06

CIBERSEGURIDAD EN LA GERENCIA DE PROYECTOS: ANÁLISIS DOCUMENTAL DE ESTUDIOS PUBLICADOS EN LATINOAMÉRICA (2012 – 2023)

CYBERSECURITY IN PROJECT MANAGEMENT: A DOCUMENTARY ANALYSIS OF PUBLISHED STUDIES: DOCUMENTARY ANALYSIS OF PUBLISHED STUDIES IN LATIN AMERICA (2012–2023)

Fecha de recepción: 2024-08-28
Fecha de aceptación: 2025-07-14
Fecha de pubñicación: xxx

Daniel Armando Ciendúa Ricaurte, DACR[15]

Fabián David Güiza Pinzón, FDGP [16]

15 Ingeniero de Sistemas, Universidad de Boyacá, Gestión e innovación en TI, daciendua@uniboyaca.edu.co
16 Especialista en Gerencia Educacional, Magister en Gerencia de Proyectos, Magister en Didactica, Phd-EdD (c) en Educación, PMP® - Project Management Professional, PMP® - Profesional en Gerencia de Proyectos, SMPC® Scrum Master Professional, GPM PrisM® - Green Project Management Practitioner - Proyectos sostenibles, Universidad de Boyacá, Gestión e innovación en TI, fdguiza@uniboyaca.edu.co

RESUMEN

En el contexto actual de transformación digital, la ciberseguridad se ha convertido en un componente estratégico para la sostenibilidad y eficiencia de las organizaciones. La gerencia de proyectos, al integrar tecnologías de la información para planificar, ejecutar y controlar iniciativas, se enfrenta a crecientes amenazas cibernéticas que comprometen la integridad de los sistemas, la confidencialidad de los datos y la continuidad operativa. Esta problemática adquiere particular relevancia en América Latina, donde la adopción tecnológica avanza, pero persisten debilidades estructurales en la gestión de riesgos digitales y en la formación del talento humano. La presente investigación tuvo como objetivo analizar los estudios publicados en Latinoamérica con relación a la ciberseguridad en la gerencia de proyectos (2012-2023). La investigación se desarrolló a partir de un enfoque cualitativo de tipo documental, apoyado en la técnica de análisis narrativo de alcance interpretativo. Las fuentes de información secundarias fueron seleccionadas por muestreo no probabilístico por conveniencia y la recolección de datos se realizó mediante una ficha de resumen analítico. Los hallazgos permitieron identificar que la información científica publicada a la fecha es limitada; de hecho, son pocos los países latinos que han documentado sobre la ciberseguridad en estas áreas exponiendo los factores de riesgo y mutación de los delitos informáticos, así mismo se reconoce que, estos estudios se centran en categorizar las fallas a nivel tecnológico desde los sistemas de información que se manejan en los proyectos pero no en consenso con los tipos de ciberamenazas que se vinculan con la formación del talento humano administrativo que encabeza las operaciones financieras y manejo de datos, que permite la incidencia de riesgos por el desconocimiento de los mismos; lo que plantea la necesidad de fortalecer las capacidades digitales desde una perspectiva de gestión integral de proyectos.

Palabras clave:
Gerencia de proyectos, Ciberseguridad, Riesgos Digitales, Transformación Digital, Tecnologías de la Información y la Comunicación (TIC).

ABSTRACT

In the current landscape of digital transformation, cybersecurity has become a strategic component for the sustainability and operational efficiency of organizations. Project management, by integrating information technologies to plan, execute, and monitor initiatives, faces increasing cyber threats that compromise system integrity, data confidentiality, and business continuity. This issue is particularly relevant in Latin America, where technological adoption is advancing, yet structural weaknesses persist in digital risk management and in the training of human capital. This study set out to analyze academic publications from Latin America related to cybersecurity in project management between the years 2012 and 2023. It employed a qualitative documentary approach, supported by interpretive narrative analysis. Secondary sources were selected through non-probabilistic convenience sampling, and data collection was conducted using an analytical summary card as the main instrument. The findings revealed a notable gap in the existing literature, with few Latin American countries having documented cybersecurity issues in the context of project management. Those that have addressed the topic tend to focus on technological failures from the standpoint of information systems used in projects, while neglecting consensus on the types of cyber threats associated with the training and competencies of administrative personnel who oversee financial operations and data handling. This omission increases exposure to risk due to lack of awareness, underscoring the need to strengthen digital capacities from an integrated project management perspective.

