al. (2025).

REFLEXIÓN DOCENTE ¿Qué estrategias de ciberseguridad puedo implementar hoy en mi aula digital para proteger a mis estudiantes y promover una cultura de uso seguro y responsable de la tecnología?

CAPÍTULO 4: Estrategias y protocolos de ciberseguridad docente

4.1 Introducción a la ciberseguridad docente en el aula digital

La consolidación de entornos educativos digitales ha transformado el rol del docente, quien ya no se limita a la transmisión de conocimientos, sino que asume responsabilidades relacionadas con la gestión tecnológica, la protección de la información y la prevención de riesgos digitales. En este contexto, la ciberseguridad docente emerge como un componente esencial para garantizar la integridad de los procesos educativos y la protección de los actores involucrados.

La figura del docente se posiciona como el primer filtro de seguridad en el aula digital, ya que es quien orienta el uso de las herramientas tecnológicas y establece las normas de interacción en los entornos virtuales. Esta responsabilidad implica la adopción de estrategias que permitan prevenir amenazas,

gestionar incidentes y promover una cultura de seguridad en el uso de la tecnología (Rodríguez & Jiménez, 2026).

El incremento de ataques cibernéticos en entornos educativos ha evidenciado la necesidad de fortalecer las competencias digitales de los docentes, especialmente en lo relacionado con la identificación de riesgos y la implementación de medidas de protección. La falta de formación en ciberseguridad puede generar vulnerabilidades que comprometan la seguridad de los sistemas y la información (Herrera et al., 2025).

Asimismo, la creciente complejidad de las herramientas digitales requiere que los docentes desarrollen habilidades para gestionar entornos tecnológicos de manera segura, lo que incluye la configuración de plataformas, la protección de datos y la supervisión del uso de la tecnología por parte de los estudiantes (Ramos et al., 2025).

4.2 Estrategias docentes para la prevención de riesgos digitales

La prevención de riesgos digitales en el aula requiere la implementación de estrategias pedagógicas y tecnológicas que permitan reducir la exposición a amenazas y garantizar la seguridad de los usuarios. Estas estrategias deben ser integradas en la práctica docente y adaptadas a las características del contexto educativo.

Una de las estrategias más relevantes es la educación en ciberseguridad, que implica la formación de los estudiantes en el uso seguro de la tecnología. Esta formación debe abordar aspectos como la protección de datos, la identificación de amenazas y el uso responsable de las herramientas digitales. La integración de estos contenidos en el currículo educativo contribuye a desarrollar competencias que permiten prevenir riesgos digitales (Solano et al., 2025).

Otra estrategia fundamental es la supervisión del uso de las herramientas digitales, que permite identificar comportamientos de riesgo y actuar de manera oportuna para prevenir incidentes. El docente debe establecer normas claras sobre el uso de la tecnología y garantizar su cumplimiento, promoviendo un entorno seguro para el aprendizaje (Fuentes, 2025).

Asimismo, la implementación de metodologías activas, como el aprendizaje basado en proyectos y la gamificación, permite abordar la ciberseguridad de manera dinámica y participativa. Estas metodologías facilitan la comprensión de los riesgos digitales y promueven el desarrollo de habilidades prácticas para la protección de la información (Suárez, 2025).

4.3 Protocolos de seguridad en el aula digital

Los protocolos de seguridad constituyen un conjunto de normas y procedimientos que regulan el uso de la tecnología en el aula digital, con el objetivo de prevenir riesgos y garantizar la protección de la

información. Estos protocolos deben ser diseñados de manera integral, considerando tanto los aspectos técnicos como los pedagógicos.

Uno de los elementos clave de los protocolos de seguridad es la gestión de accesos, que permite controlar quiénes pueden acceder a la información y en qué condiciones. Esta gestión debe incluir la asignación de permisos según el rol de cada usuario y la implementación de mecanismos de autenticación que refuercen la seguridad de las cuentas (Orellana & Moran, 2025).

Asimismo, los protocolos deben establecer normas para la protección de los datos personales, garantizando que la información sea utilizada únicamente para fines educativos y que se respete la privacidad de los usuarios. Estas normas deben ser conocidas por todos los actores educativos y aplicadas de manera consistente (Domínguez, 2025).

Otro aspecto relevante es la definición de procedimientos para la gestión de incidentes de seguridad, que permitan actuar de manera oportuna

ante situaciones de riesgo. Estos procedimientos deben incluir la identificación del incidente, la notificación a las autoridades correspondientes y la implementación de medidas correctivas.

