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. 487 - 498

Control tecnológico para gestión de riesgos en aulas de innovación pedagógica: revisión conceptual

Technological control for risk management in educational innovation classrooms: A conceptual review

Nancy Reyes Ramos
p7000081698@ucvvirtual.edu.pe
https://orcid.org/0009-0008-0108-1750
Universidad César Vallejo. Piura, Perú

Gladys Lola Luján Johnson
ljohnsongl@ucvvirtual.edu.pe
https://orcid.org/0000-0002-4727-6931
Universidad César Vallejo. Piura, Perú

Linda Edith Reyes Ramos de Alvia
lereyes@ucvvirtual.edu.pe
https://orcid.org/0000-0001-6615-0405
Universidad César Vallejo. Piura, Perú

Jorge Antonio Mariluz Jiménez
jmariluz@eesppemiliabarcia.edu.pe
https://orcid.org/0000-0002-9895-4042
Escuela de Educación Superior Pedagógica Emilia Barcia Boniffatti. Lima, Perú

Artículo recibido 11 de septiembre de 2025 /Arbitrado 09 de octubre de 2025 /Aceptado 06 de noviembre 2025 /Publicado 27 de noviembre de 2025

https://doi.org/10.62319/simonrodriguez.v.5i10.79

RESUMEN

La transformación digital educativa global posiciona el control tecnológico como estrategia crítica para gestión de riesgos en aulas de innovación pedagógica. El objetivo del estudio es analizar las dimensiones teóricas del control tecnológico como estrategia para la gestión de riesgos en aulas de innovación pedagógica. Métodos: Se realizó revisión teórica conceptual mediante búsqueda sistemática en SciELO y bases internacionales, priorizando estudios 2015-2024 sobre tecnología educativa, gestión de riesgos digitales y gobernanza digital. El análisis siguió codificación temática para identificar dimensiones conceptuales emergentes. Los resultados arrojaron cinco dimensiones principales del control tecnológico educativo: políticas y normativas institucionales, mecanismos de supervisión y monitoreo, gestión preventiva de riesgos, respuesta y mitigación de incidentes, y capacidades institucionales especializadas. Cada dimensión integra componentes específicos que operacionalizan el constructo teórico multidimensional. Se concluye que el control tecnológico constituye un elemento estratégico en la modernización del Estado educativo, requiriendo enfoques multidimensionales que garanticen tanto la innovación pedagógica como la seguridad digital.

Palabras clave:
Control tecnológico; Innovación; Gestión de riesgos; Gobernanza digital; Modernización del Estado

ABSTRACT

The global digital transformation of education positions technological control as a critical strategy for risk management in pedagogically innovative classrooms. The objective of this study is to analyze the theoretical dimensions of technological control as a strategy for risk management in pedagogically innovative classrooms. Methods: A theoretical and conceptual review was conducted through a systematic search of SciELO and international databases, prioritizing studies from 2015-2024 on educational technology, digital risk management, and digital governance. The analysis followed thematic coding to identify emerging conceptual dimensions. The results yielded five main dimensions of educational technological control: institutional policies and regulations, oversight and monitoring mechanisms, preventive risk management, incident response and mitigation, and specialized institutional capacities. Each dimension integrates specific components that operationalize the multidimensional theoretical construct. It is concluded that technological control constitutes a strategic element in the modernization of the educational state, requiring multidimensional approaches that guarantee both pedagogical innovation and digital security.

Keywords:
Technological control; Innovation; Risk management; Digital governance; State modernization

INTRODUCCIÓN

La transformación digital de la educación ha emergido como un paradigma global que redefine los marcos de gestión pública educativa, posicionando el control del uso tecnológico como una estrategia fundamental para la administración de riesgos en entornos de innovación pedagógica (UNESCO, 2022; Rueda y Sousa, 2020). Esta reconfiguración no solo implica la incorporación de herramientas digitales, sino también la necesidad de establecer sistemas de gobernanza que garanticen entornos seguros, éticos y sostenibles para el aprendizaje.

En este escenario internacional, las instituciones educativas enfrentan un incremento exponencial de ciberamenazas, con el sector educativo registrando un aumento del 73 % en ciberataques semanales respecto al período anterior, lo que lo posiciona como el tercero más atacado a nivel mundial (Ciberseguridadtic.es, 2025; Fouad, 2021). Esta tendencia revela una creciente vulnerabilidad estructural que afecta tanto a sistemas escolares como universitarios, y exige respuestas institucionales integrales.

Particularmente en España, esta problemática se ha manifestado con intensidad: el 70 % de las universidades reportaron incidentes de ciberseguridad durante 2024, evidenciando una fragilidad sistémica que compromete desde escuelas primarias hasta centros de investigación avanzada (Éxito Educativo, 2024). Estos datos refuerzan la urgencia de implementar mecanismos de control tecnológico que respondan a las exigencias del contexto digital contemporáneo.

En paralelo, la región asiática ha desarrollado enfoques innovadores para la gestión de riesgos tecnológicos educativos. Un estudio cuantitativo realizado con 385 estudiantes universitarios en Indonesia demostró que la gestión de riesgos digitales correlaciona significativamente con el rendimiento de la innovación del aprendizaje (coeficiente de ruta = 0.222, $p < 0.001$), mientras que la alfabetización tecnológica digital muestra la influencia más fuerte en el éxito de las transformaciones educativas (coeficiente de ruta = 0.361, $p < 0.001$) (Setyadi et al., 2025). Estos hallazgos evidencian que la efectividad de la innovación pedagógica depende de marcos integrales que articulen seguridad, formación y cultura digital.