Keywords:
Project Management, Cybersecurity, Digital Risks, Digital Transformation, Information and Communication Technologies (ICT).

RESUMO

No contexto atual de transformação digital, a segurança cibernética tornou-se um componente estratégico para a sustentabilidade e eficiência das organizações. A gestão de projetos, ao integrar tecnologias da informação para planejar, executar e controlar iniciativas, enfrenta crescentes ameaças cibernéticas que comprometem a integridade dos sistemas, a confidencialidade dos dados e a continuidade operacional. Essa questão é particularmente relevante na América Latina, onde a adoção tecnológica avança, mas persistem fragilidades estruturais na gestão de riscos digitais e no desenvolvimento de talentos humanos.

Esta pesquisa teve como objetivo analisar estudos publicados na América Latina sobre segurança cibernética em gestão de projetos entre 2012 e 2023. A pesquisa foi desenvolvida utilizando uma abordagem documental qualitativa, apoiada pela técnica de análise narrativa interpretativa. Fontes de informação secundárias foram selecionadas por meio de amostragem não probabilística por conveniência, e a coleta de dados foi realizada por meio de uma ficha de resumo analítico. Os resultados revelaram que a informação científica publicada até o momento é limitada; poucos países latino-americanos documentaram a segurança cibernética nessas áreas, expondo os fatores de risco e as mutações dos crimes cibernéticos. Reconhece-se também que esses estudos se concentram na categorização de falhas tecnológicas dos sistemas de informação gerenciados em projetos, mas não em consenso com os tipos de ameaças cibernéticas que estão vinculadas à formação de talentos humanos administrativos que lideram as operações financeiras e a gestão de dados, o que permite a incidência de riscos por desconhecimento dos mesmos; o que levanta a necessidade de fortalecer as capacidades digitais a partir de uma perspectiva integral de gestão de projetos.

INTRODUCCIÓN

En la era de la transformación digital, las organizaciones enfrentan un entorno cada vez más complejo, marcado por la interconexión de sistemas, la dependencia de plataformas tecnológicas y la exposición constante a riesgos cibernéticos. En este escenario, la ciberseguridad se ha consolidado como un eje transversal en la gestión estratégica de proyectos, dado que la integridad de la información y la continuidad operativa dependen, en gran medida, de la protección de los sistemas digitales utilizados en la planificación, ejecución y control de iniciativas.

La ciberseguridad, entendida como la práctica orientada a salvaguardar los sistemas digitales en el ámbito de las tecnologías de la información (Efthymiopoulos, 2019), ha adquirido un rol estratégico en la gerencia de proyectos (Campos, 2022; Lezama, 2023). Este creciente interés responde a la intensificación de ciberamenazas como filtraciones de datos (Romero, 2021) y otros delitos informáticos que afectan de manera directa la información operativa y financiera de las organizaciones (Senabre et al., 2021), comprometiendo la continuidad de los proyectos y la sostenibilidad institucional.

Si bien en la última década se ha observado una incorporación progresiva de la ciberseguridad en los procesos de gestión de proyectos (Álvarez y Hevia, 2020), aún persiste una brecha importante en su abordaje académico. Según Mendivil et al. (2022), el tema ha sido escasamente desarrollado desde la investigación científica, particularmente en el contexto latinoamericano (Medina et al., 2019), lo que contrasta con el avance de países europeos, asiáticos y norteamericanos (Ospina y Sanabria, 2020; Romero, 2021). Estas regiones han impulsado marcos de acción orientados a mitigar riesgos y establecer estrategias robustas que aseguren la gestión organizacional sin comprometer la confidencialidad, integridad ni calidad de la información (Angelini, Bonomi, y Palma, 2022).

En este sentido, la consolidación de estrategias de ciberseguridad en los proyectos no solo fortalece la capacidad organizacional frente a amenazas emergentes, sino que también permite articular políticas internas y externas bajo estándares de gobernanza informacional (Morán, 2021; Sanabre et al., 2021). Por ello, avanzar en el análisis y comprensión de este fenómeno en la región latinoamericana constituye una necesidad urgente tanto para el desarrollo científico como para la protección estratégica de los proyectos en un entorno digital cada vez más vulnerable.

