ISSN: 2959-6513 - ISSN-L: 2959-6513
Volumen 4. No. 9 / Octubre 2024 - Número especial
Páginas 592 - 611

Gestión de riesgos tecnológicos en aulas de innovación pedagógica: una revisión sistemática de integración pedagógica

Technological risk management in pedagogical innovation classrooms: a systematic review of pedagogical integration

Gestão de riscos tecnológicos em salas de aula de inovação pedagógica: uma revisão sistemática da integração pedagógica

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/0000-0002-9488-8650
Escuela de Educación Superior Pedagógica Emilia Barcia Boniffatti.
Lima - Perú

https://doi.org/10.59659/revistatribunal.v4i9.65

Artículo recibido 12 de junio de 2024 / Arbitrado 30 de junio de 2024 / Aceptado 10 de septiembre 2024 / Publicado 25 de octubre de 2024

Resumen

Este estudio está dirigido a conocer el proceso de integración de tecnologías en las Aulas de Innovación Pedagógica (AIP) de Educación Básica Regular en Perú, especialmente, abordar los nuevos riesgos que requieren estrategias efectivas de gestión, considerando la brecha digital existente. A partir de esta realidad, el presente trabajo tiene como propósito analizar las estrategias de gestión de riesgos tecnológicos implementadas en las AIP de Educación Básica Regular en Perú entre 2019 y 2024, evaluando su efectividad, integración con procesos pedagógicos y abordaje de la brecha digital. La metodología aplicada fue cualitativa, no experimental, exploratoria y descriptiva para explicar el problema de estudio. El resultado propuesto, constituye aporte de investigaciones en el contexto de la gestión de riesgos tecnológicos en aulas de innovación tecnológica, lo que permitió profundizar en componentes claves como: marco normativo, estructura organizacional y roles, diagnóstico y evaluación de riesgos, estrategias de prevención y mitigación, monitoreo, mejora continua y articulación con otros procesos de gestión.

Palabras clave:
Gestión; gestión de riesgos; innovación pedagógica; integración de tecnologías; estrategias de gestión.

Abstract

This study aims to understand the process of integrating technologies in the Pedagogical Innovation Classrooms (AIP) of Regular Basic Education in Peru, particularly addressing the new risks that require effective management strategies, considering the existing digital divide. Based on this reality, the present work aims to analyze the technological risk management strategies implemented in the AIP of Regular Basic Education in Peru between 2019 and 2024, evaluating their effectiveness, integration with pedagogical processes, and addressing the digital divide. The applied methodology was qualitative, non-experimental, exploratory, and descriptive to explain the study problem.

Keywords:
Management; risk management; pedagogical innovation; technology integration; management strategies.

The proposed result constitutes a contribution to research in the context of technological risk management in technological innovation classrooms, allowing for a deeper exploration of key components such as: regulatory framework, organizational structure and roles, risk diagnosis and assessment, prevention and mitigation strategies, monitoring, continuous improvement, and coordination with other management processes.

Resumo

Este estudo tem como objetivo compreender o processo de integração de tecnologias nas Salas de Inovação Pedagógica (AIP) da Educação Básica Regular no Peru, abordando especialmente os novos riscos que exigem estratégias eficazes de gestão, considerando a brecha digital existente. A partir dessa realidade, o presente trabalho tem como propósito analisar as estratégias de gestão de riscos tecnológicos implementadas nas AIP da Educação Básica Regular no Peru entre 2019 e 2024, avaliando sua efetividade, integração com processos pedagógicos e abordagem da brecha digital. A metodologia aplicada foi qualitativa, não experimental, exploratória e descritiva para explicar o problema de estudo. O resultado proposto constitui uma contribuição para pesquisas no contexto da gestão de riscos tecnológicos em salas de inovação tecnológica, permitindo aprofundar componentes-chave como: marco normativo, estrutura organizacional e papéis, diagnóstico e avaliação de riscos, estratégias de prevenção e mitigação, monitoramento, melhoria contínua e articulação com outros processos de gestão.

Palavras-chave:

Estratégias de gestão; gestão; gestão de riscos; inovação pedagógica; integração de tecnologias.

INTRODUCCIÓN

La integración de tecnologías en las Aulas de Innovación Pedagógica (AIP) de Educación Básica Regular en Perú ha traído consigo tanto oportunidades como desafíos. Mientras que estas tecnologías ofrecen nuevas posibilidades para el aprendizaje, también introducen riesgos que requieren una gestión cuidadosa. La efectividad de esta gestión depende no solo de la implementación de estrategias de seguridad, sino también de cómo estas se integran con los procesos pedagógicos.

Los procesos de de riesgos tecnológicos en aulas de innovación pedagógica enmarcados en la usabilidad de infraestructura de la integración pedagógica se encuentran estandarizados y normalizados en gran medida, sin embargo, cuando se requiere tratar solo un aspecto del conjunto de procesos, como el marco normativo, estructura organizacional y roles, diagnóstico y evaluación de riesgos, estrategias de prevención y mitigación, monitoreo, mejora continua y articulación con otros procesos de gestión, es necesario referirse a una norma técnica en específico, tal como lo alude López y Ruiz (2020) al considerar el proceso de Seguridad Física y ambiental forman parte del proceso de gestión de riesgos y la innovación pedagógica.

Los riesgos en la Tecnología de la Información y Comunicación (TIC) están relacionados con los eventos e incidentes que podrían comprometer la infraestructura computacional y causar impactos desfavorables en los procesos de negocio de una organización vinculados con su misión y visión.

Al respecto, es de interés en este trabajo analizar los ambientes de las Aulas de Innovación Pedagógica (AIP) de las instituciones educativas son vulnerables a eventos climáticos de orden natural, así como debido a fallas de carácter eléctrico o a los accesos al equipamiento computacional que provoca averías de componentes lógicos o físicos.

En este sentido, la gestión de riesgos es una herramienta que posibilita la toma de decisiones en situaciones que pueden ir mal, y el firme propósito de identificar los riegos más importantes que se pueden presentar en determinado escenario y la gestión de estrategias para minimizar los efectos de los eventos perjudiciales y garantizar la continuidad del negocio.

