Artículo de revisión

Revista de Educación Simón Rodríguez

www.revistasimonrodriguez.org

Vol. 5 | No. 10 | Agosto 2025 - Enero 2026 | ISSN: 3006-1385 | ISSN-L: 3006-1385 | Pág. 132 - 142

Educación segura en la era digital, aprendizajes desde la ISO 27002:2022: una revisión sistemática

Secure education in the digital age, lessons from ISO 27002:2022: a systematic review

Jonathan Alexis Puente Zamora
jpuentez@ucvvirtual.edu.pe
https://orcid.org/0009-0007-1034-1617
Universidad César Vallejo. Lima, Perú

Darwin Leonel Atarama Vásquez
dlatarama@ucvvirtual.edu.pe
https://orcid.org/0000-0001-9876-9632
Universidad César Vallejo. Lima, Perú

Juan Marcos Vilchez Canchari
jvilchezca987@ucvvirtual.edu.pe
https://orcid.org/0000-0002-7758-7589
Universidad César Vallejo. Lima, Perú

Marlon Frank Acuña Benites
macunabe@ucvvirtual.edu.pe
https://orcid.org/0000-0001-5207-9353
Universidad César Vallejo. Lima, Perú

Roberto Juan Tejada Ruiz
truizr@ucvvirtual.edu.pe
https://orcid.org/0000-0003-3669-836X
Universidad César Vallejo. Lima, Perú

Artículo recibido 29 de abril de 2025 /Arbitrado 30 de mayo de 2025 /Aceptado 15 de julio 2025 /Publicado 15 de septiembre de 2025

https://doi.org/10.62319/simonrodriguez.v.5i10.55

RESUMEN

La ciberseguridad es un componente esencial para garantizar el derecho a aprender en entornos digitales. Este estudio tiene como objetivo analizar críticamente la viabilidad de transponer los controles de la norma ISO/IEC 27002:2022 a un marco de competencias educativas en ciberseguridad para fortalecer la resiliencia digital en la escuela pública peruana. Mediante una revisión sistemática de la literatura siguiendo las directrices PRISMA 2020, incluyéndose 11 documentos para la revisión final. Los resultados evidencian que la norma organiza prácticas dispersas y fortalece la confianza institucional, pero su implementación enfrenta limitaciones estructurales vinculadas con infraestructura tecnológica, cultura digital y ausencia de políticas públicas específicas y que la seguridad no es solo un requisito técnico, sino un aprendizaje pedagógico que forma ciudadanía digital y resiliencia escolar. Se concluye que la novedad radica en concebir la seguridad digital como un bien educativo preventivo, integrando normas internacionales, políticas nacionales y apropiación pedagógica para construir una educación segura en la era digital.

Palabras clave:
Ciberseguridad educativa; Educación digital; ISO 27002; Perú; Resiliencia digital.

ABSTRACT

Cybersecurity is an essential component for guaranteeing the right to learn in digital environments. This study aims to critically analyze the feasibility of transposing the controls of the ISO/IEC 27002:2022 standard into a cybersecurity educational competency framework to strengthen digital resilience in Peruvian public schools. This study conducted a systematic literature review following the PRISMA 2020 guidelines, including 11 documents for the final review. The results show that the standard organizes disparate practices and strengthens institutional trust, but its implementation faces structural limitations linked to technological infrastructure, digital culture, and the absence of specific public policies. It also shows that security is not only a technical requirement but a pedagogical learning process that fosters digital citizenship and school resilience. It is concluded that the novel approach lies in conceiving digital security as a preventive educational asset, integrating international standards, national policies, and pedagogical ownership to build safe education in the digital age.

Keywords:
Educational cybersecurity; Digital education; ISO 27002; Peru; Digital Resilience.

INTRODUCCIÓN

La educación contemporánea enfrenta un doble reto: innovar digitalmente y, al mismo tiempo, garantizar que esa innovación sea segura. Las instituciones educativas ya no solo custodian cuadernos y registros impresos; gestionan bases de datos que contienen información sensible de estudiantes, familias y docentes. La exposición de esos sistemas a vulneraciones informáticas compromete derechos fundamentales y afecta directamente la confianza pedagógica. De ahí que la seguridad de la información haya dejado de ser un asunto meramente técnico para convertirse en un problema central en la gobernanza educativa (Corozo, 2023).

La norma ISO 27002:2022 de la Organización Internacional de Normalización o Estandarización (2022), constituye una referencia internacional para ordenar buenas prácticas de seguridad digital, abarcando desde la gestión de identidades hasta la protección en la nube. Sin embargo, su incorporación en instituciones educativas públicas revela tensiones: por un lado, ofrece un marco sólido y actualizado; por otro lado, su implementación tropieza con brechas de infraestructura, de capacitación docente y de cultura digital. Esta paradoja se hace evidente en sistemas como el peruano, donde el discurso sobre transformación educativa digital avanza con fuerza, pero la seguridad informática se percibe todavía como un requisito externo y no como parte integral del derecho a la educación (Caballero et al., 2023).

La seguridad digital en la educación exige reconocer que no se trata de un campo nuevo, sino de un terreno que ha ido ganando complejidad a medida que la digitalización se volvió central en los sistemas escolares y universitarios. Somepalli et al. (2020), Mirtsch et al. (2021) y Bruce (2025), describen a la seguridad como innovación preventiva, gobernanza, proceso y como auditoría efectiva que añade responsabilidad.