En ese sentido, como lo plantean Álvarez y Ladino (2021), la ciberseguridad en el ámbito de la gerencia de proyectos continúa siendo un tema poco profundizado y visibilizado con la pertinencia que exige el contexto latinoamericano. La escasa atención se refleja en la limitada identificación y gestión de incidentes críticos, como lo evidencian los reportes de ataques informáticos, en su mayoría vinculados con vulnerabilidades no detectadas durante las etapas iniciales de ejecución del proyecto (Salazar & Avila, 2023; Zhou et al., 2022). A ello se suman desafíos vinculados al tratamiento legal de la información y a fallas técnicas específicas, como las relacionadas con la seguridad de las interfaces digitales y sus activos (Rivera y Contreras, 2022). Estas deficiencias, producto del desconocimiento de los profesionales administrativos que lideran estos procesos, ponen en riesgo los objetivos del proyecto al no implementarse acciones correctivas oportunas frente a las amenazas cibernéticas (Waters & Ahmed, 2020; Morán, 2021).

Por otra parte, la literatura especializada advierte que la limitada teorización e integración práctica de la ciberseguridad en los proyectos representa un obstáculo para la formación y desempeño de los profesionales en sus contextos laborales (Obando et al., 2022; Rivera y Contreras, 2022). Esta carencia se extiende, además, al ámbito educativo, donde se evidencia una débil inclusión del componente de ciberseguridad en los currículos de formación en ingeniería (Cano y Almaza, 2021) y en las disciplinas relacionadas con la gerencia de proyectos, dificultando así la preparación adecuada de los futuros profesionales para enfrentar las demandas contemporáneas de protección de la información (Domínguez-Domínguez, Flores-Laguna, y Valle-López, 2023).

Asimismo, se hace urgente visibilizar de forma crítica los delitos informáticos, no solo como eventos aislados, sino como indicadores de riesgos estructurales que deben ser comprendidos, diagnosticados y prevenidos desde una perspectiva estratégica. Tal como advierten Sviatun et al. (2021), abordar estos factores de riesgo y desventaja es esencial para que los actores responsables de las operaciones organizacionales incorporen mecanismos preventivos de manera proactiva, lo cual, como enfatiza Libién (2019), debe ser una prioridad dentro de toda estrategia de gestión de proyectos orientada a la sostenibilidad y la seguridad digital.

En esta línea, el presente artículo tuvo como objetivo central analizar los estudios publicados en Latinoamérica (2012 – 2023), que abordan la relación entre la ciberseguridad y la gerencia de proyectos. Este análisis se enmarca en la necesidad de destacar la relevancia estratégica que la ciberseguridad representa para la protección de la información organizacional y para la sostenibilidad de los negocios que las organizaciones gestionan en entornos crecientemente digitalizados (Yao & Soto, 2022).

De igual modo, se buscó identificar y sintetizar las apreciaciones que los autores analizados han formulado respecto a las ventajas y desventajas que la seguridad informática implica en el desarrollo y operación de proyectos y empresas, entendiendo que dichas percepciones son clave para configurar lineamientos de acción frente a las vulnerabilidades y fortalezas observadas en los sistemas digitales institucionales (Tomašević et al., 2020)

METODOLOGÍA

La presente investigación se desarrolló bajo un enfoque metodológico cualitativo, sustentado en un diseño documental (Zamora, 2019). El análisis aplicado fue de carácter narrativo, con un alcance interpretativo orientado a comprender los datos en su contenido contextual y semántico (Younas et al., 2023). En este sentido, se examinó la categoría de ciberseguridad en el ámbito de la gerencia de proyectos con el fin de identificar sus propiedades, ventajas, riesgos y demás elementos distintivos presentes en la producción científica recolectada (Schiliro, 2023).