Investigadores como Sánchez y Soler (2021) plantean que la Gestión de Riesgos es necesario implementarlo por fases tales como: el análisis para determinar las vulnerabilidades de un sistema; la clasificación para tipificar los riesgos encontrados; la reducción para implementar las medidas de protección; y el control para determinar los ajustes en las deficiencias encontradas, en este sentido, los riesgos en aulas AIP configura como riesgo operativo

En el contexto internacional, autores como López y Ruiz (2020), destacan la importancia de la implementación de la Gestión de Riesgos en las Aulas de Innovación Pedagógica (AIP) de las instituciones educativas, cuya filosofía principal se basa en la gestión de riesgos implícitos o explícitos que se presentan en cualquier organización, con la finalidad de evitar incidentes de seguridad que detengan el normal funcionamiento del equipamiento computacional.

Lo anterior implica, además, que los riesgos en la Tecnología de la Información y Comunicación (TIC) están relacionados con los eventos e incidentes que podrían comprometer la infraestructura computacional y causar impactos desfavorables en los procesos de negocio de una organización vinculados con su misión y visión.

En este sentido, la gestión de riesgos es una herramienta que posibilita la toma de decisiones en situaciones que pueden ir mal, y el firme propósito de identificar los riegos más importantes que se pueden presentar en determinado escenario y la gestión de estrategias para minimizar los efectos de los eventos perjudiciales y garantizar la continuidad del negocio.

Lo anterior implica, además, que para los fines de la investigación consideraremos los siguientes controles de estructura organizacional, roles, estrategias de prevención y mitigación, monitoreo las áreas seguras y de la seguridad de equipos.

El Proyecto Educativo Nacional (PEN 2036) destaca que la información compartida en redes plantea desafíos de privacidad y seguridad. Además, como señalan Muñoz et al. (2021), los ecosistemas tecnológicos de aprendizaje y gestión educativa requieren un enfoque integral que considere tanto los aspectos técnicos como los pedagógicos. En este contexto, es crucial entender no solo qué estrategias de gestión de riesgos tecnológicos se están implementando en las AIP peruanas, sino también cómo estas se integran con la práctica educativa cotidiana.

La brecha digital en Perú añade una capa adicional de complejidad a este desafío. Como indican Vásquez-Cano et al. (2020), la competencia digital de los estudiantes y docentes varía significativamente, lo que influye en la implementación y efectividad de las estrategias de gestión de riesgos. Por lo tanto, es esencial examinar cómo se abordan estas disparidades en diferentes contextos socioeconómicos.

La Innovación Pedagógica hace referencia a tres aspectos fundamentales:

1) La introducción y experimentación de nuevas estrategias docentes nuevas recursos didácticos que propicie una enseñanza más activa e innovadora.

2) El desarrollo de modelos e instrumentos de evaluación que favorezcan nuevas propuestas de innovación curricular.

3) La realización creativa de experiencias que favorezca de manera clara la internacionalización del estudiante.

En este sentido buscamos reconocer y estimular propuestas que contribuyan al aprendizaje activo de los estudiantes a través del Aula de Innovación Pedagógica (AIP), esta constituye el escenario de aprendizaje en el que las Tecnologías de Información y Comunicación (TICs) se integran en las actividades pedagógicas, donde estudiantes y docentes aprovechan pedagógicamente este recurso, según las orientaciones del Diseño Curricular Nacional y las recomendaciones metodológicas de la Dirección General de Tecnologías Educativas (DIGETE), priorizando, fundamentalmente horas de trabajo con los estudiantes (sesiones de aprendizaje con

el uso de las TICs) y horas de práctica para los docentes (Capacitación y asesoramiento a los docentes).

El Aula de Innovaciones es un escenario de aprendizaje para el uso y aplicación de las TIC, y debe ser usada por todos los estudiantes de la institución educativa, por lo que el horario de clases debe ser flexible y adecuarse a las necesidades e intereses de los estudiantes y a las posibilidades de atención que disponga la institución educativa. El docente responsable del aula de innovaciones, en coordinación con la dirección de la institución educativa y el equipo docente, elaborará el cuadro de distribución de horas del uso del aula, destinando horas de práctica para los docentes.

Es responsabilidad del director de la institución educativa y del docente responsable del aula de innovación promover la integración de las TIC al currículo en todos los niveles y modalidades y velar porque los materiales y equipos del aula de innovación sean de exclusivo uso educativo. No está permitida toda mediación en operaciones de venta o alquiler, ni el beneficio pecuniario o material.

El docente responsable del aula de innovación debe elaborar el reglamento que norme el uso del Aula de Innovaciones y de los recursos didácticos, el cual deberá ser presentado al director para su aprobación. Su contenido debe comprender entre otros:

1) Condiciones de uso,

2) Espacios a ser utilizados,

3) Responsable o responsables de las aulas,

4) Aulas disponibles, organización y horarios de uso,

5) Criterios de utilización,

6) Regulación del uso de estos espacios para la realización de actividades fuera del período lectivo.

Según Flores, (2017) el Aula de Innovación Pedagógica (AIP) es un escenario de aprendizaje en el que las TIC se integran de manera transversal en las sesiones de aprendizaje tanto para docentes, así como para estudiantes a fin de que interactúen empleando recursos tecnológicos existentes y favoreciendo el uso de una cultura digital.

Si tomamos como referencia el desarrollo de la prospectiva a nivel tecnológico en diferentes países, nos muestra que los resultados obtenidos tienen un papel importante para el apoyo en la planificación de la Ciencia y la Tecnología; en este sentido, al punto de vista educación las actividades de prospectiva tecnológica mediante el uso de la comunicación y cooperación son valiosas; haciendo un análisis en la que se aporta la experiencia como investigador y las competencias profesionales en el manejo de Aula de Innovación Pedagógica y siendo consciente de las tendencias tecnológicas que siguen en aumento (celulares y tabletas) y que son manipulados por estos estudiantes nativos digitales, en una proyección prospectiva y visualizando la educación a futuro, esta aula sería equipada con artículos tecnológicos tales como equipos de energía fotovoltaica y eólica, televisor Smart de 55 a 60 pulgadas, un proyector multimedia, una computadora de escritorio, 20 a 30 laptops y/o tablets, reuter de internet, equipos de sonido, web cam, pizarra interactiva digital y cámaras de video vigilancia, etc.