Las primeras aproximaciones estaban ligadas a la gestión tecnológica: proteger servidores, asegurar accesos, instalar antivirus. Sin embargo, en la última década, la discusión se ha desplazado hacia dimensiones pedagógicas, éticas y sociales. Para Tomczyk y Potyrała (2021), la escuela ya no puede limitarse a ser consumidora de tecnología, sino que debe convertirse en un agente formador de competencias digitales seguras. En este sentido, la norma ISO 27002:2022, aunque concebida para organizaciones de todo tipo, adquiere una relevancia particular en el campo educativo, pues su adopción puede traducirse en aprendizajes institucionales que trascienden la técnica y tocan directamente la fenomenología educativa (Amine et al., 2023).

Desde la perspectiva normativa, la ISO 27002:2022 es el resultado de una evolución de estándares que, en sus primeras versiones, se enfocaban en controles técnicos, pero que hoy incluyen principios de gobernanza, cultura organizacional y gestión de riesgos emergentes (Bustamante et al., 2021). Así, da Silva et al. (2025), subraya que esta actualización refleja un cambio de paradigma: pasar de un enfoque centrado en el cumplimiento formal a otro orientado a la resiliencia. Para el ámbito educativo, esto significa que la norma no debe verse solo como un requisito burocrático, sino como un marco que ayuda a construir confianza digital en toda la comunidad escolar.

Diversos estudios regionales han documentado el incremento de ciberataques dirigidos contra instituciones educativas, motivados por la vulnerabilidad de sus sistemas y por el valor de la información que gestionan; Guaña (2023), señala que la exposición de datos estudiantiles afecta no solo la privacidad, sino también la credibilidad institucional, lo que impacta en la continuidad de los procesos de enseñanza-aprendizaje. En contextos de precariedad, como ocurre en gran parte de América Latina, los riesgos se multiplican porque la inversión en seguridad digital suele considerarse secundaria frente a otros gastos urgentes. De ahí que Mohamed Hashim et al. (2022), consideren que el estado de la cuestión muestre un

vacío: mientras la transformación digital es un tema recurrente en políticas educativas, la seguridad de esa digitalización recibe menos atención normativa y académica.

El vacío teórico se amplía al observar que pocos estudios integran la seguridad digital con categorías pedagógicas como confianza, resiliencia o fenomenología educativa. La mayoría de los análisis técnicos se enfocan en controles y procedimientos, pero dejan de lado la pregunta por cómo esos mecanismos se traducen en aprendizajes. Hidalgo et al. (2022), documenta la importancia de capacitar al personal en el manejo seguro de contraseñas y accesos, pero rara vez se problematiza que enseñar a proteger la información puede convertirse en una práctica pedagógica transversal, que fomente ciudadanía digital y ética del cuidado en los estudiantes. Este hallazgo sugiere un terreno fértil para la innovación: situar la seguridad de la información no como un tema externo a la educación, sino como parte del currículo y de la cultura escolar.

En relación con la fenomenología educativa, los estudios psicosociales muestran que los incidentes de seguridad no son neutrales, pues afectan el clima institucional y la percepción de confianza. Un estudiante que percibe que su institución no protege adecuadamente su información se siente menos seguro para interactuar en plataformas digitales, lo que puede limitar su participación y aprendizaje. Sousa y Dias (2025), destacan que la implementación de estándares de seguridad no solo protege datos, sino que reduce la ansiedad digital y fortalece la percepción de legitimidad de la institución. Desde esta perspectiva, la ISO 27002:2022 debe entenderse como un instrumento pedagógico indirecto, pues crea condiciones de confianza que impactan directamente en el aprendizaje.

Se reporta, además, la importancia de la resiliencia digital. En contextos de crisis, como la pandemia de COVID-19, las instituciones con marcos de seguridad consolidados lograron sostener la continuidad de sus procesos educativos con menos interrupciones. En cambio, las escuelas que carecían de protocolos de seguridad vieron multiplicarse los riesgos: accesos no autorizados, pérdidas de información y dificultades para garantizar la privacidad en entornos virtuales. Wibowo et al. (2025), concluyen que la resiliencia educativa no depende solo de plataformas tecnológicas, sino de la capacidad de gestionar riesgos y responder a incidentes. Para países como el Perú, donde las desigualdades estructurales son profundas, se reconoce que sin seguridad digital, la innovación tecnológica corre el riesgo de convertirse en un factor que amplía las brechas en lugar de reducirlas (Rodríguez, 2024).

De ahí que, la actualización ISO 27002:2022 sea relevante en educación por su reorganización en 93 salvaguardas agrupadas en categorías, organizacional, factor humano, físico y tecnológico, lo que facilita mapear roles y rutinas escolares; quién accede a qué, cómo se protege físicamente, cómo se opera y qué se registra (Brezavšček y Vidmar, 2023). Sin embargo, la adopción de la ISO 27002:2022 en el sector educativo de América Latina y Perú enfrenta notorias limitaciones. La principal es la brecha de recursos, donde instituciones públicas y privadas carecen del presupuesto para implementar los controles técnicos y organizativos requeridos (Marques et al., 2024). Sumado a esto, existe una escasa cultura de ciberseguridad y una percepción de que es un lujo, no una necesidad. Esta norma, al ser un marco genérico, no considera las realidades específicas de infraestructura tecnológica precaria y la alta heterogeneidad de sistemas educativos en la región, dificultando su aplicación práctica y efectiva (Rumiche, 2022).