Para tal propósito, se recurrió a fuentes secundarias seleccionadas mediante un muestreo no probabilístico por conveniencia (Hernández, 2021). Los criterios de inclusión fueron establecidos en correspondencia con la pertinencia temática respecto a la ciberseguridad en la gerencia o gestión de proyectos, exigiendo además que los textos correspondieran a estudios científicos o publicaciones académicas indexadas en metabuscadores y bases de datos como EBSCO, Dialnet, Google Académico, Scopus y E-libro. También se incluyeron documentos provenientes de repositorios institucionales de trabajos de grado de universidades nacionales y extranjeras, siempre que pertenecieran al contexto latinoamericano y estuvieran publicados entre 2012 y 2022.

En la siguiente tabla se presenta el esquema categorial de análisis, el cual tuvo como propósito codificar y organizar las unidades de búsqueda en categorías más delimitados y estructuradas, facilitando así su análisis e interpretación. Este esquema funcionó como una herramienta clave para establecer relaciones temáticas entre los distintos estudios seleccionados.

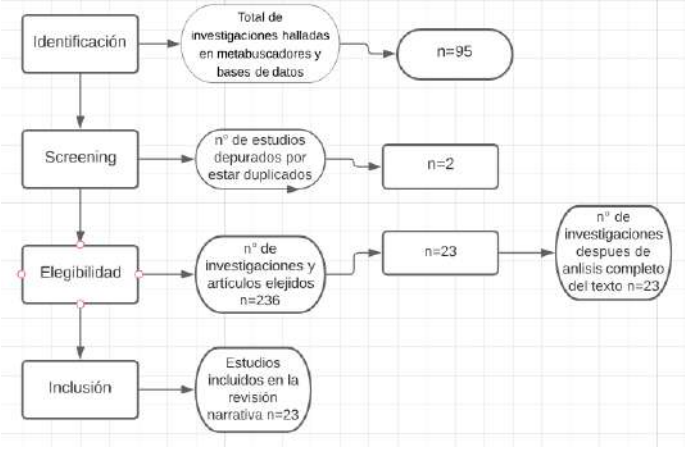
Tabla 1.
Esquema categorial de análisis.

Categoría central	*Subcategorías*	*Microcategorías*
Ciberseguridad en gerencia / gestión de proyectos	*Producción científica*	*Procedencia y características.*
	Ciberseguridad	• *Ventajas y riesgos documentados* • *Categorías comunes* • *Tipos de ciberamenazas registradas.*

Fuente. Elaboración propia.

El plan de análisis de la información y los datos recolectados se realizó mediante la aplicación de la técnica de revisión documental, empleando como instrumento la ficha técnica de resumen analítico (Franco y Solórzano, 2020). Esta herramienta permitió sistematizar los hallazgos de manera coherente y rigurosa, asegurando la trazabilidad de las categorías y subcategorías emergentes.

Figura 1.
Proceso de búsqueda, selección y análisis de investigaciones



Fuente: Elaboración propia.

La Figura 1 presenta un diagrama de flujo que ilustra el proceso de búsqueda, selección y análisis de investigaciones, correspondiente a una revisión documental sistemática sobre la relación entre la gerencia de proyectos y las Tecnologías de la Información y la Comunicación (TIC).

1. Fase de Identificación
En esta etapa inicial, se realizó una búsqueda exhaustiva de estudios a través de metabuscadores y bases de datos académicas, tanto nacionales como internacionales, incluyendo repositorios institucionales, libros digitales, informes técnicos y artículos científicos. El objetivo fue localizar documentos relevantes relacionados con la temática de estudio. Como resultado de esta búsqueda, se identificaron un total de 95 documentos (n=95).

2. Fase de Cribado (Screening)
Los documentos recuperados fueron sometidos a un proceso de depuración, eliminando duplicados y registros que no cumplían con los criterios básicos de selección. En esta fase, se excluyeron 2 estudios duplicados (n=2), lo que redujo el corpus de análisis.

3. Fase de Elegibilidad
Posteriormente, se analizaron 236 documentos en total que inicialmente cumplían con los criterios temáticos establecidos, enfocados en estudios que abordaban la intersección entre la gerencia de proyectos y el uso de TIC. Sin embargo, tras una lectura completa y detallada de los textos, sólo 23 investigaciones (n=23) fueron consideradas pertinentes para los objetivos de la revisión, por su relevancia, rigor metodológico y contextualización en escenarios relacionados.