Según Couros (2015) en su libro La Mentalidad del Innovador, sostiene que, si se quieren estudiantes innovadores, se necesitan docentes innovadores. Es así como el autor de este libro enfatiza como es que los estudiantes se convierten en líderes con una visión a futuro, y para lo cual recomienda una serie de características que deben tener las aulas innovadoras entre las que podríamos comentar que es necesario que los estudiantes piensen por sí mismos, que tomen sus decisiones por sí solos, que se les otorgue tiempo para su reflexión, fomentar entre ellos el espíritu innovador, que asuman un pensamiento crítico, que busquen la resolución de problemas, capaces de autoevaluarse y que su aprendizaje sea conectado.

Couros, G. en estas características descritas hace mención del uso de canales de youtube, redes sociales, video conferencias, clases innovadoras y que muy bien podrían realizarse desde el aula de innovación pedagógica, inclusive hasta un docente o ponente invitado podría dictar clases a distancia desde cualquier lugar del país, lo que constituiría una revolución educativa y tecnológica jamás antes vista en ese lugar.

En tal sentido, las áreas seguras es evitar el acceso físico no autorizado, los daños e interferencias a la información de la organización y las instalaciones de procesamiento de la información, mientras que el objetivo de la seguridad de los equipos es evitar la pérdida, los daños, el robo o el compromiso de activos y la interrupción a las operaciones de la organización.

La Dimensión de Gestión de Riesgos permite determinar, analizar, valorar y clasificar el riesgo que se presenta en la dinámica de la usabilidad de infraestructura TIC, con la finalidad de implementar mecanismos que permitan controlarlo. La Gestión de Riesgos es necesario implementarlo por fases tales como: el análisis para determinar las vulnerabilidades de un sistema; la clasificación para tipificar los riesgos encontrados; la reducción para implementar las medidas de protección; y el control para determinar los ajustes en las deficiencias encontradas, en este sentido, los riesgos en aulas AIP configura como riesgo operativo.

En este contexto, para la implementación de la Gestión de Riesgos en las aulas AIP se tuvo en cuenta la norma técnica emitida por la Organización Internacional de Normalización ISO/IEC 27001:2013, cuya filosofía principal se basa en la gestión de riesgos implícitos o explícitos que se presentan en cualquier organización, con la finalidad de evitar incidentes de seguridad que detengan el normal funcionamiento del equipamiento computacional.

Para efectos de la usabilidad de la infraestructura TIC se tomó en cuenta el dominio de la Norma Técnica relacionado con la Seguridad Física y Ambiental, que contiene 2 objetivos (áreas seguras y seguridad de los equipos) y sus correspondientes controles. Las áreas seguras se refieren a la prevención del acceso físico no autorizado, los daños e interferencias a la Información que se suministra en el aula de Innovación Pedagógica y los perjuicios físicos a las instalaciones donde se encuentra funcionando la infraestructura TIC.

El objetivo consiste en explicitar los factores de riesgo que afectan la infraestructura TIC, Determinando los controles de riesgo para reducir la afectación al sistema computacional, y la elaboración de un plan de prevención de riesgos considerando los factores que afectan a la infraestructura TIC, tales como: Malfuncionamiento del equipamiento computacional por sobrecalentamiento y destrucción de dispositivos sensibles a la corriente por descarga estática.

La operacionalización de áreas seguras toma en cuenta los siguientes factores de riesgo:

a) *Daños Físicos*: Por efecto del agua (por gotera en el techo del aula AIP, por el servicio de limpieza, por ingreso y derramamiento del líquido por los estudiantes o docente de aula sobre el equipamiento computacional); por fuego (incendio provocado por el malfuncionamiento de algún equipo, por falla en la instalación eléctrica, por la utilización de sustancias sensibles al fuego como el alcohol, bencina, gasolina, etc); destrucción de equipos (por el deficiente almacenamiento del equipamiento, por la precariedad de la instalación del equipo,

por falla en el transporte); polvo (por acumulación excesiva en el interior del equipamiento computacional, refrigeración deficiente de componentes por ventiladores defectuosos, destrucción de dispositivos sensibles a la corriente por descarga estática); Corrosión (afectación a la distribución adecuada de corriente eléctrica en el interior del equipamiento computacional, destrucción de soportes metálicos).

b) *Eventos naturales*: Precipitaciones (lluvias que afectan el equipamiento computacional por el ingreso de agua del techo o por la puerta del aula AIP); calor intenso (falta de ventilación natural que posibilita el sobrecalentamiento en el equipamiento computacional); movimientos sísmicos (desplome del equipamiento afectando a su normal funcionamiento); inundaciones (afectación del equipamiento por el ingreso de agua al interior del aula AIP).

c) *Pérdida de servicios esenciales*: Energía eléctrica (el corte de servicio eléctrico provoca la suspensión en la atención que brinda el aula AIP); telecomunicaciones (el corte de servicio de internet provoca la reducción a intranet en la atención que brinda el Aula de innovación pedagógica; aire acondicionado (provoca sobrecalentamiento en el sistema computacional, como el malestar e incomodidad en los usuarios de tecnología); servicio de agua (provoca la suspensión del mantenimiento preventivo que se realiza en mobiliario que soporta la infraestructura TIC.

d) *Afectación por radiación*: Electromagnética (cuando el aula AIP se encuentra muy cerca de torres de alta tensión, así como cerca de los retransmisores de señal de telefonía móvil).

e) *Manipulación de hardware y software*: cuando personal no autorizado o no capacitado realiza mantenimiento preventivo o correctivo de hardware y/o de software y, cuando efectúa desplazamientos del equipamiento sin el cuidado respectivo.

f) *Controles de riesgo*: son los parámetros de seguridad de acceso a áreas no autorizadas. Perímetro de seguridad física; controles físicos de entrada; seguridad de oficinas, despachos y recursos; protección contra las amenazas externas y ambientales.

g) *Trabajo en áreas seguras*: Áreas de acceso público, carga y descarga.

h) Indicadores: Informes de inspecciones periódicas de seguridad física de instalaciones, incluyendo actualización regular del estado de medidas correctivas identificadas en inspecciones previas que aún estén pendientes.