Teniendo en cuenta este contexto, se requiere cuestionarse ¿cómo pueden los controles de la ISO/IEC 27002:2022 configurar un modelo pedagógico de ciber-resiliencia para el ecosistema educativo público peruano?, ¿qué lecciones de política educativa en ciberseguridad pueden derivarse del análisis comparado entre sistemas de common law y civil law? De ahí que el objetivo de este artículo de revisión sistemática fue analizar críticamente la viabilidad de transponer los controles de la norma ISO/IEC 27002:2022 a un marco de competencias educativas en ciberseguridad para fortalecer la resiliencia digital en la escuela pública peruana.

METODOLOGÍA

Para la presente investigación se empleó una revisión sistemática de la literatura, siguiendo las directrices de la declaración PRISMA 2020 (Preferred Reporting Items for Systematic Reviews and Meta-Analyses). Este método permite asegurar la transparencia, rigurosidad y replicabilidad del proceso de búsqueda, selección y síntesis de la evidencia científica.

La estrategia de búsqueda se diseñó para identificar estudios relevantes en las bases de datos académicas Scopus, Web of Science y Google Scholar. Se utilizaron términos de búsqueda en español e inglés, combinando palabras clave como "seguridad de la información", "educación digital", "ISO 27002", "riesgos digitales en escuelas", "ciberseguridad en educación", "information security", "digital education", "cybersecurity in schools", y "educational data protection".

1. Scopus

sql

(TITLE-ABS-KEY ("information security" OR "cybersecurity" OR "information security" OR "educational data protection") AND TITLE-ABS-KEY ("digital education" OR "schools" OR "k-12" OR "educational institution*") AND TITLE-ABS-KEY ("ISO 27002" OR "risk management" OR "risk assessment" OR "digital risks")) AND (LIMIT-TO (LANGUAGE , "English") OR LIMIT-TO (LANGUAGE , "Spanish"))

- Tipo de Documento: Article, Review, Conference Paper.
- Área Temática: Social Sciences, Computer Science.

2. Web of Science (WoS)

sql

(TS=(("information security" OR "cybersecurity" OR "information security" OR "data protection") AND ("digital education" OR "school*" OR "k-12" OR "primary education" OR "secondary education") AND ("ISO 27002" OR "risk management" OR "risk assessment" OR "digital risk*"))) AND LA=(English OR Spanish)

- Año: 2022 al 2025.
- Tipo de Documento: Article, Review, Proceedings Paper.
- Categorías de WoS: Education Educational Research, Computer Science Information Systems, Management.

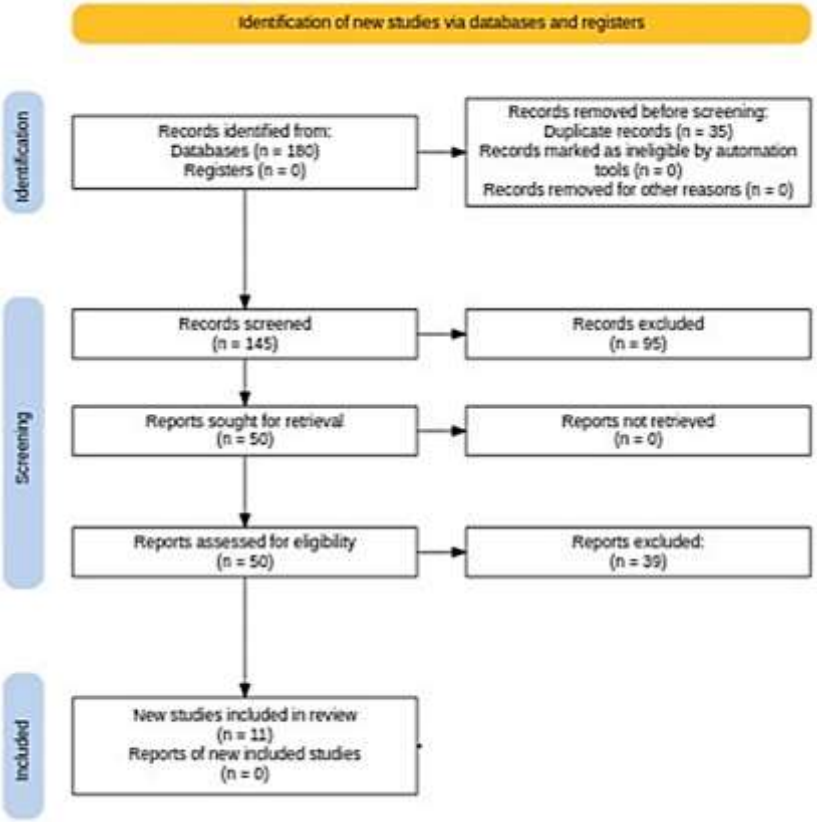
3. Google Académico (Google Scholar)

    - Sql "information security" "digital education" "ISO 27002" school
    - Sql cybersecurity education "risk assessment" "K-12"
    - Sql "seguridad de la información" "educación digital" "riesgos digitales" escuelas

Los criterios de inclusión para la selección de los estudios fueron: (a) artículos de investigación, revisiones y capítulos de libros publicados entre 2020 y 2025; (b) estudios que abordaran la seguridad de la información en el contexto educativo, con especial interés en la educación básica y media; (c) trabajos que analizaran la implementación de estándares de seguridad como la familia ISO 27000; y (d) investigaciones que discutieran los riesgos y desafíos de la digitalización en la educación. Se excluyeron artículos de opinión, noticias y estudios no revisados por pares.