4. Fase de Inclusión
Finalmente, los 23 estudios seleccionados fueron incluidos en la revisión narrativa. Esta etapa implicó un análisis cualitativo del contenido, destacando enfoques, beneficios, riesgos, adaptabilidad y aplicaciones prácticas de las TIC en proyectos de distinta índole. Asimismo, se consideraron experiencias de diferentes países que enriquecieron el análisis comparativo y ofrecieron perspectivas contextualizadas.

El diseño metodológico adoptado para esta revisión se alinea con los lineamientos generales de una revisión sistemática narrativa, que permite integrar información diversa desde un enfoque cualitativo. Se aplicaron filtros de inclusión y exclusión progresiva, guiados por criterios temáticos, metodológicos y de pertinencia contextual, con el proposito de construir un cuerpo de evidencia sólido para el análisis comparativo.

RESULTADOS

En adelante, se presentan los resultados acordes al esquema categorial de análisis. En ese sentido, la siguiente tabla condensa los hallazgos según la procedencia y características de la producción científica publicada (2012 – 2023).

Procedencia	Colombia 30,3% Chile 8%	Ecuador 4% Argentina 8%	Perú 30% Venezuela 8%	El Salvador 4% México 4%	
Enfoques metodológicos	Mixto 4%	Cuantitativo 60%	Cualitativo 36%		
Año de publicación	*2014 (1)* *2021 (5)*	2016 (1) 2022 (2)	2018 (2)	2019 (1) 2023 (8)	2020 (3)

Fuente. Elaboración propia.

A partir de los datos expuestos en la tabla 2, se observa que Colombia encabeza el número de investigaciones publicadas en el área, con una participación del 30,3 % del total de estudios identificados hasta 2023. De acuerdo con Ospina y Sanabria (2020), esta alta producción académica se relaciona directamente con el aumento sostenido de incidentes cibernéticos en organizaciones tanto públicas como privadas, lo que ha obligado a las entidades a implementar medidas urgentes de seguridad informática (Pattnaik et al., 2023). En este contexto, se han impulsado investigaciones que buscan visibilizar esta problemática como parte de una estrategia de gestión del riesgo informático (Valoyes, 2019; Jiménez et al., 2022).

Asimismo, este liderazgo en producción científica también se explica por los esfuerzos institucionales del Estado colombiano, que han promovido la recopilación de información técnica y contextual como insumo para la formulación de una política pública nacional de seguridad de la información. Diversas entidades han desarrollado líneas de acción que responden a esta necesidad, impulsando iniciativas en sectores estratégicos y generando aportes relevantes para el diseño de marcos normativos y técnicos (Álvarez y Ladino, 2021; Borrero, 2015; Villamil et al., 2020).

En particular, Cano (2020), los altos índices de producción científica en Colombia también se vinculan con la integración progresiva de la ciberseguridad en proyectos y operaciones dentro de los planes curriculares de formación profesional y de posgrado en diversas universidades del país. Esta inclusión ha sido impulsada, en parte, por la Asociación Colombiana de Ingenieros de Sistemas, la cual ha tomado como referencia los resultados investigativos desarrollados desde su institución, abordando tanto la seguridad de la información como las tendencias emergentes en infraestructura informática necesaria para el desarrollo eficiente de los negocios (Nkongolo, Mennega & Zyl, 2023; Kumar, 2004).