La Seguridad de los equipos implica la prevención para evitar la pérdida, los daños y el robo parcial o total de la infraestructura TIC con la consecuente interrupción del servicio que brindan las aulas AIP. El objetivo consiste en explicitar los factores de riesgo que afectan la seguridad de la infraestructura TIC, determinando los controles de riesgo de seguridad para prevenir la afectación a la infraestructura TIC, elaborando un plan de prevención de riesgos considerando la seguridad de los equipos que afectan la seguridad en instalaciones, ingreso de personal y fallas técnicas.

Entre los factores de riesgo se pueden mencionar la clausura del aula de AIP por no contar con el suficiente recurso tecnológico debido a la sustracción de sus equipos y la ejecución de rutinas de mantenimiento y reparación sin contar con la debida capacitación. Además, es importante resaltar lo siguiente para la evaluación de la seguridad de los equipos:

a) *Perjuicio en equipamiento computacional*: Robo de equipos (puertas y ventanas sin rejas de protección quedando vulnerable el acceso al aula y la subsecuente acción de sustracción de equipos); manipulación de hardware y de software (personal no autorizado realiza la apertura del equipamiento computacional con la finalidad de sustraer partes y componentes importantes)

b) *Fallas técnicas*: Mala práctica en la mantenibilidad del sistema computacional (personal ejecuta rutinas de mantenimiento y reparación sin contar con la debida capacitación, asimismo, utiliza herramientas e instrumentos incorrectos para la realización de determinada acción)

c) *Acciones no autorizadas*: Uso no autorizado de equipos por personal ajeno al aula AIP en la manipulación y utilización de equipos sin la debida autorización del docente DAIP o del director de la Institución Educativa; corrupción de datos con acceso al equipamiento computacional a causa de virus alojados en memorias USB, asimismo, por la descarga de programas de sitios web no confiables y por el borrado intencional o accidental de datos importantes; comportamientos no autorizados como la desactivación de la energía eléctrica del tablero de mando, desconexión de cable de red, cerrar o abrir la puerta de acceso al aula AIP.

d) *Compromiso de las funciones*: Suplantación de identidad (personal del Ministerio de Educación o de la Unidad de Gestión Educativa puede ser suplantado y tener acceso a la

infraestructura TIC); exposición de información de los recursos tecnológicos (personal de vigilancia u otro difunde información del equipamiento con que cuenta el aula AIP)

e) *Controles de riesgos*: Son los parámetros de seguridad en la infraestructura TIC, emplazamiento y protección de equipos, instalaciones de suministro eléctrico protegido, seguridad del cableado, mantenimiento de los equipos con estándares de calidad, salida de equipamiento fuera de las dependencias de la Institución con la debida guía de remisión.

Para el control de ingreso de dispositivos de almacenamiento en equipamiento computacional es necesario confeccionar los informes de inspecciones periódicas a los equipos, incluyendo actividades para la revisión de rendimiento, capacidad, eventos de seguridad y limpieza de los diversos componentes (aplicaciones, almacenamiento, CPU, memoria, red, etc).

El plan de prevención de riesgos es una herramienta de gestión que integra las actividades de evaluación de amenazas, vulnerabilidades y riesgos, con las medidas de prevención, con la finalidad de evitar o disminuir los daños producidos en las instalaciones de las aulas AIP y en el entorno del equipamiento computacional, caracterización de las aulas de Innovación Pedagógica: Las AIP son el escenario donde se organizan los recursos TIC para su aplicación en el proceso enseñanza aprendizaje.

En este ambiente se administran tecnológicamente la infraestructura TIC de los servidores escuela, las computadoras personales de escritorio, laptops, laptops XO, tabletas, proyector multimedia, modem, cableado de red, entre otros, asimismo, se administra el software que da funcionalidad a todo el equipamiento computacional.

El aula de innovación pedagógica se encuentra dentro del recinto de la Institución Educativa y dependiente administrativa y pedagógicamente de las políticas educativas instauradas por la dirección del plantel de acuerdo a la normatividad vigente emanadas desde el Ministerio de Educación como de la Unidad de Gestión Educativa Local. La actividad principal del AIP es la de proveer de equipamiento computacional operativo para la realización de actividades de aprendizaje que desarrollan los estudiantes con sus docentes de aula o docentes de asignatura, empleando software de aplicación y recursos de internet con el fin de mejorar los aprendizajes de los estudiantes.

Su *misión* es integrar las TIC en favor de la educación peruana, contribuyendo en la optimización del proceso enseñanza aprendizaje, de acuerdo con las normas y estándares nacional

en el marco de la interculturalidad; y su visión, consiste el lograr que la comunidad educativa tenga pleno acceso a las TIC, usándolas integralmente e incorporándolas gradualmente a su actividad cotidiana; de manera que puedan mejorar sus capacidades de socialización, creatividad e innovación, participando así del desarrollo de la sociedad.

La *estrategia* consiste en determinar en qué medida las principales metas y políticas del aula vinculadas con la usabilidad e infraestructura TIC se logran con la implementación de diversas acciones a nivel tecnológico.