En consecuencia, la conceptualización del control tecnológico en el ámbito educativo trasciende la mera supervisión de dispositivos, constituyéndose en un sistema complejo de gobernanza digital que articula políticas institucionales, procedimientos operativos y capacidades organizacionales (Rueda y Sousa, 2020; EY Technology Governance, 2025). Los marcos teóricos internacionales reconocen que las aulas de innovación pedagógica requieren sistemas de control específicos que equilibren libertad creativa con seguridad digital, como lo evidencian estudios sobre entornos educativos modernos (Grant y Booth, 2009; Setyadi et al., 2025).

Desde la perspectiva de la gestión pública educativa, diversos estudios han establecido fundamentos que permiten articular el control tecnológico con procesos de supervisión institucional. Por ejemplo, Bracho y Bracho (2016) abordan la gestión del talento humano en organizaciones educativas, mientras que González y Martínez (2010) analizan mecanismos de monitoreo de compromisos educativos en América Latina, proporcionando bases conceptuales para sistemas regionales de supervisión que se extienden al ámbito tecnológico.

Asimismo, los estudios de Pérez et al. (2017) sobre sistemas de formación especializada en supervisión educativa ofrecen un análisis comparativo de trece modelos escolares a nivel mundial, estableciendo marcos referenciales para la implementación de mecanismos de control tecnológico específicos. Esta línea se complementa con la investigación de Rodríguez et al. (2023), que analiza los

efectos de la supervisión escolar en la calidad educativa primaria y secundaria, aportando evidencia empírica sobre la efectividad de dichos sistemas en contextos diversos.

Por otra parte, la literatura especializada ha documentado una amplia gama de riesgos tecnológicos en contextos educativos, que incluyen desde ciberbullying y grooming hasta vulneraciones de propiedad intelectual y exposición a contenidos inapropiados (García et al., 2019; Morales et al., 2020; Rivas, 2015). En este sentido, los estudios de Canese et al. (2021) sobre percepciones del uso de tecnologías educativas durante la pandemia de COVID-19 revelan desconexiones críticas entre actores institucionales, lo que incrementa las vulnerabilidades sistémicas.

En el ámbito latinoamericano, investigaciones recientes han profundizado en la gestión de riesgos tecnológicos. Hernández et al. (2022) ofrecen panoramas comprensivos sobre amenazas digitales en la región, mientras que López et al. (2023) analizan específicamente la gestión de crisis tecnológicas en entornos escolares. A su vez, Silva et al. (2021) propone protocolos de respuesta ante incidentes de ciberseguridad, estableciendo marcos operativos para la atención de emergencias tecnológicas en instituciones educativas.

Finalmente, en el contexto europeo, estudios de campo realizados en Turquía con 394 docentes de educación primaria y secundaria evidencian que los niveles de concienciación sobre seguridad de la información se sitúan en un nivel moderado (puntuación promedio: 144.78 ± 38.87 en escala 48–240), con deficiencias específicas en el conocimiento de amenazas como phishing, ingeniería social y ciberacoso (Sapanca y Kanbul, 2022). En España, los estudios de SIC Spain (2024) y Gaptain (2024) sobre ciberseguridad y convivencia escolar evidencian la interconexión entre seguridad digital y dinámicas socioeducativas, estableciendo nexos conceptuales entre control tecnológico y gestión integral de riesgos educativos.

La gestión efectiva del control tecnológico requiere el desarrollo de capacidades institucionales específicas que integren competencias técnicas con habilidades de gestión educativa, articulando saberes operativos con enfoques estratégicos de gobernanza (Marquez y Díaz, 2005; Pérez et al., 2023). En esta línea, el estudio de Reyes (2024), aporta una base teórica robusta al identificar los principales enfoques de articulación entre pedagogía digital y gestión de riesgos. Su análisis sistemático evidencia que la efectividad del control tecnológico depende de la capacidad institucional para integrar marcos normativos, formación especializada y cultura organizacional orientada a la protección digital (Ramos, et al. 2008).

Asimismo, la investigación de Herrera-López et al. (2019) sobre herramientas tecnológicas en educación superior evidencia la necesidad de formación especializada para maximizar beneficios y minimizar riesgos asociados al uso educativo de tecnologías. Complementariamente, los estudios de Medina-Rodríguez et al. (2024) sobre ciberseguridad en educación superior, mediante revisión bibliométrica, establecen tendencias contemporáneas que orientan el desarrollo de capacidades institucionales especializadas en protección digital.

La efectividad del control tecnológico también depende del desarrollo de marcos normativos integrales que articulen políticas institucionales con estándares internacionales de seguridad digital (OECD, 2025; UNESCO, 2022). En esta línea, los estudios de Rivero et al. (2002) sobre gestión educativa para la transformación escolar establecen precedentes conceptuales que permiten construir políticas tecnológicas coherentes y contextualizadas.

Por otra parte, las investigaciones de Silva et al. (2018) sobre implementación de sistemas de monitoreo aportan perspectivas técnicas sobre la instrumentación de políticas de control tecnológico,

mientras que los estudios metodológicos de Sandelowski y Barroso (2007) ofrecen marcos para la síntesis de evidencias cualitativas, fundamentales en el desarrollo de políticas educativas basadas en evidencia.