La selección de los estudios se llevó a cabo siguiendo la metodología PRISMA, la cual se representa de manera visual en un diagrama de flujo (Figura 1). Inicialmente, dos evaluadores analizaron de forma independiente los títulos y resúmenes de todos los registros obtenidos en la búsqueda bibliográfica. Los artículos que, tras esta revisión inicial, parecían cumplir con los criterios de inclusión, pasaron a una fase de evaluación de texto completo. La elegibilidad final de cada estudio se determinó tras este examen exhaustivo. En caso de surgir discrepancias entre los revisores, estas se resolvieron mediante debate hasta alcanzar un consenso o, de ser necesario, con la consulta a un tercer investigador. Siguiendo este proceso se incluyeron 11 artículos para su estudio.

Figura 1. *Diagrama de flujo para la selección de los artículos según PRISMA*



La extracción de datos de los estudios incluidos se realizó utilizando una plantilla prediseñada, que recogía información sobre: autor(es) y año de publicación, país del estudio, tipo de institución educativa, metodología empleada, principales hallazgos y conclusiones. La síntesis de la información se realizó de forma narrativa, organizando los resultados en torno a los ejes temáticos definidos en la introducción: ambigüedad normativa, riesgos psicoeducativos, experiencias comparadas e innovaciones preventivas.

RESULTADOS

El análisis documental realizado permitió identificar un conjunto de resultados que ilustran tanto los alcances como las limitaciones de la implementación de la ISO 27002:2022 en el contexto de una institución educativa pública de Piura. Estos resultados se organizan en tres ejes: la identificación de beneficios inmediatos, la visibilización de obstáculos estructurales y la proyección comparada hacia sistemas educativos con mayor madurez digital.

Se constató que la norma ofrece un marco de referencia que ordena prácticas ya conocidas, pero que en muchos casos no estaban sistematizadas en las instituciones. Por ejemplo, la gestión de accesos y contraseñas, la delimitación de permisos de usuario y la importancia de contar con planes de respuesta ante incidentes eran prácticas dispersas que, bajo la guía de la ISO 27002:2022, adquirieron coherencia y jerarquía. En el caso de Piura, Aznar et al. (2024), plantean que los directivos reportaron que el uso de controles estandarizados contribuyó a mejorar la percepción de confianza entre docentes y personal administrativo, al demostrar que existía un plan claro para proteger datos sensibles de estudiantes.

De igual forma, los resultados de Antunes et al. (2021) y Escurra y Canese (2024), revelan limitaciones significativas. La implementación efectiva de la norma enfrenta barreras relacionadas con la falta de infraestructura tecnológica actualizada, la escasa capacitación de los actores escolares y la ausencia de políticas nacionales que vinculen seguridad de la información con calidad educativa. Existen instituciones, donde los servidores son obsoletos y que gran parte del almacenamiento se realiza en dispositivos personales de docentes, lo que expone los datos a riesgos de pérdida o filtración. Asimismo, Latorre y Tnibar (2023), consideran que las capacitaciones recibidas son esporádicas y más centradas en aspectos técnicos que en la comprensión pedagógica de la seguridad digital. Esta constatación refuerza la idea de que el problema no es únicamente técnico, sino cultural: sin una apropiación educativa, la norma corre el riesgo de convertirse en un requisito formal de difícil sostenibilidad.

Del mismo modo, el contraste con experiencias comparadas evidenció que los países con marcos regulatorios más sólidos y con inversiones sostenidas en seguridad digital educativa mostraron mayor resiliencia frente a crisis. Silva et al. (2020), documentan que en sistemas europeos la integración de estándares de seguridad en políticas nacionales permitió sostener la continuidad pedagógica incluso en contextos de disrupción como la pandemia de COVID-19. En cambio, en Perú y otros países latinoamericanos, la falta de articulación entre seguridad y educación dejó a muchas instituciones expuestas a incidentes que comprometieron la privacidad de los estudiantes y la estabilidad de los procesos formativos (Constante, 2025). Este hallazgo marca una diferencia crítica: la ISO 27002:2022 puede ser útil, pero su impacto depende de la existencia de una política pública que lo respalde y lo traduzca en recursos efectivos para las escuelas.

Así mismo, Ahmedi y Ibrahimi (2024), evidencian que la seguridad digital debe concebirse como parte del derecho a la educación. Si los estudiantes no tienen garantía de que sus datos están protegidos, su experiencia formativa se desarrolla en un entorno de vulnerabilidad que erosiona la confianza. Aquí la fenomenología educativa se cruza con la gestión de datos: la seguridad no es un añadido técnico, sino una condición de posibilidad para que el aprendizaje ocurra con tranquilidad y continuidad.