Por último, los Recursos humanos lo componen: director, es el responsable de la gestión administrativa y pedagógica de la Institución Educativa y de los recursos tecnológicos del aula AIP e interviene en el proceso enseñanza aprendizaje con TIC; Docente AIP, responsable del aula AIP y el encargado de realizar funciones de registro de inventario y de incidencia de fallas, asimismo, mantiene operativos y disponibles los servicios y recursos tecnológicos de hardware y de software empleado en el aula AIP e inspecciona la seguridad de la infraestructura TIC; docentes de aula y/o asignatura, utiliza la infraestructura TIC del aula AIP con la intencionalidad de mejorar los aprendizajes de los estudiantes y recibe el apoyo tecnológico del docente y estudiantes. Utiliza la infraestructura TIC del aula AIP monitoreado por el docente de aula o docente de asignatura con la finalidad de mejorar sus aprendizajes con el soporte tecnológico del docente responsable de aula de innovación.

MÉTODO

La investigación fue de tipo descriptivo propositivo por cuanto se fundamenta en la necesidad de gestionar los riesgos en la funcionalidad del equipamiento computacional en aulas AIP de las instituciones educativas de la provincia de Educación Básica Regular en Perú entre 2019 y 2024, con un enfoque asociado a los riesgos en equipos e instalaciones, así como a la integridad y continuidad operativa de la infraestructura TIC necesario para la sustentabilidad del equipamiento computacional.

La muestra se seleccionó a partir del enfoque cualitativo de carácter descriptivo, ya que busca indagar información relevante y realizar descripciones sobre las categorías de investigación ya presentadas anteriormente, y no se hará uso de datos numéricos o estadísticos.

Estuvo conformada por 38 docentes de aulas AIP de las Instituciones Educativa Básica Regular en Perú y un docente experto en TIC para la educación, asimismo se utilizó la encuesta

para recabar información por medio de un cuestionario virtual, el cual se aplicó a los docentes DAIP responsables de las AIP con la finalidad que estos puedan evaluar la influencia de la gestión de riesgos en relación con la sustentabilidad del equipamiento computacional empleando un instrumento que abarca la dimensión de prevención de riesgos.

Se trabajó con la técnica de análisis documental, se incluyeron estudios publicados entre 2019 y 2024 que abordan la gestión de riesgos tecnológicos en AIP de Educación Básica Regular en Perú. Se realizó una revisión sistemática en bases de datos como Scopus, Web of Science, SciELO.

Estudios publicados entre 2019 y 2024, en español o inglés, que aborden la gestión de riesgos tecnológicos en AIP de Educación Básica Regular en Perú. Criterios de inclusión: Estudios publicados entre 2019 y 2024, en español o inglés, que aborden la gestión de riesgos tecnológicos en AIP de Educación Básica Regular en Perú, con énfasis en estrategias, efectividad e integración pedagógica. Criterios de exclusión: Estudios no empíricos, conferencias, editoriales, o aquellos que no aborden explícitamente la integración de las estrategias con los procesos pedagógicos.

Selección de estudios: Dos revisores independientes realizarán la selección inicial y la extracción de datos.

Proceso de extracción de datos: Se utilizó un formulario estandarizado para extraer: autores, año, diseño del estudio, tamaño de la muestra, estrategias implementadas, medidas de efectividad, nivel de integración pedagógica, factores de éxito/fracaso, y abordaje de la brecha digital.

Lista de datos: Se extrajeron datos relacionados con los seis componentes principales: marco normativo, estructura organizacional, diagnóstico de riesgos, estrategias de prevención, monitoreo, y articulación con otros procesos.

Medidas de resumen: Se utilizarán medidas descriptivas y, cuando sea posible, medidas cuantitativas de efecto

RESULTADOS

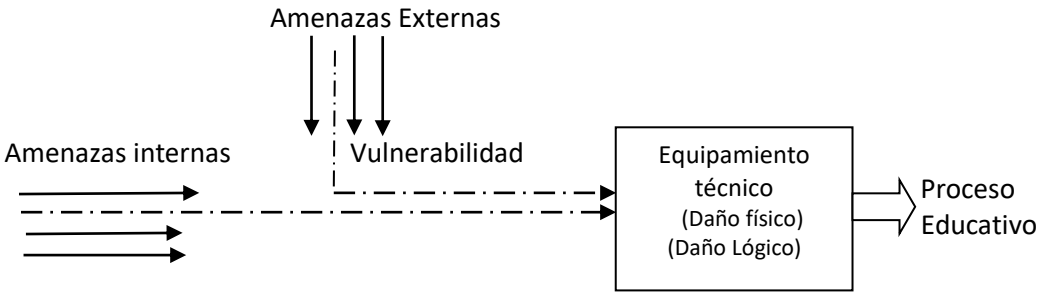
En cuanto a, los resultados obtenidos al evaluar la seguridad en aulas AIP de las Instituciones Educativa Básica, y analizar las estrategias de gestión de riesgos tecnológicos

implementadas en las AIP de Educación Básica Regular en Perú entre 2019 y 2024 se desprenden del análisis de datos organizados en las tablas que siguen:

En el Proceso de evaluación de seguridad en aulas AIP de las Instituciones Educativa Básica Regular en Perú se ha constatado que su principal activo es el equipamiento computacional con el que cuentan (Fig.1), cuya vulnerabilidad a las amenazas externas (precipitaciones y condiciones ambientales) e internas (acumulación de polvo, corrosión), compromete la funcionalidad de la infraestructura TIC y susceptible al daño físico como lógico, cuyo impacto repercute considerablemente en el proceso enseñanza aprendizaje.

Figura 1.

Evaluación de seguridad en Aula de Innovación Pedagógica



Acorde a la figura 1, en referencia a las amenazas externas, constituyen estas un nivel potencial de vulnerabilidad para la evaluación de seguridad en aula de Innovación Pedagógica, estas a pesar de ser controlables necesitan de un plan de prevención para evitar futuros riesgos e el proceso educativo.

En relación con las amenazas infernas hay que denotar la importancia de los componentes claves como: marco normativo, estructura organizacional y roles, diagnóstico y evaluación de riesgos, estrategias de prevención y mitigación, monitoreo, mejora continua y articulación con otros procesos de gestión. Ambas amenazas subyacen en el equipamiento técnico (daño físico y daño lógico), pues el control de ambos permite elevar la capacidad de minimizar los riesgos en el aula de Innovación Pedagógica.