La relevancia de esta investigación se fundamenta en la creciente dependencia tecnológica de los procesos educativos globales y en la emergencia de nuevos riesgos digitales que amenazan la integridad formativa. Los datos contemporáneos evidencian que el sector educativo es intrínsecamente vulnerable, debido a su función como ecosistema que maneja datos sensibles mientras promueve entornos colaborativos abiertos.

La incorporación acelerada de tecnologías emergentes en entornos educativos introduce imperativos de control específicos que requieren marcos conceptuales actualizados para garantizar la protección sistémica. Esta evolución tecnológica demanda la construcción de capacidad estatal especializada para la gestión de riesgos emergentes en el ámbito educativo digital, como lo evidencian las políticas contemporáneas de transformación digital educativa (OECD, 2025; EY Technology Governance, 2025).

En este marco, la presente investigación se inscribe en el campo emergente de la gobernanza digital educativa internacional, respondiendo a la necesidad identificada por múltiples estudios especializados de desarrollar marcos teóricos que integren perspectivas de gestión pública, tecnología educativa y seguridad digital en contextos de innovación pedagógica (Rueda y Sousa, 2020; Grant y Booth, 2009; Bracho y Bracho, 2016).

El alcance del estudio abarca la conceptualización multidimensional del control tecnológico como variable compuesta que integra dimensiones de políticas y normativas, mecanismos de supervisión, gestión preventiva de riesgos, respuesta a incidentes y capacidades institucionales, estableciendo conexiones teóricas con evidencia empírica documentada en diferentes contextos geográficos y sistemas educativos.

Finalmente, el objetivo de esta revisión conceptual es analizar las dimensiones teóricas del control de uso tecnológico como estrategia para la gestión de riesgos en aulas de innovación pedagógica desde una perspectiva internacional comparada, estableciendo un marco conceptual integral que contribuya al desarrollo de políticas públicas educativas en el contexto de la modernización del Estado y la transformación digital global de la educación.

MÉTODO

La presente investigación adoptó un enfoque teórico conceptual siguiendo los lineamientos metodológicos propuestos por Grant y Booth (2009) para revisiones narrativas en ciencias sociales. Este enfoque permitió la síntesis e integración de conocimientos teóricos dispersos en diferentes campos disciplinarios para construir marcos conceptuales coherentes que trasciendan los estudios individuales y generen interpretaciones de orden superior.

El diseño del estudio se estructuró a partir de una aproximación sistemática de revisión conceptual, que integra perspectivas multidisciplinarias provenientes de la gestión pública, la tecnología educativa, la ciberseguridad y la gobernanza digital. Esta metodología resultó particularmente adecuada para el objetivo de desarrollar un marco teórico integral que articule las dimensiones conceptuales del control tecnológico educativo desde una perspectiva internacional comparada, permitiendo identificar patrones, tensiones y vacíos teóricos en la literatura especializada.

La estrategia de búsqueda y selección de fuentes se llevó a cabo mediante consulta sistemática en bases de datos especializadas, priorizando SciELO como fuente principal debido a su representatividad en la producción científica latinoamericana, complementada con otros repositorios institucionales para obtener perspectivas globales. Los criterios de inclusión contemplaron artículos publicados entre 2015 y 2024, con el fin de garantizar la actualidad conceptual; estudios en español, inglés y portugués, para asegurar diversidad geográfica y lingüística; investigaciones centradas en tecnología educativa, gestión de riesgos digitales y gobernanza digital en educación; así como marcos teóricos vinculados a la modernización del Estado y la gestión pública educativa.

La estrategia de búsqueda utilizó términos controlados y combinaciones booleanas que incluyeron "control tecnológico educativo", "gestión riesgos digitales", "gobernanza digital educación", "ciberseguridad educativa", "supervisión tecnológica" y "políticas TIC educación". La búsqueda se complementó con consultas a organismos internacionales como UNESCO, OECD, Microsoft Threat Intelligence e institutos nacionales de ciberseguridad para incorporar perspectivas de política pública y datos estadísticos actualizados sobre amenazas tecnológicas en el sector educativo.

El análisis y síntesis conceptual se desarrollaron mediante un proceso de codificación temática, basado en la técnica de análisis de contenido cualitativo. Este proceso permitió identificar categorías emergentes que posteriormente se organizaron en dimensiones conceptuales articuladas. La síntesis se sustentó en el enfoque de “metasíntesis” propuesto por Sandelowski y Barroso (2007), lo cual facilitó la integración de hallazgos cualitativos provenientes de diversas fuentes, generando interpretaciones de orden superior que incorporan tanto perspectivas regionales como internacionales.

Finalmente, la validación teórica del marco conceptual propuesto se realizó mediante triangulación de fuentes, contrastando hallazgos de diferentes tradiciones disciplinarias y verificando la coherencia con marcos teóricos consolidados en gestión pública, tecnología educativa y ciberseguridad. Este proceso de validación incluyó la verificación de consistencia interna entre dimensiones conceptuales y la coherencia con experiencias internacionales documentadas en diferentes contextos geográficos y sistemas educativos.

RESULTADOS

El análisis sistemático de la literatura permitió identificar el control de uso tecnológico como una variable compuesta de carácter multidimensional, estructurada en torno a cinco dimensiones principales (Ver Figura 1). Cada una de estas dimensiones incorpora componentes específicos que operacionalizan el constructo teórico, permitiendo su aplicación en contextos educativos diversos. Esta conceptualización integral surge como respuesta a la creciente complejidad de los entornos educativos digitalizados y a la necesidad de marcos teóricos comprensivos que articulen, de manera coherente, perspectivas provenientes de la gestión pública, la tecnología educativa y la ciberseguridad.