Por otro lado, los hallazgos de Gavidia (2023) y Paspuel y Pablo (2024), muestran que cada control de la ISO 27002:2022 puede convertirse en un aprendizaje pedagógico. Enseñar a los estudiantes a gestionar contraseñas seguras no solo reduce riesgos, sino que educa en responsabilidad digital. Delimitar los accesos según roles no es solo administración técnica, sino también un ejercicio de ética y confianza. Diseñar planes de respuesta ante incidentes no es únicamente cumplir con un protocolo, sino educar en prevención y resiliencia. Esta lectura pedagógica transforma la norma en una herramienta de formación ciudadana en el ámbito digital.

Por ello, se resalta que el impacto de la norma no puede evaluarse únicamente desde indicadores técnicos de cumplimiento. Pata Atarama (2024), resulta más relevante aún es medir cómo su implementación influye en el clima institucional, en la percepción de confianza de las familias y en la continuidad de los aprendizajes. En el caso de la institución de Piura, los docentes expresaron que, a pesar de las carencias de infraestructura, el solo hecho de contar con lineamientos claros redujo la ansiedad frente a incidentes pasados de pérdida de datos. Este dato sugiere que la seguridad digital tiene también un componente emocional y

cultural que debe integrarse a las políticas educativas.

Finalmente, para Andrade et al. (2024), la discusión prospectiva muestra que el futuro de la educación segura dependerá de la capacidad de articular tres dimensiones: el marco normativo internacional (ISO 27002:2022), la política pública nacional y la apropiación pedagógica local. Ninguna de estas dimensiones, por sí sola, garantiza resiliencia. La norma sin política se queda en el papel; la política sin apropiación escolar se convierte en burocracia ineficaz; la apropiación local sin marco normativo puede caer en improvisación. Solo la convergencia de estas tres dimensiones permitirá construir una educación segura en la era digital, capaz de prevenir riesgos y de fortalecer la confianza social en la escuela pública.

DISCUSIÓN

En este estudio se evidencia que los continuos procesos de transformación tecnológica actúan como una espada de doble filo dentro del ámbito educativo. Por un lado, ofrecen oportunidades inéditas para expandir el acceso, la comunicación y las formas de aprendizaje; pero, por otro, generan vulnerabilidades que ponen en riesgo la integridad de la información personal, institucional y financiera de quienes participan en estos entornos. Autores como Li y Zhang (2025), coinciden en que la seguridad no puede ser vista como un componente técnico aislado, sino como un aspecto transversal que conecta con la confianza, la ética y la responsabilidad social de las instituciones educativas.

Los hallazgos sugieren que la creciente digitalización de los procesos educativos obliga a replantear no solo las infraestructuras tecnológicas, sino también la cultura institucional en torno a la protección de datos y la ciberseguridad. Se coincide con el criterio de Paspuel y Pablo (2024), quienes plantean que la adopción de normas como la ISO/IEC 27002 (2022), presentada por se presenta como un recurso valioso, pero su sola implementación no garantiza resultados tangibles si no se acompaña de formación constante del personal docente y administrativo, así como de una pedagogía digital que enseñe a estudiantes y familias a reconocer los riesgos y a proteger activamente sus datos.

Cabe destacar, además, que las vulnerabilidades cibernéticas se entrelazan con problemas humanos de mayor amplitud, aspecto que concuerda con Mar et al. (2024), para quienes la introducción de la tecnología en los espacios educativos ha favorecido nuevas profesiones, pero también ha incrementado la incertidumbre laboral y revelado dilemas éticos que van desde el uso responsable de la inteligencia artificial hasta el respeto por la privacidad digital de los estudiantes. En este sentido, los hallazgos de la presente edición concuerdan con Serrano (2021), cuando postula que la seguridad en la educación digital debe entenderse no solo como resguardo de sistemas, sino como condición básica para defender derechos, dignidad e igualdad de oportunidades en una sociedad marcada por la aceleración tecnológica.

En este sentido, los resultados de esta revisión sistemática confirman que la seguridad de la información en entornos educativos no puede ser concebida como un aspecto periférico, sino como un elemento estructural de la calidad y sostenibilidad de la educación digital, aspectos que son validados por Morales et al. (2024). En esta misma línea se concuerda con Cali y Álava (2025), quienes exponen que el análisis de los conceptos clave y de los marcos normativos actualmente vigentes, como la familia ISO/IEC 27000, plantea un marco de referencia sólido para comprender cómo se construye una educación segura y qué desafíos enfrentan las instituciones al respecto.

De igual forma, la revisión evidenció que, aunque existe un desarrollo robusto en la normativa internacional, los estudios específicos en educación todavía son incipientes. Este hallazgo resulta revelador, mientras los sectores productivos y financieros avanzan rápidamente en la implementación de sistemas de ciberseguridad, el ámbito educativo, como plantea Gavidia (2023), sigue rezagado, dejando expuestas brechas

importantes. Este desfase, como plantea Guaña (2023), no solo compromete la confidencialidad de la información académica y administrativa, sino que también puede afectar el bienestar de las comunidades educativas, donde circula información altamente sensible, incluyendo datos personales, de salud y financieros.

El hecho de que las experiencias documentadas de implementación de la norma ISO/IEC 27002 (2022) en instituciones educativas sean escasas resalta una oportunidad de evolución para el sector. Se concuerda con Saquisari (2025), quien plantea que las prácticas ya probadas en organizaciones de otros campos pueden servir como guía práctica para diseñar políticas educativas que protejan los datos y garanticen entornos confiables de aprendizaje digital. De este modo, lo que en un inicio parece un reto técnico, en realidad se traduce en una responsabilidad ética y social para los gestores educativos, quienes deben armonizar las innovaciones de la era digital con la seguridad y la dignidad de las personas.