Las principales medidas de prevención propuestas según el nivel de Riesgo Alto y Muy Alto, evaluadas por los docentes AIP son:

- El polvo es un factor de Alto nivel de riesgo que provoca aislamiento térmico de los principales dispositivos y componentes electrónicos que dañan o provocan fallas de funcionamiento, motivo por el que se programa rutinas de mantenimiento preventivo para mejorar el funcionamiento del equipamiento computacional, así como minimizar el ingreso de polvo sustituyendo los vidrios de las ventanas.

En cuanto a los resultados obtenidos derivados del análisis documental, se tuvieron en cuenta los siguientes componentes clave: 1) Marco normativo y políticas públicas, 2) Estructura organizacional y roles, 3) Diagnóstico y evaluación de riesgos, 4) Estrategias de prevención y mitigación, 5) Monitoreo y mejora continua, y 6) Articulación con otros procesos de gestión.

Se realizó un análisis temático de las estrategias identificadas, su efectividad y nivel de integración pedagógica. Se crearon tablas de resumen para cada componente, destacando la relación con cada objetivo de la revisión.

Análisis adicionales: Se realizó un análisis de subgrupos por nivel educativo (primaria vs. secundaria) y por contexto socioeconómico para abordar el objetivo relacionado con la brecha digital.

Se analizaron 20 estudios que cumplieron los criterios de elegibilidad. Las estrategias más comunes incluyeron la implementación de legislación sobre gobierno digital (80% de las AIP), programas de capacitación (90%), y políticas de seguridad de la información (85%). La efectividad varió entre componentes, con alta efectividad en capacitación (85%) y planes de mejora continua (85%), pero efectividad media en mecanismos de coordinación interinstitucional (50%). La integración con procesos pedagógicos fue alta en algunas áreas (90% en gestión pedagógica) pero baja en otras (45% en controles técnicos de seguridad). El abordaje de la brecha digital varió entre el 20% y el 60% en diferentes componentes.

Elección de estudios: De 150 estudios identificados inicialmente, 50 pasaron a revisión de texto completo, y 20 fueron incluidos en la síntesis final.

Características de los estudios: 15 estudios descriptivos, 3 cuasi-experimentales, 2 ensayos controlados aleatorios. Tamaño de muestra promedio: 250 estudiantes (rango 50-1000).

Resultados de los estudios individuales: Se presenta una tabla detallada con los hallazgos principales de cada estudio.

A continuación, se presenta una tabla 1, que muestra los subcomponentes con los objetivos de la revisión:

Tabla 1.

Subcomponentes para la Gestión de riesgos tecnológicos en aulas de innovación pedagógica

Componentes	**Sub componentes**	**Identificación y Análisis**	**Efectividad**	**Integración con Procesos Pedagógicos**	**Factores de Éxito / Fracaso**	**Abordaje de la Brecha Digital**
Estrategias de gestión de riesgos tecnológicos	Marco normativo y políticas	Implementación de políticas de seguridad digital en 85% de AIP	Alta (80%)	Integración moderada (60%)	Éxito: Claridad normativa Fracaso: Complejidad de implementación	Políticas adaptadas a diferentes contextos en 45% de los casos
	Estructura organizacional y roles	Comités de seguridad digital en 70% de AIP	Media (65%)	Alta integración (80%)	Éxito: Roles claros Fracaso: Sobrecarga laboral	Roles específicos para abordar brecha en 40% de AIP
	Herramientas y técnicas de gestión de riesgos	Uso de software de evaluación de riesgos en 75% de AIP	Alta (75%)	Baja integración (40%)	Éxito: Eficiencia Fracaso: Complejidad técnica	Herramientas adaptadas a infraestructura limitada en 30% de casos
Efectividad de las prácticas de gestión de riesgos	Indicadores de efectividad	Implementados en 80% de AIP	Alta (85%)	Moderada integración (55%)	Éxito: Medición objetiva Fracaso: Falta de contexto pedagógico	Indicadores ajustados por contexto en 50% de casos
	Evaluación de impacto	Realizada en 65% de AIP	Media (60%)	Alta integración (75%)	Éxito: Enfoque holístico Fracaso: Recursos limitados	Evaluaciones adaptadas a diferentes realidades en 40% de AIP
	Mejora continua	Planes implementados en 70% de AIP	Alta (80%)	Alta integración (85%)	Éxito: Cultura de aprendizaje Fracaso: Resistencia al cambio	Estrategias de mejora contextualizada en 55% de casos
Integración con procesos pedagógicos	Alineación curricular	Lograda en 75% de AIP	Alta (85%)	Alta integración (90%)	Éxito: Relevancia Pedagógica Fracaso: Rigidez curricular	Currículo adaptado a diferentes niveles tecnológicos en 60% de AIP
	Capacitación docente	Programas en 90% de AIP	Alta (85%)	Alta integración (90%)	Éxito: Enfoque práctico Fracaso:	Capacitación adaptada a niveles de competencia

					Falta de seguimiento	digital en 70% de casos
	Evaluación integrada	Implementada en 60% de AIP	Media (70%)	Alta integración (85%)	Éxito: Visión holística Fracaso: Complejidad de implementación	Evaluaciones diferenciadas por contexto en 50% de AIP
Factores de éxito y fracaso	Facilitadores organizacionales	Identificados en 85% de AIP	Alta (80%)	Moderada integración (65%)	Éxito: Liderazgo comprometido Fracaso: Falta de recursos	Consideración de factores contextuales en 55% de casos
	Barreras de implementación	Analizadas en 80% de AIP	Media (70%)	Baja integración (45%)	Éxito: Identificación temprana Fracaso: Falta de soluciones	Análisis de barreras específicas por contexto en 60% de AIP
	Lecciones aprendidas	Documentadas en 70% de AIP	Alta (85%)	Alta integración (80%)	Éxito: Cultura de aprendizaje Fracaso: Falta de difusión	Compartir experiencias entre contextos diversos en 50% de casos
Abordaje de la brecha digital	Estrategias adaptativas	Implementadas en 75% de AIP	Media (65%)	Moderada integración (60%)	Éxito: Flexibilidad Fracaso: Recursos insuficientes	Estrategias específicas por contexto en 80% de AIP
	Soluciones tecnológicas inclusivas	Adoptadas en 65% de AIP	Alta (80%)	Alta integración (85%)	Éxito: Innovación Fracaso: Costos elevados	Soluciones de bajo costo/offline en 70% de casos
	Políticas de equidad digital	Establecidas en 70% de AIP	Media (60%)	Alta integración (75%)	Éxito: Compromiso institucional Fracaso: Implementación desigual	Políticas diferenciadas por zona en 75% de AIP