4.4 Gestión de incidentes de ciberseguridad

La gestión de incidentes constituye un componente esencial en la ciberseguridad docente, ya que permite responder de manera efectiva ante situaciones que comprometan la seguridad de los entornos digitales. Esta gestión debe ser planificada y estructurada, con el fin de minimizar el impacto de los incidentes y garantizar la continuidad de los procesos educativos.

Uno de los primeros pasos en la gestión de incidentes es la identificación de la amenaza, que implica reconocer la naturaleza del problema y evaluar su impacto. Esta etapa es fundamental para determinar las acciones que deben ser tomadas y para evitar la propagación del incidente (Vega, 2026).

Posteriormente, se debe proceder a la contención del incidente, implementando medidas que permitan limitar su impacto y evitar que afecte a otros sistemas o usuarios. Esta etapa puede incluir la desconexión de dispositivos, la suspensión de cuentas o la restricción del acceso a determinados recursos.

Finalmente, la recuperación del sistema implica la restauración de las condiciones normales de funcionamiento y la implementación de medidas que permitan prevenir futuros incidentes. Este proceso debe incluir una evaluación del incidente y la identificación de las causas que lo originaron.

4.5 Caso aplicado: protocolo docente ante ataque de phishing

Un ejemplo relevante de la aplicación de protocolos de ciberseguridad en el aula se presenta en la gestión de un ataque de phishing dirigido a estudiantes de una institución educativa. En este caso, los estudiantes recibieron correos electrónicos

fraudulentos que simulaban ser enviados por la institución, solicitando información personal.

El docente, al identificar la situación, implementó un protocolo de seguridad que incluyó la notificación a las autoridades, la advertencia a los estudiantes y la suspensión temporal de las cuentas afectadas. Asimismo, se realizó una actividad educativa orientada a la identificación de ataques de phishing, lo que permitió fortalecer la conciencia digital de los estudiantes (Freccero et al., 2025).

Este caso demuestra la importancia de contar con protocolos claros y de actuar de manera oportuna ante incidentes de seguridad, así como el rol del docente en la prevención y gestión de riesgos digitales.

4.6 Construcción de una cultura institucional de ciberseguridad

La implementación efectiva de estrategias de ciberseguridad en el ámbito educativo no puede

depender únicamente de acciones individuales del docente, sino que requiere la consolidación de una cultura institucional que promueva prácticas seguras en todos los niveles del sistema educativo. Esta cultura se construye a partir de la integración de valores, normas y comportamientos orientados a la protección de la información y al uso responsable de la tecnología.

Una cultura de ciberseguridad implica que todos los actores educativos, incluyendo directivos, docentes, estudiantes y personal administrativo, asuman la seguridad digital como una responsabilidad compartida. Este enfoque permite generar un entorno educativo más seguro, donde las prácticas de protección de la información se convierten en parte del comportamiento cotidiano (Casa, 2025).

La construcción de esta cultura requiere la implementación de programas de sensibilización y formación que permitan a los usuarios comprender los riesgos asociados al uso de la tecnología y adoptar

medidas para prevenirlos. Estas iniciativas deben ser continuas y adaptarse a las necesidades del contexto educativo, considerando la evolución constante de las amenazas digitales (Herrera et al., 2025).

Asimismo, la cultura de ciberseguridad debe estar respaldada por políticas institucionales que regulen el uso de la tecnología y establezcan responsabilidades claras para cada actor. Estas políticas permiten garantizar la coherencia en la implementación de las estrategias de seguridad y facilitar la gestión de los riesgos digitales (Vega, 2026).

4.7 Formación docente avanzada en ciberseguridad

La formación docente en ciberseguridad constituye un elemento clave para la implementación de estrategias efectivas en el aula digital. Esta formación debe ir más allá de los conocimientos básicos sobre el uso de herramientas tecnológicas, incorporando competencias relacionadas con la

gestión de riesgos, la protección de datos y la respuesta ante incidentes de seguridad.

El docente debe desarrollar habilidades para identificar vulnerabilidades en los sistemas, evaluar riesgos y aplicar medidas de protección adecuadas. Esto implica la adquisición de conocimientos técnicos, así como la capacidad de integrar la ciberseguridad en su práctica pedagógica (Guillén, 2025).