De esta manera, la revisión sistemática realizada ratifica que la seguridad y la privacidad en línea figuran como derechos sustantivos amparados por instrumentos internacionales postulados por las Naciones Unidas (2006), como la Convención sobre los Derechos del Niño de las Naciones Unidas, que, en sus artículos 7 y 10, establece el acceso a entornos protegidos como una obligación fundamental de los Estados y las instituciones educativas. Sin embargo, los resultados obtenidos muestran que la distancia entre los principios normativos y la práctica cotidiana en entornos digitales es significativa y preocupante, especialmente para niñas, niños y adolescentes, considerados sujetos de especial protección por la comunidad internacional, lo que concuerda con Ordóñez y Valdivieso (2023). Las vulnerabilidades detectadas en el uso de plataformas educativas dejan entrever que la afirmación de estos derechos, más que una realidad material, sigue siendo una aspiración pendiente en muchos contextos.

Se concuerda con Alvarado et al. (2024), quienes plantean que el derecho al respeto de la privacidad y la protección de la intimidad es esencial para el equilibrio emocional y el desarrollo psicosocial, y exige respuestas institucionales firmes e innovadoras. Aunque la Declaración Universal de Derechos Humanos subrayó la importancia de estos principios hace más de medio siglo, la aceleración digital y la incorporación masiva de tecnología en la educación han creado escenarios inéditos que obligan a repensar su aplicación. Los datos sugieren que las amenazas actuales no solo ponen en entredicho la seguridad de los sistemas, sino que pueden tener repercusiones en el bienestar y la confianza de toda una generación de estudiantes, quienes ven en la escuela un espacio de protección que debe actualizarse frente a los retos tecnológicos.

En consecuencia, la sistematización de los problemas vinculados a la seguridad y la privacidad en la educación digital es un paso ineludible para evaluar si los compromisos establecidos por normas, convenciones y acuerdos internacionales se cumplen de manera efectiva. Solo mediante un control riguroso y una actualización permanente de las prácticas institucionales se podrá garantizar la materialización de los derechos de la infancia y la adolescencia en el contexto educativo actual (Lara-Jaramillo y Romero-Romero, 2023). Este ejercicio no solo atiende una exigencia legal, sino que responde a una deuda ética y social con las generaciones más jóvenes, demandando una mirada crítica, humana y comprometida con la transformación real de la experiencia educativa.

En definitiva, la contrastación con otros autores confirma la evidencia generada por el análisis de los estudios incluidos en la revisión, la discusión plantea que la educación digital no puede desligarse de su dimensión de seguridad. Cada avance tecnológico conlleva un riesgo inherente, y la única manera de reducirlo es integrando la normativa, la formación docente y la sensibilización estudiantil en una estrategia integral. No se trata solo de cumplir requisitos normativos, sino de generar confianza y proteger los derechos de quienes participan en el hecho educativo. Esa es la base para avanzar hacia una educación segura, inclusiva y sostenible en el contexto de transformación acelerada que caracteriza al siglo XXI.

CONCLUSIONES

La presente revisión sistemática ha permitido analizar en profundidad el impacto de la norma ISO 27002:2022 en la gestión de la seguridad de la información en el contexto educativo, con un enfoque particular en la realidad de la escuela pública peruana. La principal conclusión de este estudio es que la seguridad digital, más allá de ser un requisito técnico, debe ser concebida como un bien educativo de carácter preventivo, cuya implementación es fundamental para garantizar el derecho a una educación de calidad en la era digital.

La adopción de estándares internacionales como la ISO 27002:2022 es un paso necesario, pero no suficiente. Para que estos marcos normativos sean efectivos, deben ir acompañados de políticas públicas que aborden las brechas de infraestructura, promuevan la formación docente en competencias digitales y fomenten una cultura de seguridad en toda la comunidad educativa. La novedad de este trabajo radica en proponer una visión integral de la seguridad digital que articula la dimensión normativa, tecnológica y pedagógica.

Finalmente, se destaca la importancia de la resiliencia digital como un componente esencial de la calidad educativa. La capacidad de las instituciones para anticipar, resistir y recuperarse de los incidentes de seguridad es un indicador clave de su madurez institucional. En este sentido, la inversión en ciberseguridad no solo protege la información, sino que también fortalece la confianza y la legitimidad del sistema educativo en su conjunto. Las futuras líneas de investigación deberían explorar, a través de estudios de caso, las experiencias de apropiación pedagógica de los estándares de seguridad en diferentes contextos educativos.

CONFLICTO DE INTERESES

Los autores declaran que no existe conflicto de intereses para la publicación del presente artículo científico.