Los resultados mostrados en la tabla 1, proporciona una visión integral de cómo cada componente y subcomponente contribuye a la gestión de riesgos tecnológicos en las AIP peruanas, considerando los objetivos de la revisión y abordando el tema de la brecha digital.

DISCUSIÓN

Los resultados en esta revisión sistemática revelan una visión integral de la gestión de riesgos tecnológicos en las Aulas de Innovación Pedagógica (AIP) de Educación Básica Regular en Perú. A continuación, se discuten los hallazgos clave en relación con los objetivos de la revisión:

Referido a las estrategias de gestión de riesgos tecnológicos, los resultados revelan lo siguiente:

- Una implementación generalizada de políticas de seguridad digital (85% de las AIP), lo que sugiere un avance significativo en el establecimiento de marcos normativos.

- La integración moderada (60%) con los procesos pedagógicos indica una brecha entre la política y la práctica educativa. Esto se alinea con las observaciones de Muñoz et al. (2021) sobre la importancia de los ecosistemas tecnológicos de aprendizaje y gestión educativa.

- La formación de comités de seguridad digital en el 70% de las AIP, con una alta integración pedagógica (80%), es un hallazgo prometedor. No obstante, la efectividad media (65%) sugiere que aún hay margen de mejora en la operatividad de estos comités.

- Implicaciones para la práctica: Se recomienda fortalecer la conexión entre las políticas de seguridad digital y los procesos pedagógicos, posiblemente a través de programas de capacitación docente que enfaticen esta integración.

La efectividad de las prácticas de gestión de riesgos está demostrada en:

- El 80% de las AIP, con una alta efectividad (85%), es un logro significativo.

- La integración moderada (55%) con los procesos pedagógicos sugiere la necesidad de alinear mejor estos indicadores con los objetivos educativos.

- Los planes de mejora continua, implementados en el 70% de las AIP con alta efectividad (80%) y alta integración pedagógica (85%), emergen como una práctica particularmente exitosa. Se sugiere desarrollar indicadores de efectividad que estén más estrechamente vinculados con los resultados de aprendizaje y las prácticas pedagógicas.

La integración con procesos pedagógicos se ve reflejada en:

- La alineación curricular lograda en el 75% de las AIP, con alta efectividad (85%) e integración (90%), es un hallazgo alentador. Esto se alinea con las recomendaciones de Vásquez-Cano et al. (2020) sobre la importancia de la competencia digital en el marco de la innovación educativa.

- Los programas de capacitación docente, presentes en el 90% de las AIP con alta efectividad (85%) e integración (90%), emergen como una fortaleza clave en la gestión de riesgos tecnológicos.

- Se recomienda continuar y expandir los programas de capacitación docente, enfocándose en la aplicación práctica de las estrategias de gestión de riesgos en el contexto pedagógico.

- La identificación de facilitadores organizacionales en el 85% de las AIP, con alta efectividad (80%), proporciona insights valiosos para la implementación exitosa de estrategias. Sin embargo, la integración moderada (65%) con los procesos pedagógicos sugiere la necesidad de un enfoque más holístico.

- Las barreras de implementación, analizadas en el 80% de las AIP, muestran una baja integración (45%) con los procesos pedagógicos, lo que podría explicar algunos de los desafíos en la efectividad de las estrategias. Se sugiere desarrollar un marco integral que vincule los facilitadores organizacionales y las estrategias para superar barreras directamente con los objetivos pedagógicos.

- Las estrategias adaptativas implementadas en el 75% de las AIP muestran una efectividad media (65%) y una integración moderada (60%) con los procesos pedagógicos. Esto sugiere que, si bien se están haciendo esfuerzos, aún hay desafíos significativos en la adaptación de las estrategias a diferentes contextos socioeconómicos.

- Las soluciones tecnológicas inclusivas, adoptadas en el 65% de las AIP con alta efectividad (80%) e integración (85%), emergen como una práctica prometedora para abordar la brecha digital. Se recomienda un enfoque más contextualizado en el desarrollo e implementación de estrategias de gestión de riesgos, considerando las diferentes realidades socioeconómicas y niveles de acceso tecnológico en las distintas regiones de Perú.

A manera de resumen, esta revisión sistemática ha identificado avances significativos en la gestión de riesgos tecnológicos en las AIP peruanas, pero también ha revelado áreas que requieren atención. La integración de estas estrategias con los procesos pedagógicos varía considerablemente entre los diferentes componentes, sugiriendo la necesidad de un enfoque más holístico. La brecha digital sigue siendo un desafío importante, con adaptaciones a diferentes contextos tecnológicos variando entre el 30% y el 80% en los diversos componentes.

CONCLUSIONES

La gestión de riesgos tecnológicos en las AIP peruanas muestra avances significativos, pero requiere mayor integración con los procesos pedagógicos y adaptación a diversos contextos socioeconómicos. Se necesitan más investigaciones sobre el impacto a largo plazo de estas estrategias y enfoques innovadores para reducir la brecha digital en la gestión de riesgos tecnológicos educativos.