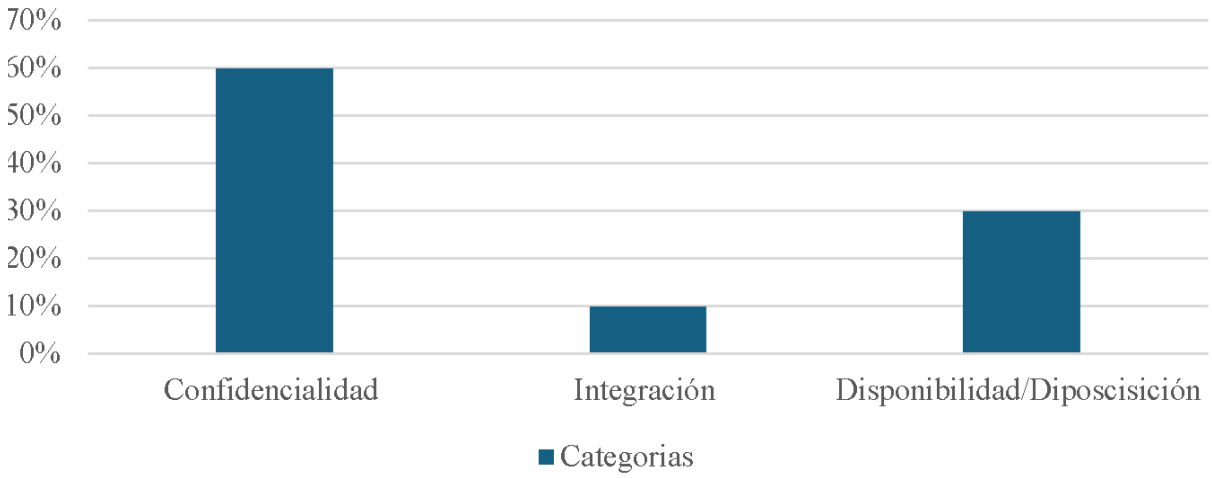
Por otro lado, Perú también destaca con el 30 % de los estudios analizados, ubicándose como uno de los países con mayor producción académica sobre ciberseguridad en proyectos, una situación que, según Poma y Vargas (2019) y Cerna y Peña (2023), responde a condiciones similares a las de Colombia, relacionadas con el incremento de ataques a sistemas de información, redes sociales y PYMES en el sector público y privado (Inoguchi & Macha, 2017). En contraste, se evidenció una participación significativamente menor en otros países latinoamericanos: Chile, Argentina y Venezuela con 8% cada uno, y Ecuador, El Salvador y México con 4% cada uno. Esta disparidad sugiere que la categoría de ciberseguridad aún no ha alcanzado la misma relevancia regional, particularmente en el cono sur, donde, como advierten Álvarez y Hevia (2020), los marcos de protección legal para la identificación y notificación de vulnerabilidades siguen siendo incipientes y poco desarrollados en proyectos y empresas (Campos, 2022; Lezama, 2023).

En relación con la naturaleza metodológica de los estudios analizados, se identificó que la mayoría se enmarcan en un enfoque cuantitativo, representando el 60 % del total. Esto evidencia una clara preferencia por el uso de herramientas estadísticas y numéricas para identificar tendencias, frecuencias y promedios sobre el fenómeno de estudio. En contraste, solo el 36 % de los trabajos presentan una orientación cualitativa, centrada en la interpretación contextual y subjetiva de los problemas vinculados a la ciberseguridad organizacional y al desarrollo operativo de los proyectos. Finalmente, solo un 4% de las investigaciones adopta un enfoque mixto, que busca integrar ambas perspectivas —cuantitativa y cualitativa— con el fin de generar una comprensión heurística más amplia de la realidad en la que se ejecutan estos procesos (Mendivil et al., 2022; Obando et al., 2022).

Respecto a la distribución temporal de las publicaciones, se observa una clara concentración en 2023. Según Feito et al. (2023), este aumento responde a la mutación y expansión de los delitos informáticos durante la pandemia de Covid-19, lo cual obligó a las organizaciones a implementar mecanismos de respuesta y adaptación frente a las nuevas amenazas digitales (Khatri, Cherukuri, & Kamalov, 2023). Por el contrario, se identificó una escasa producción entre 2014 y 2019, lo que sugiere que la ciberseguridad aún no era reconocida como una problemática recurrente dentro del ámbito de la gestión de proyectos (Libién, 2019). Estos hallazgos refuerzan la idea de que el auge de los delitos informáticos está directamente relacionado con las consecuencias disruptivas del contexto pandémico, como también lo confirman Flores (2023) y Gurumendi (2023).

Ahora bien, respecto a la figura 2 ilustra los hallazgos de la subcategoría Categorías Comunes identificados en las investigaciones publicadas a la fecha.

Figura 2.
Categorías halladas en los estudios publicados.



Fuente: Elaboración propia.