1) Políticas y normativas de control tecnológico

Esta dimensión constituye el fundamento regulatorio del control tecnológico educativo y constituye el marco institucional que legitima y orienta las prácticas de control en los entornos de innovación pedagógica. Los hallazgos revelan que esta dimensión se estructura en torno a dos componentes principales que operan de manera articulada para establecer el ecosistema normativo necesario:

Marco Regulatorio Institucional: comprende el sistema de políticas internas que definen parámetros de uso tecnológico y establecen las directrices fundamentales para la gestión de recursos digitales. Los estudios evidencian que la existencia formal de políticas específicas, su claridad y actualización periódica, así como su alineación con marcos regulatorios nacionales, constituyen indicadores críticos de madurez institucional en la gestión tecnológica educativa.

Protocolos de Seguridad Digital: incluyen procedimientos técnicos y administrativos diseñados para proteger sistemas tecnológicos educativos. En este ámbito, la protección de datos personales, las medidas de ciberseguridad, los procedimientos ante incidentes y las políticas de acceso emergen como elementos fundamentales que garantizan la integridad, confidencialidad y disponibilidad de la información en contextos educativos digitalizados.

2) **Mecanismos de supervisión y monitoreo,**

Esta dimensión se conceptualiza como un sistema integrado de procesos, herramientas y metodologías orientadas al seguimiento continuo, evaluación y control de las actividades tecnológicas en entornos educativos para garantizar el cumplimiento de objetivos pedagógicos y normativos. Sus componentes son;

Sistemas de monitoreo en tiempo real: incluyen herramientas tecnológicas para la observación, registro y análisis continuo de actividades digitales en el momento de su ejecución. La literatura consultada revela que la capacidad de detección de uso inadecuado, la implementación de alertas automáticas y la trazabilidad de acciones constituyen indicadores operativos clave que permiten una gestión proactiva de los riesgos tecnológicos.

Supervisión pedagógica tecnológica: constituye un proceso sistemático de acompañamiento docente y evaluación del cumplimiento de objetivos educativos mediante el uso de tecnologías. En este contexto, la identificación de desviaciones educativas, el acompañamiento docente en el uso tecnológico, la evaluación del cumplimiento de objetivos pedagógicos y la retroalimentación continua emergen como elementos distintivos que aseguran la alineación del uso tecnológico con los propósitos formativos institucionales.

3) **Gestión preventiva de riesgos**

Esta dimensión, adopta un enfoque proactivo y sistemático orientado a la identificación, evaluación, prevención y mitigación de riesgos asociados al uso de tecnologías en contextos educativos, mediante la implementación de medidas anticipatorias y estrategias de control. Los componentes identificados en esta dimensión reflejan tanto aspectos diagnósticos como operativos de la gestión de riesgos.

Identificación y evaluación de riesgos: proceso metodológico de reconocimiento, análisis y valoración sistemática de amenazas, vulnerabilidades y riesgos potenciales derivados del uso de tecnologías en entornos educativos. La literatura consultada evidencia que el mapeo de riesgos tecnológicos potenciales, incluyendo fenómenos como ciberbullying, grooming, sexting y malware, junto con el análisis de vulnerabilidades del sistema, la evaluación de impacto pedagógico y la categorización de niveles de riesgo, constituyen indicadores centrales de este componente.

Medidas preventivas implementadas: abarca el conjunto de acciones, controles técnicos y procedimientos establecidos para prevenir la materialización de riesgos tecnológicos y proteger a los usuarios del entorno educativo. Los hallazgos revelan que los filtros de contenido y aplicaciones, las restricciones de acceso por perfiles de usuario, el control de horarios y tiempos de uso, y la designación de espacios físicos de uso supervisado representan estrategias operativas fundamentales en la

prevención de riesgos digitales en contextos educativos.

4) Respuesta y mitigación de incidentes

Esta dimensión, se conceptualiza como un sistema estructurado de procedimientos, recursos y capacidades organizacionales diseñado para responder de manera efectiva y oportuna ante incidentes tecnológicos, minimizando su impacto y facilitando la recuperación del entorno educativo. Comprende dos componentes que abordan tanto la respuesta inmediata como el aprendizaje organizacional derivado de los incidentes.

Protocolos de respuesta inmediata: constituyen procedimientos preestablecidos y estandarizados que definen las acciones específicas a ejecutar inmediatamente después de la detección de un incidente tecnológico. La literatura revisada identifica como elementos críticos los procedimientos documentados de respuesta ante incidentes, los tiempos de reacción establecidos según la severidad del evento, el escalamiento de situaciones críticas a niveles superiores de autoridad y especialización, y los protocolos de comunicación con los diversos actores involucrados, incluyendo directivos, docentes, estudiantes, padres de familia y autoridades competentes.

Medidas correctivas y de mejora: abarca las acciones implementadas posterior a la resolución de incidentes, orientadas a eliminar causas raíz, fortalecer defensas y mejorar los procesos de respuesta futura. En este ámbito, el análisis post-incidente, los ajustes en políticas y procedimientos basados en hallazgos y lecciones aprendidas, y el aprendizaje organizacional sistemático constituyen elementos de mejora continua que transforman cada incidente en una oportunidad de fortalecimiento institucional.