Asimismo, la formación docente debe incluir aspectos relacionados con la ética digital, promoviendo el uso responsable de la tecnología y el respeto por la privacidad de los usuarios. Estos principios son fundamentales para garantizar un entorno educativo seguro y para fomentar la ciudadanía digital (Solano et al., 2025).

La capacitación continua se convierte en un elemento esencial en este proceso, ya que permite a los docentes adaptarse a los cambios tecnológicos y a las nuevas amenazas digitales. En este sentido, las instituciones educativas deben promover programas

de formación que permitan fortalecer las competencias digitales de los docentes y mejorar su capacidad para gestionar la ciberseguridad en el aula.

4.8 Caso aplicado 2: implementación de políticas de ciberseguridad en una institución educativa

Un caso relevante en la implementación de estrategias de ciberseguridad docente se presenta en una institución educativa que desarrolló un conjunto de políticas orientadas a la protección de los entornos digitales. Estas políticas incluían normas sobre el uso de plataformas educativas, la gestión de datos personales y la prevención de riesgos digitales.

La implementación de estas políticas permitió mejorar la seguridad de los sistemas y reducir la incidencia de incidentes de ciberseguridad. Asimismo, se evidenció un aumento en la conciencia digital de los docentes y estudiantes, lo que contribuyó a fortalecer la cultura de seguridad en la institución (Domínguez, 2025).

Este caso demuestra la importancia de contar con políticas claras y de promover la participación de todos los actores educativos en la implementación de estrategias de ciberseguridad.

4.9 Caso aplicado 3: desarrollo de competencias en ciberseguridad mediante gamificación

Otro caso relevante se observa en la implementación de estrategias de gamificación para la formación en ciberseguridad, donde los docentes utilizaron herramientas digitales para desarrollar competencias en los estudiantes. Estas estrategias incluyeron la realización de actividades interactivas, juegos educativos y simulaciones de riesgos digitales.

La gamificación permitió mejorar la motivación de los estudiantes y facilitar la comprensión de conceptos relacionados con la ciberseguridad. Asimismo, se evidenció un incremento en la capacidad de los estudiantes para identificar

amenazas y aplicar medidas de protección (Suárez, 2025).

Este caso demuestra el potencial de las metodologías innovadoras para la enseñanza de la ciberseguridad y resalta la importancia de integrar estas estrategias en la práctica docente.

4.10 Modelo integral de ciberseguridad docente

El desarrollo de un modelo integral de ciberseguridad docente implica la integración de estrategias pedagógicas, tecnológicas y organizacionales que permitan garantizar la protección de los entornos educativos. Este modelo debe considerar la interacción entre los diferentes actores educativos y promover una cultura de seguridad que facilite la implementación de prácticas responsables.

En este contexto, el modelo integral debe incluir la formación docente, la implementación de protocolos de seguridad, la gestión de riesgos y la

evaluación continua de los sistemas. Estos elementos permiten abordar la ciberseguridad de manera holística y garantizar la sostenibilidad de las estrategias implementadas (Ramos et al., 2025).

Asimismo, el modelo debe promover la participación activa de los estudiantes en la gestión de la ciberseguridad, fomentando el desarrollo de competencias que les permitan actuar de manera segura en entornos digitales. Este enfoque contribuye a la construcción de una ciudadanía digital responsable y preparada para enfrentar los desafíos del mundo digital.

4.11 Síntesis del capítulo

En síntesis, la ciberseguridad docente constituye un elemento fundamental para garantizar la protección de los entornos educativos en la era digital. A lo largo de este capítulo se ha evidenciado la importancia de implementar estrategias y protocolos que permitan prevenir riesgos, gestionar

incidentes y promover el uso responsable de la tecnología.

Se ha destacado la relevancia de la formación docente, la construcción de una cultura institucional de ciberseguridad y la implementación de modelos integrales que permitan abordar los desafíos del entorno digital. Asimismo, los casos analizados demuestran la efectividad de las estrategias implementadas y su impacto en la mejora de la seguridad de los sistemas educativos.

Finalmente, la integración de la ciberseguridad en la práctica docente se presenta como una oportunidad para transformar la educación y garantizar la protección de los actores educativos, contribuyendo al desarrollo de entornos de aprendizaje seguros, responsables y preparados para los desafíos del siglo XXI.