REFERENCIAS

Ahmedi, B. y Ibrahimi, A. (2024). Mastering information security through standard implementation. International Journal of Informatics Communication Technology, 13(3), 428-435. https://doi.org/10.11591/ijict.v13i3.pp428-435

Alvarado, N. A., Solórzano, J. J. y Martínez, O. (2024). El derecho a la intimidad en el entorno laboral, desafíos en el ordenamiento jurídico ecuatoriano. *Revista Lex*, *7*(27), 1625-1639. https://doi.org/10.33996/revistalex.v7i27.266

Amine, A. M., Chakir, E. M., Issam, T. y Khamlichi, Y. I. (2023). A Review of Cybersecurity Management Standards Applied in Higher Education Institutions. *International Journal of Safety Security Engineering*, *13*(6). https://doi.org/10.18280/ijsse.130614

Andrade, F., Alarcon, J. C., Ortega, X. F. y González, J. L. (2024). Teoría general de sistemas: un enfoque estratégico para la planificación institucional. *Revista Venezolana de Gerencia: RVG*, *29*(105), 388-400. https://doi.org/10.52080/rvgluz.29.105.24

Antunes, M., Maximiano, M., Gomes, R. y Pinto, D. (2021). Information security and cybersecurity management: A case study with SMEs in Portugal. *Journal of Cybersecurity Privacy*, *1*(2), 219-238. https://doi.org/10.3390/jcp1020012

Atarama, T. (2024). Pérez García, A., Feijoo Fernández, B. y López Martínez A.(ed.).(2024). Los menores ante las redes sociales. Pensamiento crítico y reflexión ética. *Revista de Comunicación*, *23*(2), 383-385. http://dx.doi.org/10.26441/rc23.2-2024-r1-3031

Aznar, B., Casarramona, A., Grané, J., Lorente, J., Prats, M.-À. y Ballester, L. (2024). Uso responsable de Internet y seguridad digital: revisión sistemática de programas educativos. *Estudios Sobre Educación*, *47*, 125-152. https://doi.org/10.15581/004.47.006

Brezavšček, A. y Vidmar, D. (2023). *Recent changes in the ISO 27000 series of information security standards*. Peter Land. https://doi.org/10.3726/b22722

Bruce, C. V. (2025). Auditoría de sistemas de información para la seguridad y eficiencia organizacional. *Experior*, *4*(1), 3-17. https://doi.org/10.56880/experior41.1

Bustamante, S., Valles, M. Á., Cuellar, I. E. y Lévano, D. (2021). Políticas basadas en la ISO 27001: 2013 y su influencia en la gestión de seguridad de la información en municipalidades de Perú. *Enfoque UTE*, *12*(2), 69-79. https://doi.org/10.29019/enfoqueute.743

Caballero, J. J., Chavez, E. D., Lopez, M. E., Inciso, E. S. y Méndez, J. (2023). Autonomous learning in higher education. Systematic review. *Salud, Ciencia y Tecnología*, *3*, 391-391. https://doi.org/10.56294/saludcyt2023391

Cali, F. E. y Álava, J. E. (2025). Propuesta de la normativa ISO/IEC para la gobernanza de ciberseguridad en el procesamiento de datos críticos. *Sinergia Académica*, *8*(5), 656-677. https://doi.org/10.51736/sa679

Constante, E. M. (2025). *Medidas de seguridad para la protección de datos sensibles de estudiantes y ex estudiantes de Uniandes* [Magíster en cumplimiento, lavado de activos y protección de datos Universidad Regional Autónoma de Los Andes "Uniandes"]. Ambato - Ecuador. https://dspace.uniandes.edu.ec/bitstream/123456789/18751/1/UA-MCL-EAC-006-2025.pdf

Corozo, K. E. (2023). Modelo de evaluación madurez de gestión de seguridad de la información en centros de datos: Information Security Assessment Model for Data Centers. *Cumbres*, *9*(1), 39-50. https://doi.org/10.48190/cumbres.v9n1a3

da Silva, R., de Souza Pinto, J., Zanon, L. G., Sigahi, T. F., Salati, G. H., Moro, S. R. y Anholon, R. (2025). Information security management: a fuzzy DEMATEL analysis of the new ISO/IEC 27001: 2022 controls. *Information Computer Security*. https://doi.org/10.1108/ICS-10-2024-0269

Escurra, M. Á. y Canese, V. (2024). Las Tecnologías de la Información y Comunicación en la Educación Superior Militar en Paraguay. *Revista de Análisis y Difusión de Perspectivas Educativas y Empresariales*, *4*(8), 54-77. https://doi.org/10.56216/radee022024ago.a05

Gavidia, J. V. (2023). Propuesta de modelo en seguridad informática en el control de un sistema informático aplicando ISO 27002 y CSF de NIST. *Revista Ingeniería e Innovación del Futuro*, *2*(1), 41-52. https://doi.org/10.62465/riif.v2n1.2023.10

Guaña, E. J. (2023). La importancia de la seguridad informática en la educación digital: retos y soluciones. *RECIMUNDO: Revista Científica de la Investigación y el Conocimiento*, *7*(1), 609-616. https://dialnet.unirioja.es/servlet/articulo?codigo=8977055

Hidalgo, B. G., Bonilla, J. R. y Rivera, Y. A. (2022). E-learning en el proceso enseñanza aprendizaje en la educación superior: una revisión de la literatura: E-learning in the teaching and learning process in higher education: a literature review. *Revista Científica Ecociencia*, *9*(2), 1-29. https://doi.org/10.21855/ecociencia.92.619

Latorre, M. J. y Tnibar, C. (2023). Digital Security in Educational Training Programs: A Study based on Future Teachers' Perceptions. *Information technologies learning tools*, *95*(3), 102-111. https://doi.org/10.33407/itlt.v95i3.5204