5) Capacidades institucionales para el control

Abarca el conjunto de recursos humanos especializados, infraestructura tecnológica, competencias organizacionales y capacidades de gestión que posee la institución educativa para ejercer control efectivo sobre el uso de tecnologías. Esta dimensión se estructura en dos componentes complementarios que reflejan tanto el capital humano como el capital técnico necesario para la gestión efectiva del control tecnológico.

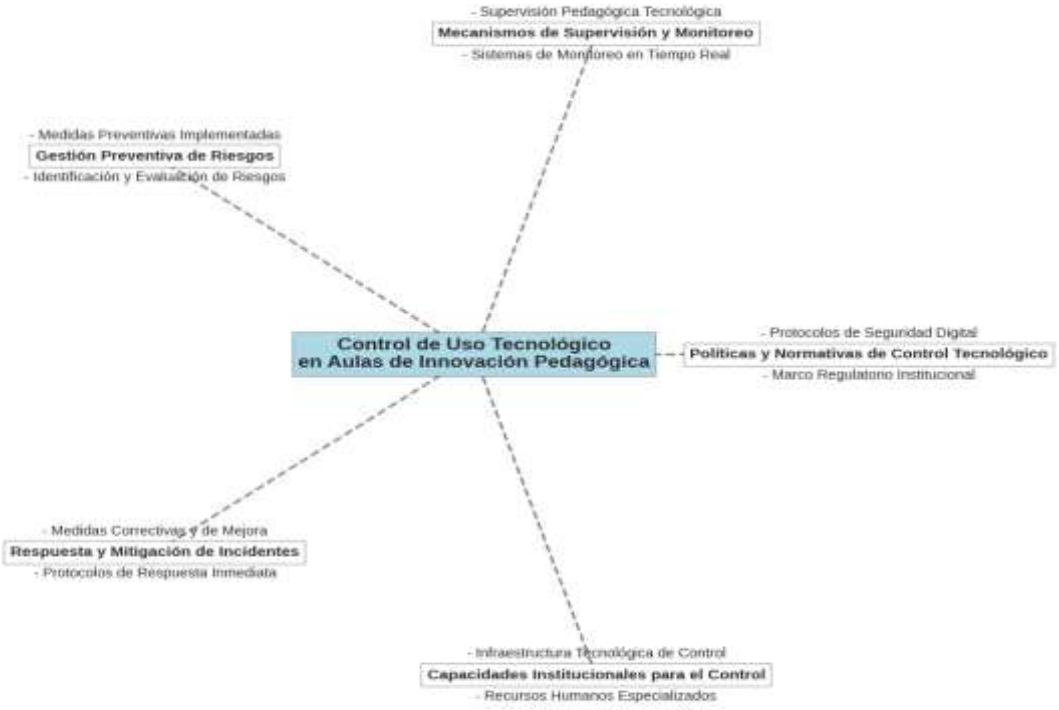
Recursos humanos especializados: comprende el personal calificado con competencias específicas en gestión tecnológica educativa, ciberseguridad y riesgos digitales, capaz de liderar y ejecutar estrategias de control tecnológico. Los hallazgos evidencian que el personal capacitado en gestión tecnológica, las competencias en gestión de riesgos digitales, los programas de formación continua y la definición clara de roles y responsabilidades constituyen indicadores fundamentales de capacidad humana institucional.

Infraestructura tecnológica de control: abarca el conjunto de herramientas tecnológicas, sistemas informáticos, equipos especializados y recursos técnicos disponibles para ejercer supervisión y control sobre el uso de tecnologías educativas. En este componente, la disponibilidad de herramientas tecnológicas de control, la capacidad técnica de la infraestructura en términos de robustez, escalabilidad y funcionalidad, la integración de sistemas de gestión que asegure interoperabilidad entre diferentes plataformas, y el mantenimiento y actualización sistemática de sistemas emergen como indicadores críticos que determinan la capacidad técnica institucional para implementar estrategias efectivas de control tecnológico.

Esta estructura multidimensional identificada a través del análisis de la literatura representa una conceptualización integral del control de uso tecnológico en aulas de innovación pedagógica, articulando elementos normativos, operativos, preventivos, reactivos y de capacidad institucional en un marco teórico coherente que puede orientar tanto la investigación académica como el desarrollo de

políticas públicas educativas en el contexto de la digitalización y modernización del Estado educativo.

Figura 1. *Dimensiones del control de uso tecnológico en aulas de innovación pedagógica.*



DISCUSIÓN

Los resultados obtenidos del estudio, permiten afirmar que el control de uso tecnológico en aulas de innovación pedagógica constituye un constructo multidimensional complejo, que trasciende las aproximaciones unidimensionales o instrumentales tradicionalmente empleadas en la literatura. Esta conceptualización integral se alinea con los postulados de la gobernanza digital educativa (Rueda y Sousa, 2020) y representa una contribución significativa al campo de la gestión pública educativa, al proponer una arquitectura teórica que articula dimensiones normativas, operativas, preventivas, reactivas y estructurales. En este sentido, la estructura pentadimensional identificada refleja la complejidad inherente a la gestión de riesgos tecnológicos en contextos educativos innovadores, y responde a la necesidad de marcos teóricos que integren, de forma coherente, perspectivas de gestión pública, tecnología educativa y ciberseguridad, superando los enfoques fragmentados y sectoriales prevalentes en la literatura especializada.