La ciberseguridad en el ámbito educativo se ha consolidado como un elemento esencial para garantizar la protección de los entornos digitales y la seguridad de los actores involucrados en el proceso

educativo. A lo largo de esta obra se ha evidenciado que la integración de la tecnología en la educación, si bien ofrece múltiples beneficios, también implica la aparición de riesgos que deben ser gestionados de manera adecuada.

El análisis desarrollado en los diferentes capítulos permite concluir que la ciberseguridad no depende únicamente de la implementación de herramientas tecnológicas, sino también del comportamiento de los usuarios y de las políticas institucionales. La formación en competencias digitales, la adopción de buenas prácticas y la implementación de estrategias de seguridad constituyen elementos clave para la protección de los entornos educativos.

Asimismo, la construcción de una cultura de ciberseguridad se presenta como un desafío fundamental para las instituciones educativas, ya que permite promover el uso responsable de la tecnología y fortalecer la confianza en los sistemas digitales. Este enfoque requiere la participación activa

de todos los actores educativos y la integración de la ciberseguridad en el currículo educativo.

Finalmente, la educación en ciberseguridad se configura como una herramienta clave para la formación de ciudadanos digitales responsables, capaces de enfrentar los desafíos del entorno digital y de contribuir a la construcción de una sociedad más segura y equitativa. Este libro constituye un aporte para la comprensión y aplicación de estrategias de ciberseguridad en el ámbito educativo, promoviendo el desarrollo de entornos de aprendizaje seguros y sostenibles.

REFERENCIAS

Acosta, M. E. (2025). *Drones y Ciberseguridad en la ense˜nanza de la Ingenierı´a Civil*.

Baños, M. M. (2025). Uso de tecnologías educativas en el aula de bachillerato: Un enfoque en el impacto sobre el rendimiento académico. *EDUCERE*, *3*(1), 27-38. https://doi.org/10.71657/educere.v3i1.3663

Bustos, M., & Lizardo, J. (2025). *Responsabilidad social de la inteligencia artificial aplicados en el aula de clase*. http://repository.unad.edu.co/handle/10596/77710

Casa, W. G. (2025). *La educación digital y su rol en la prevención ante la ciberdelincuencia juvenil en Ecuador*. https://repositorio.uisek.edu.ec/handle/123456789/5530

Domínguez, R. A. (2025). Políticas digitales en educación y seguridad: Un acercamiento en nivel básico

mexicano. En T. Ordaz, L. Pons, & T. Guzmán, *Investigaciones sobre el vínculo educación y tecnología educativa* (1.ª ed., pp. 137-155). Ediciones Comunicación Científica; Consejo Mexicano de Investigación Educativa; Universidad Autónoma de Querétaro. https://doi.org/10.52501/cc.282.06

Fabián, C. C. (2025). *Convivencias en la era digital, aportes a la actualización de los AEC*. https://repositorio.21.edu.ar/handle/ues21/29966

Freccero, B., Queiruga, C., Venosa, P., & Díaz, F. (2025). *CTF en escuelas secundarias 2.0: Una plataforma para la organización de competencias de ciberseguridad escolares*. Simposio Argentino de Educación en Informática (SAEI 2025) - JAIIO 54 (Universidad de Buenos Aires, 4 al 7 de agosto de 2025). http://sedici.unlp.edu.ar/handle/10915/190420

Fuentes, L. A. (2025). *Convivencia 2.0: Actualización de Acuerdos Escolares para el Siglo XXI en la Unidad*

Educativa Maryland. https://repositorio.21.edu.ar/handle/ues21/30423

Gladys, C. M., & Milena, M. M. C. (2025). *Fortalecimiento de las habilidades digitales y la seguridad digital, a través de secuencias didácticas y el uso de recursos educativos digitales en los niños y niñas de grado quinto a de la Institución Educativa Zapata de Necoclí, Antioquia*. https://hdl.handle.net/11227/19401

Gonzalez, M. Y., Yadicela, R. E. S., Verdezoto, A. M. Z., & Samaniego, M. D. C. (2025). Ciberseguridad y ciudadanía digital: Desafíos en la formación de adolescentes en Ecuador. *Revista Científica Arbitrada Multidisciplinaria PENTACIENCIAS*, *7*(5), 354-363. https://doi.org/10.59169/pentaciencias.v7i5.1669

Guillén, A. (2025). *La Alfabetización Digital en el ejercicio de la Docencia del Centro Educativo San Francisco De Asís*.