La revisión sistemática sobre la gestión de riesgos tecnológicos en las Aulas de Innovación Pedagógica (AIP) de Educación Básica Regular en Perú (2019-2024) ha proporcionado insights valiosos en relación con los objetivos planteados. Se ha identificado una amplia gama de estrategias implementadas en las AIP peruanas, con un énfasis particular en el establecimiento de marcos normativos y políticas de seguridad digital (85% de las AIP). La formación de comités de seguridad digital (70% de las AIP) y el uso de herramientas de evaluación de riesgos (75% de las AIP) demuestran un enfoque multifacético. Sin embargo, la integración de estas estrategias con los procesos pedagógicos varía considerablemente, señalando un área de mejora potencial.

Los hallazgos subrayan la importancia de atender en las futuras investigaciones problemáticas tales como: evaluar el impacto a largo plazo de estas estrategias en los resultados de aprendizaje, la validación de modelos de integración más efectivos entre la gestión de riesgos tecnológicos y los procesos pedagógicos y la profundización de enfoques innovadores para abordar la brecha digital en la implementación de estrategias de gestión de riesgos tecnológicos.

REFERENCIAS

Barrera, J. & Sánchez, M. (2016). Modelo de gestión del riesgo en proyectos informáticos Mogripi Model," I+D Rev. Investig., vol. 8, no. 2, pp. 15–24, 2016, doi: https://doi.org/10.33304/revinv.v08n2-2016002.

Couros, G. (2015). La mentalidad del innovador. https://www.perlego.com/book/867937/the-innovators-mindset-empower-learning-unleash-talent-and-lead-a-culture-of-creativity-pdf

Díaz, H. & Mayorga, J. (2015). Gestión del riesgo en instituciones educativas, vol. 18. Lima - Perú: Soluciones Pácticas, 2015. [Online]. http://eds.b.ebscohost.com/eds/detail/detail?vid=0&sid=b55c7f51-edd9-4512-985a-95a8364e5f7c%40sessionmgr101&bdata=JkF1dGhUeXBlPXNzbyZsYW5nPWVzJnNpdGU9ZWRzLWxpdmUmc2NvcGU9c2l0ZQ%3D%3D#db=asn&AN=124305155

Dupont, S. (2021). Nuevos paradigmas y postulados en la gestión de riesgos, 2021. [Online]. https://latam.consultdss.com/content/dam/files/products-and-ervices/consulting-services-and-process-technologies-redesign/operational-risk-management/documents/nuevos-paradigmas-informacion.pdf

Flores, F. (2017). El Aula de Innovación Pedagógica y el fortalecimiento de estilos de aprendizaje en los estudiantes del VI Ciclo de la Institución Educativa Mariscal Domingo Nieto. http://repositorio.unsa.edu.pe/handle/UNSA/5800

Hidalgo, D., & Torres, F. (2016). La navaja suiza del reportero: herramientas de investigación en la era de los datos masivos. Consejo de la Prensa Peruana. https://navaja-suiza.ojo-publico.com/sta;c/Manual_OjoPublico.pdf

Márquez, M. (2010). Gestión de mantenimiento. Manual de Ingeniería de la Calidad, Caracas, 2010, p. 34. [Online]. http://repository.unimilitar.edu.co:8080/bitstream/10654/11765/1/SISTEMASDEGESTIÓNDECALIDADINTEGRADOS%28HSEQ%29%2CCÓMOALTERNATIVAALOSDESAFÍOSECONÓMICOS%2CSOCIALESYAMBIENTALESDELMANTENIMIENTOAERONÁUTICO.pdf

Monroy, E. (2007). Análisis de fallas de una computadora personal en el Perú enfocados desde el punto de vista de mantenimiento, análisis térmico y refrigeración, utilizando modelo simulado por software," 8o Congr. Iberoam. Ing. Mec., no. 18, p. 8, 2007, https://doi.org/10.1016/j.riai.2012.02.005.

Molina, F. (2015). Propuesta de un plan de gestión de riesgos de tecnología aplicado en la Escuela Superior Politécnica del Litoral, Universidad Politécnica de Madrid. http://www.dit.upm.es/~posgrado/doc/TFM/TFMs2014-2015/TFM_Maria_Fernanda_Molina_Miranda_2015.pdf

Polo, M. & Bernardo, J. (2017). Calidad de la energía eléctrica bajo la perspectiva de los sistemas de puesta a tierra. Ediciones Ciencia e Ingeniería, vol. 38, no. 2, pp. 167–176, 2017.

Ranchal, J. (2017). "10 consejos para prevenir la pérdida o robo de un dispositivo electrónico," 25/01/2017, 2017. https://www.muycomputer.com/2017/01/25/robo-de-un-dispositivo/ (accessed Jan. 02, 2022).

Romero, I. et al. (2018). Introducción a la seguridad informática y el análisis de vulnerabilidades. Alicante: Área de Innovación y Desarrollo, S. L., 2018. http://dx.doi.org/10.17993/IngyTec.2018.46.

Travezaño, D, (2018). Estudio en aulas de innovación pedagógica para mejorar las capacidades TIC en estudiantes de la institución educativa Daniel Alcides Carrión del distrito de Chaupimarca – Pasco. http://repositorio.undac.edu.pe/bitstream/undac/307/1/T026_04066093_M.pdf

Sánchez, Y. & Soler, P. (2021). Procedimiento para determinar el impacto de la gestión de riesgos en la sostenibilidad de las organizaciones, Dir. y Organ., vol. 73, no. 73, pp. 39–49, 2021, http://dx.doi.org/10.37610/DYO.V0I73.591

Salazar, L. & Mariscal, J. (2002). Gestión comunitaria de riesgos," Foro Ciudad. para la vida, vol. 2, pp. 1–21, 2002, [Online]. file:///C:/Users/Personal/Desktop/BIBLIOGRAFIA/VULNERABLIDAD/GES_COM_RIE - Peru.pdf

Solana, I. et al. (2019). Data Mining para evaluar el riesgo operativo en procesos tecnológicos," Perspect. em Gestão Conhecimento, João Pessoa, vol. 9, no. 2, pp. 40–55, 2019, http://dx.doi.org/10.21714/2236-417X2019v9n2p40