El marco conceptual propuesto tiene implicaciones directas para los procesos de modernización del Estado en el ámbito educativo. La dimensión de políticas y normativas se articula con los principios de gobernanza digital y transparencia institucional, mientras que las dimensiones operativas -supervisión, gestión preventiva y respuesta a incidentes- reflejan la transición hacia modelos de gestión pública basados en evidencia, orientados a resultados y centrados en la anticipación de riesgos. Particularmente, la inclusión de las capacidades institucionales como dimensión diferenciada reconoce que la efectividad del control tecnológico no depende exclusivamente de la existencia de normativas o

herramientas, sino de la disponibilidad de recursos humanos especializados y de infraestructura técnica adecuada. Esta perspectiva se encuentra en consonancia con los enfoques de construcción de capacidad estatal propuestos por la literatura contemporánea en gestión pública (Reyes, 2024), así como con los marcos de resiliencia institucional frente a amenazas digitales emergentes.

Sin embargo, el análisis también revela tensiones conceptuales entre control tecnológico e innovación pedagógica que requieren consideración teórica. La literatura evidencia que marcos de control excesivamente restrictivos pueden inhibir la creatividad y experimentación pedagógica, mientras que controles insuficientes exponen a estudiantes y docentes a riesgos significativos (Hernández et al., 2022). Esta tensión estructural sugiere la necesidad de marcos conceptuales dinámicos que permitan equilibrios adaptativos entre control e innovación, evitando tanto la tecnofobia como la tecnofilia. En este contexto, la noción de "control inteligente" emerge como una perspectiva prometedora, al proponer sistemas de control flexibles, sensibles al contexto y capaces de ajustarse a las necesidades pedagógicas sin comprometer la seguridad digital.

Adicionalmente, el análisis identifica vacíos significativos en la conceptualización de los aspectos éticos del control tecnológico educativo. La literatura revisada evidencia una atención limitada a dimensiones críticas como la privacidad estudiantil, la autonomía pedagógica y los derechos digitales, los cuales resultan fundamentales en el marco de sociedades democráticas y sistemas educativos inclusivos. De manera complementaria, se observa un desarrollo teórico insuficiente en torno a los mecanismos de participación estudiantil y docente en el diseño, implementación y evaluación de los sistemas de control tecnológico. Esta limitación resulta especialmente relevante desde las perspectivas de la gestión pública participativa y la democracia educativa, que promueven la corresponsabilidad, la transparencia y la legitimidad institucional.

Por otra parte, el análisis revela una correspondencia significativa en la identificación de los principales riesgos tecnológicos -como el ciberbullying, el grooming o la exposición a contenidos inapropiados-, pero también divergencias importantes en las estrategias de control recomendadas. Mientras algunos autores priorizan mecanismos técnicos automatizados (como filtros de contenido, restricciones de acceso o monitoreo en tiempo real), otros enfatizan enfoques formativos centrados en la alfabetización digital crítica y la construcción de ciudadanía digital. Esta discrepancia refleja diferencias epistemológicas sobre la naturaleza del control tecnológico educativo: mientras unos lo conciben como una función técnica de vigilancia, otros lo entienden como un proceso pedagógico de acompañamiento y formación. Esta tensión sugiere la necesidad de marcos teóricos integradores que reconozcan la complementariedad entre control técnico y formación ética, y que promuevan una visión holística del control como práctica educativa situada.

Finalmente, es necesario reconocer las limitaciones metodológicas del presente estudio. Al tratarse de una revisión conceptual de tipo narrativo, la selección de fuentes, aunque sistemática, puede estar sujeta a sesgos de interpretación y cobertura. Además, la ausencia de validación empírica directa limita la generalización de los hallazgos, por lo que se recomienda su contrastación futura mediante estudios de caso, investigaciones mixtas o validaciones empíricas en contextos educativos específicos. Asimismo, la concentración de fuentes en el ámbito latinoamericano y europeo podría delimitar la aplicabilidad del modelo en otras regiones con dinámicas sociotécnicas distintas. Estas limitaciones no invalidan los hallazgos, pero sí invitan a su interpretación crítica y a su ampliación en futuras investigaciones.

CONCLUSIONES

Esta revisión conceptual ha permitido desarrollar un marco teórico integral para la comprensión del control de uso tecnológico como estrategia de gestión de riesgos en aulas de innovación pedagógica, cumpliendo con el objetivo planteado de analizar sus dimensiones teóricas desde la perspectiva de la gestión pública y la gobernabilidad digital. La conceptualización pentadimensional propuesta constituye una contribución significativa al campo de la gestión pública educativa, al ofrecer una base teórica sólida que trasciende los enfoques fragmentados previamente dominantes en la literatura especializada. Este marco integra de manera coherente perspectivas de gobernanza digital, gestión de riesgos y modernización del Estado, articulación especialmente relevante en el contexto latinoamericano, donde los procesos de digitalización educativa requieren modelos conceptuales sensibles a las particularidades regionales.

Los hallazgos derivados de esta investigación tienen implicaciones directas para el diseño e implementación de políticas públicas educativas en el ámbito tecnológico. La estructura dimensional identificada puede orientar el desarrollo de marcos regulatorios, protocolos operativos y sistemas de evaluación que garanticen simultáneamente la innovación pedagógica y la seguridad digital, superando la falsa dicotomía entre control y creatividad. En este sentido, la conceptualización de las capacidades institucionales como dimensión crítica sugiere que las políticas públicas deben trascender el plano normativo e incorporar componentes sustantivos de fortalecimiento organizacional, desarrollo de recursos humanos especializados e inversión en infraestructura tecnológica. Esta perspectiva se vincula con los enfoques contemporáneos de construcción de capacidad estatal, reconociendo que la efectividad de las políticas depende tanto de su diseño formal como de las condiciones institucionales para su implementación.