Li, Z. y Zhang, W. (2025). Technology in education: Addressing legal and governance challenges in the digital era. *Education Information technologies learning tools*, *30*(7), 8413-8443. https://doi.org/10.1007/s10639-024-13036-9

Mar, O., Rodríguez, A., Solórzano, W. L., Amén, P. G., Santos, L. M. y Pinargote, B. J. J. (2024). La Inteligencia Artificial: desafíos para la educación. *Editorial Internacional Alema*. https://editorialalema.org/libros/index.php/alema/article/view/34/33

Marques, D. A., Schmitzi, D. y Amilkar, K. (2024). Framework for Security Risk Assessment (FSRA) and Fuzzy Risk Inference System (FRIS) based on Standard ISO/IEC 27002: 2022. *Revista de Informática Teórica e Aplicada*, *31*(2), 43-55. https://doi.org/10.22456/2175-2745.136309

Mirtsch, M., Blind, K., Koch, C. y Dudek, G. (2021). Information security management in ICT and non-ICT sector companies: a preventive innovation perspective. computers and security, 109: 102383. *Computers & Security*, *109*. https://doi.org/10.1016/j.cose.2021.102383

Mohamed Hashim, M. A., Tlemsani, I. y Matthews, R. (2022). Higher education strategy in digital transformation. *Education Information technologies learning tools*, *27*(3), 3171-3195. https://doi.org/10.1007/s10639-021-10739-1

Morales, F. I., Medina, J. M. y Rodríguez, O. (2024). Seguridad digital y violencias estructurales: perspectivas y desafíos contemporáneos. *Dilemas contemporáneos: Educación, Política y Valores*. https://doi.org/10.46377/dilemas.v12i.4486

Naciones Unidas. (2006). *Convención sobre los derechos del niño*. UNICEF. https://www.un.org/es/events/childrenday/pdf/derechos.pdf

Ordóñez, L. O. y Valdivieso, G. J. (2023). El derecho a la educación digital: una oportunidad para afianzar un modelo de cultura digital para la paz. *Revista de Cultura de paz, 7*, 123-140. https://doi.org/10.58508/cultpaz.v7.143

Organización Internacional de Normalización o Estandarización. (2022). *ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection — Information security controls*. ISO. https://www.iso.org/obp/ui/es/#iso:std:iso-iec:27002:ed-3:v2:en

Paspuel, T. y Pablo, J. (2024). *Propuesta de un plan de mitigación de riesgos basado en la evaluación de los controles de la ISO 27002, para la identificación de vulnerabilidades: Caso empresa DIBEAL* [Maestría en Seguridad Informática, Universidad Tecnológica Israel]. Quito, Ecuador. http://repositorio.uisrael.edu.ec/handle/47000/4138

Rodríguez, R. (2024). Brecha digital y transformación social: el impacto de las nuevas tecnologías en América Latina y el Caribe. *Acceso. Revista Puertorriqueña de Bibliotecología y Documentación*, *5*, 29. https://revistas.upr.edu/index.php/acceso/article/view/21537/19143

Rumiche, R. E. (2022). *Implementación de un plan de seguridad informática basado en la norma ISO IEC/27002, para optimizar la gestión en la Corte Superior de Justicia de Lima* [Ingeniero de Sistemas Computacionales, Universidad Privada del Norte]. Lima, Perú. https://hdl.handle.net/11537/29848

Saquisari, A. P. (2025). El impacto de las políticas de privacidad de datos en la confianza de los padres en la educación en línea: un análisis comparativo de diferentes marcos regulatorios. *Revista Política y Ciencias Administrativas*, *4*(1), 119-136. https://doi.org/10.62465/rpca.v4n1.2025.142

Serrano, M. M. (2021). La educación digital constitucional como contenido esencial del derecho fundamental a la educación. *Revista DH/ED: derechos humanos y educación*(4), 113-135. https://dialnet.unirioja.es/servlet/articulo?codigo=8126365

Silva, A., Daza, J. M. y Perkumiené, D. (2020). La regulación de los derechos y obligaciones de carácter no patrimoniales entre los cónyuges en la jurisprudencia española, colombiana y lituana. *Derecho global. Estudios sobre derecho y justicia*, *5*(14), 17-45. https://doi.org/10.32870/dgedj.v5i14.309

Somepalli, S. H., Tangella, S. K. R. y Yalamanchili, S. (2020). Information security management. *Holistica Journal of Business Public Administration*, *11*(2), 1-16. https://doi.org/10.2478/hjbpa-2020-0015

Sousa, G. R. y Dias, E. (2025). Privacy in Chatbot Conversation-Driven Development: A Comprehensive Review and Requirements Proposal. *ACM Transactions on Software Engineering Methodology*, *34*(7). https://doi.org/10.1145/373057

Tomczyk, Ł. y Potyrała, K. (2021). Parents' knowledge and skills about the risks of the digital world. *South African Journal of Education*, *41*(1). https://doi.org/10.15700/saje.v41n1a1833

Wibowo, B., Yuswanto, A., Hidayat, T. y Ibrahim, N. (2025). Cyber Resilience to Digital Threats for Education Institutions 4.0. *International Journal of Management Science Application*, *4*(1), 35-45. https://doi.org/10.58291/ijmsa.v4i1.370