https://repositorio.usam.ac.cr/xmlui/handle/111506/localhost/xmlui/handle/111506/3059

Herrera, D., Mendoza, T., León, L., Zambrano, M., & Nuñez, A. (2025). La importancia de la educación en ciberseguridad para niños. *593 Digital Publisher CEIT*, *10*(Extra 1), 5-19. https://dialnet.unirioja.es/servlet/articulo?codigo=9988539

López, K., Rivadeneira, R., & Muñoz, M. F. C. (2025). Artículo Aplicación de la metodología Design Thinking en el aula para la prevención de delitos cibernéticos en Colegios. *Revista Conrado*, *21*(S1), e4820-e4820. https://conrado.ucf.edu.cu/index.php/conrado/article/view/4820

Medina, F. E. (2025). *Evaluación de la ciberseguridad y privacidad en instituciones educativas de los niveles Primario y secundario en Trenque Lauquen, provincia de Buenos Aires*. https://repositorio.21.edu.ar/handle/ues21/29950

Mejía, R. (2026). *Competencia digital, inteligencia artificial y ecosistemas rducativos del futuro*. 1-554. https://www.torrossa.com/en/resources/an/6214225

Montilla, M., & Omar, V. (2025). *Análisis de los principales riesgos de ciberseguridad en los estudiantes de básica secundaria en Colombia*. http://repository.unad.edu.co/handle/10596/75514

Orellana, P., & Moran, J. (2025). *Auditoría de ciberseguridad y detección de vulnerabilidades en plataformas de edutainment: Un enfoque para la protección de datos sensibles y el fortalecimiento de la privacidad* [masterThesis]. http://dspace.ups.edu.ec/handle/123456789/31411

Perez, J. M. O., & Zapata, S. G. (2025). *PLATAFORMA EDUCATIVA BASADA EN MOODLE CON HERRAMIENTAS DE GAMIFICACIÓN PARA PROMOVER LA CONCIENCIACIÓN Y*

CAPACITACION EN CIBERSEGURIDAD EN VARIAS INSTITUCIONES EDUCATIVAS DE MEDELLÍN.

Ramos, N. R., Johnson, G. L. L., Alvia, L. E. R. R. de, & Jiménez, J. A. M. (2025). Control tecnológico para gestión de riesgos en aulas de innovación pedagógica: Revisión conceptual. *Revista Simón Rodríguez*, *5*(10), 487-498. https://doi.org/10.62319/simonrodriguez.v.5i10.79

Rodríguez, V. G., & Jimenez, S. C. E. (2026). Conciencia y Prácticas en Ciberseguridad en Bachillerato: Análisis Temático para Intervenciones Educativas. *Ciencia Latina Revista Científica Multidisciplinar*, *10*(1), 5941-5955. https://doi.org/10.37811/cl_rcm.v10i1.22706

Solano, A. Y. V., Hernández, L. D. C., & Camelo, G. E. H. (2025). Educación digital responsable para la prevención de delitos informáticos en Bucaramanga, Colombia. *Ciencia y Educación*,

6(11), 239-247. https://doi.org/10.5281/zenodo.17926163

Starnari, B. F., Queiruga, C., Venosa, P., & Díaz, J. (2025). CTF en escuelas secundarias 2.0: Una plataforma para la organización de competencias de ciberseguridad escolares. *JAIIO, Jornadas Argentinas de Informática*, *11*(8), 269-283. https://revistas.unlp.edu.ar/JAIIO/article/view/19963

Suárez, C. (2025). *Gamificación para el desarrollo de habilidades cognitivas en Ciberseguridad* [masterThesis]. http://dspace.ups.edu.ec/handle/123456789/30593

Tolaba, G. P. (2025). *Prevención del bullying en el INSM: Fortalecimiento de la convivencia y la ciudadanía digital*. https://repositorio.21.edu.ar/handle/ues21/30541

Tulimirović, B., & Jiménez, E. G. (2026). *Pedagogías para un futuro sostenible*. Dykinson.

Vega, A. (2026). *Análisis de la ejecución y cumplimiento normativo de las políticas de ciberseguridad en la educación pública y privada en bogotá, 2010-2025*. https://hdl.handle.net/10882/18995

CIBERSEGURIDAD PARA DOCENTES

Guía Práctica para la Protección del **Aula Digital**

Live Working EDITORIAL

ISBN: 978-9942-580-57-3