El marco conceptual desarrollado abre múltiples líneas de investigación futura que demandan atención académica urgente. Se requieren estudios empíricos que permitan operacionalizar las dimensiones identificadas y desarrollar instrumentos de medición válidos y confiables, facilitando el tránsito de la conceptualización teórica hacia la evaluación práctica de sistemas de control tecnológico en contextos educativos reales. Particular atención merece, investigaciones que examinen las relaciones entre dimensiones y su impacto diferenciado en los resultados educativos, así como estudios comparativos que analicen variaciones en la implementación del control tecnológico según niveles educativos, tipos de institución y características socioculturales.

Adicionalmente, se identifican vacíos teóricos que deben ser abordados en futuras investigaciones, especialmente en lo relativo a los aspectos éticos del control tecnológico educativo. Se requiere el desarrollo de marcos conceptuales que equilibren la eficacia del control con el respeto a los derechos digitales, la privacidad estudiantil y la autonomía pedagógica. Esta línea resulta crítica para el diseño de modelos de control tecnológico democráticos y participativos, que superen las aproximaciones tecnocráticas y reconozcan la agencia de estudiantes y docentes en la gobernanza digital educativa.

En términos de recomendaciones para la práctica, se sugiere que las instituciones educativas adopten enfoques sistémicos para la implementación del control tecnológico, reconociendo que su efectividad depende de la articulación coherente de las cinco dimensiones identificadas. Sistemas que privilegian exclusivamente componentes técnicos -como filtros o restricciones de acceso- sin el respaldo de políticas claras, capacitación del recurso humano especializado y protocolos de respuesta tienden a ser inefectivos o generar resistencias institucionales. Asimismo, se recomienda que las autoridades educativas nacionales y regionales desarrollen marcos regulatorios que orienten sin restringir excesivamente la autonomía institucional, reconociendo la diversidad de contextos y

necesidades específicas de cada institución.

Finalmente, esta revisión sugiere que el control tecnológico educativo debe ser comprendido como un elemento estratégico en los procesos de modernización del Estado contemporáneo, trascendiendo su caracterización como función meramente administrativa o técnica. La capacidad estatal para gestionar eficazmente los riesgos tecnológicos en contextos educativos emerge como un indicador de madurez institucional y de eficacia gubernamental en la era digital.

En este sentido, la gestión de riesgos tecnológicos educativos se posiciona como una función estratégica del Estado moderno, que requiere marcos conceptuales, metodológicos e instrumentales específicos, capaces de reconocer tanto las oportunidades como los desafíos de la transformación digital. La construcción de sistemas de control tecnológico efectivos y democráticos representa, en última instancia, un desafío de gobernabilidad que trasciende el ámbito técnico para inscribirse en los procesos más amplios de transformación del Estado en el siglo XXI, donde la capacidad de gobernar lo digital se constituye como dimensión fundamental de la gobernabilidad democrática.

REFERENCIAS

Bracho, K., y Bracho, M. (2016). Gestión del talento humano en organizaciones educativas. *Revista de Ciencias Sociales*, 22(2), 148-165. https://bit.ly/3bracho2016

Canese, V., Mereles, J., y Amarilla, R. (2021). Desconexión entre actores: percepciones del uso de tecnologías educativas durante la pandemia por COVID-19. *Revista Colombiana de Educación*, 1(82), 201-224. https://doi.org/10.17227/rce.num82-11175

Ciberseguridadtic.es (2025) Incremento del 73% en ciberataques semanales al sector educativo https://ciberseguridadtic.es/actualidadendpoint/el-sector-educativo-registra-un-incremento-del-73-en-ciberataques-semanales-respecto-a-2024-202505209016.htm

Éxito Educativo / Europa Press (2024) 70% de universidades españolas sufrieron ciberataques https://www.europapress.es/sociedad/noticia-casi-70-universidades-espanolas-sufrieron-ciberataques-ciberincidentes-ultimo-ano-imc-20250618113441.html

EY Technology Governance (2025) Tendencias de gobernanza tecnológica en educación https://www.ey.com/es_co/board-matters/juntas-directivas-colombia-2025-priorizan-innovacion-y-tecnologia

Fouad, N. S. (2021). Securing higher education against cyberthreats: from an institutional risk to a national policy challenge. *Journal of Cyber Policy*, 6(2), 137-154. https://doi.org/10.1080/23738871.2021.1973526

Gaptain (2024) Estudio 'Educación digital y Convivencia escolar 2024. https://gaptain.com/blog/nuevo-estudio-educacion-digital-y-convivencia-escolar-2024/

García, L., Fernández, M., y Rodríguez, P. (2019). Uso problemático de las TIC en adolescentes. *Revista Mexicana de Investigación Educativa*, 24(81), 103-124. https://bit.ly/3garcia2019

González, L., y Martínez, R. (2010). Mecanismos de monitoreo de los compromisos en educación en América Latina: sistemas regionales de indicadores educativos. *Revista Mexicana de Investigación Educativa*, 15(45), 381-409. https://bit.ly/3gonzalez2010

Governance Institute of Australia (2024) Curso sobre gobernanza en ciberseguridad https://www.governanceinstitute.com.au/courses/e09688-cyber-security-governance/

Grant, M. J., y Booth, A. (2009). A typology of reviews: an analysis of 14 review types and associated methodologies. *Health Information & Libraries Journal*, 26(2), 91-108. https://doi.org/10.1111/j.1471-1842.2009.00848.x

Hernandez, M., Lopez, C., y Silva, R. (2022). Panorama de riesgos por el uso de la tecnología en América Latina. *Revista Colombiana de Educación*, 1(84), 300-325. https://doi.org/10.17227/rce.num84-12456

Herrera-López, J., Sánchez-Pérez, M., y González-Martínez, A. (2019). Herramientas tecnológicas en el proceso de enseñanza-aprendizaje en estudiantes de educación superior. *Revista

Iberoamericana para la Investigación y el Desarrollo Educativo*, 10(19), 1-25. https://bit.ly/3herrera2019

López, R., Martínez, C., y Fernández, A. (2023). Gestión de crisis tecnológicas en entornos educativos. *Revista de Gestión Educativa*, 12(4), 78-95. https://doi.org/10.15359/rgpe.12-4.4

Márquez, J., y Diaz, J. (2005). Formación del recurso humano por competencias. *Revista Venezolana de Gerencia*, 10(29), 132-146. https://bit.ly/3marquez2005

Morales, P., Rodríguez, C., y López, M. (2020). Adolescentes frente a los riesgos en el uso de las TIC. *Revista Mexicana de Investigación Educativa*, 25(84), 117-140. https://bit.ly/3morales2020

Pérez, D., Hernández, L., y Martínez, R. (2023). Capacidad de gestión de recursos humanos en las empresas. *Revista de Ingeniería Industrial*, 44(1), 58-75. https://bit.ly/3perez2023

Pérez, M., Rodríguez, A., y González, C. (2017). Propuesta de un sistema de formación especializada en supervisión educativa: análisis comparativo de 13 sistemas de supervisión escolar en el mundo. *Revista Mexicana de Investigación Educativa*, 22(74), 165-191. https://bit.ly/3perezm2017

Programa KIDS CENTRIC. SIC SPAIN 3.0 (2024) Estudio sobre ciberseguridad y convivencia escolar https://pdabullying.com/uploads/2024/05/SIC-SPAIN-3.0-Estudio-Ciberseguridad-y-Convivencia-escolar-24.pdf

Ramos, G., Sosa, M., y Acosta, F. (2008). Una ruta metodológica para evaluar la capacidad institucional. *Revista Mexicana de Sociología*, 70(2), 253-289. https://bit.ly/3ramos2008

Reyes, N., Lujan, G., Reyes, L., y Mariluz, J. (2024). Gestión de riesgos tecnológicos en aulas de innovación pedagógica: una revisión sistemática de integración pedagógica. https://doi.org/10.59659/revistatribunal.v4i9.65

Rivas, J. (2015). Riesgos en el uso de TIC en alumnos de enseñanza básica: el caso de un colegio en Chillan, Chile. *Revista Integra Educativa*, 8(3), 179-197. https://bit.ly/3rivas2015

Rivero, M., Gómez, P., y Abreu, R. (2002). Gestión educativa para la transformación de la escuela. *Revista Venezolana de Gerencia*, 7(20), 150-175. https://bit.ly/3rivero2002

Rodríguez, A., Hernández, M., y López, C. (2023). Efectos de la supervisión escolar sobre la calidad educativa en primaria y secundaria. *Revista Mexicana de Investigación Educativa*, 28(96), 116-142. https://bit.ly/3rodriguez2023

Rueda, C., y Sousa, M. (2020). Sobre la gobernanza digital, política digital y educación. *Revista Colombiana de Sociología*, 43(2), 88-112. https://doi.org/10.15446/rcs.v43n2.82120

Sandelowski, M., y Barroso, J. (2007). Handbook for synthesizing qualitative research. Springer Publishing Company. https://www.scirp.org/reference/referencespapers?referenceid=1196746

Sapanca, H. F., y Kanbul, S. (2022). Risk management in digitalized educational environments: Teachers' information security awareness levels. *Frontiers in Psychology*, 13, 986561. https://doi.org/10.3389/fpsyg.2022.986561

Setyadi, A., Pawirosumarto, S., Damaris, A., Ichwanuddin, W., Sulistyo, F. A., Hendrayani, E., y Rozak, H. A. (2025). Risk management, digital technology literacy, and modern learning environments in enhancing learning innovation performance: A framework for higher education. *Education and Information Technologies*, 30, 15095-15123. https://doi.org/10.1007/s10639-025-13380-4

Silva, J., Ramirez, P., y Torres, L. (2018). Implementación de un sistema de monitoreo de área amplia a escala de laboratorio para sistemas eléctricos de potencia. *Revista Mexicana de Ingeniería Biomédica*, 39(2), 195-208. https://bit.ly/3silva2018

Silva, P., González, R., y Martínez, A. (2021). Protocolos de respuesta a incidentes de ciberseguridad. *Revista de Ingeniería y Tecnología*, 18(2), 112-128. https://doi.org/10.15359/rie.18-2.7

UNESCO (2022) Estrategia de la UNESCO sobre la Innovación Tecnológica en la Educación (2022-2025). https://unesdoc.unesco.org/ark:/48223/pf0000378847_spa