Teniendo en cuenta los hallazgos expuestos en la Figura 2, se identifica que 60% de los estudios analizados incorporan dentro de su estructura metodológica y referencial el análisis de la Confidencialidad como categoría central (Kamanzi & Romania, 2019). No obstante, este abordaje se ha orientado principalmente a identificar las afectaciones a la información bajo esta dimensión, particularmente en lo que respecta a las garantías que ofrece la gerencia de proyectos para controlar quiénes pueden acceder a la información y de qué manera se realiza dicho acceso durante el desarrollo de las operaciones organizacionales (Domínguez-Domínguez, Flores-Laguna, & Valle-López, 2023). En ese marco, los estudios puntualizan en los riesgos derivados de fugas de información y violaciones de privacidad, proponiendo estrategias preventivas frente a amenazas como el phishing, el robo de datos y otros ataques similares (Gupta et al., 2023). Es importante destacar que esta concentración temática responde al hecho de que dichas vulnerabilidades constituyen una de las formas más frecuentes de delincuencia informática a nivel global (Ramesh & Maheswari, 2012), lo cual explica su posicionamiento como una preocupación prioritaria en la agenda investigativa sobre ciberseguridad en proyectos.

En contraste, únicamente 30 % de las investigaciones analizadas se enfocaron en la categoría de Disponibilidad, centrando su atención en aspectos relacionados con el aseguramiento, la fiabilidad y el acceso oportuno a los datos durante las operaciones de los proyectos (Humblet et al., 2015). Estos estudios procuraron analizar cómo garantizar que la información esté accesible en el momento requerido, tanto para los usuarios como para los procesos internos críticos. En particular, se observaron contribuciones que profundizan en la evaluación de amenazas vinculadas a la denegación del servicio (DoS) y a la interrupción deliberada de los sistemas (Yang et al., 2022). Esta línea de investigación ha cobrado especial relevancia en áreas funcionales como las finanzas y el mercadeo, donde un ataque cibernético puede tener consecuencias significativas sobre el flujo de operaciones, comprometiendo la continuidad y el éxito del proyecto (Salmela, 2008).

Por último, sólo 10 % de las investigaciones revisadas se centraron en la categoría de Integridad, entendida como la garantía de que la información no sea alterada, manipulada o utilizada de forma indebida (Huberts, 2018). Esta categoría se asocia principalmente a la protección frente a la modificación no autorizada de datos, los cambios maliciosos y la suplantación de identidad. Según Caamaño y Gil (2020), este limitado abordaje puede explicarse por el hecho de que muchas investigaciones no profundizan en la estructura textual o descriptiva de la información vinculada a los procesos operativos y gerenciales de las organizaciones. En cambio, su enfoque se orienta a asegurar que dicha información no sea vulnerada ni manipulada por actores externos con fines ilícitos o distorsionadores (Domínguez-Domínguez, Flores-Laguna & Valle-López, 2023). Esta línea de análisis resulta crucial en contextos donde la integridad de los datos constituye un activo crítico para la toma de decisiones estratégicas y la sostenibilidad organizacional.

En relación con la subcategoría de Ventajas y Riesgos, se identificó que la totalidad de los estudios revisados incluye referencias explícitas a estos dos elementos como componentes fundamentales del análisis. En cuanto a las ventajas, los autores coinciden en que la implementación de estrategias de ciberseguridad en la

gestión de proyectos contribuye significativamente a la protección de los datos y a la reducción de pérdidas financieras (Kesswani & Kumar, 2015). Esto se debe a que los delitos informáticos no solo afectan la continuidad y productividad de los procesos operativos, sino que también generan impactos económicos relevantes sobre la inversión, el presupuesto y la preservación de la información crítica (Ayo et al., 2018).

De manera puntual, los estudios identifican ventajas concretas que fortalecen la gestión de proyectos frente a amenazas digitales, tales como: la evaluación del tipo y factor de riesgo, la implementación de controles preventivos, detectivos, compensatorios, correctivos y disuasorios, así como la utilización de sistemas de escaneo para la detección temprana de vulnerabilidades (Kamal et al., 2020). Estas acciones no sólo permiten anticiparse a posibles incidentes, sino que mejoran la capacidad de respuesta institucional y refuerzan la resiliencia operativa de los proyectos.

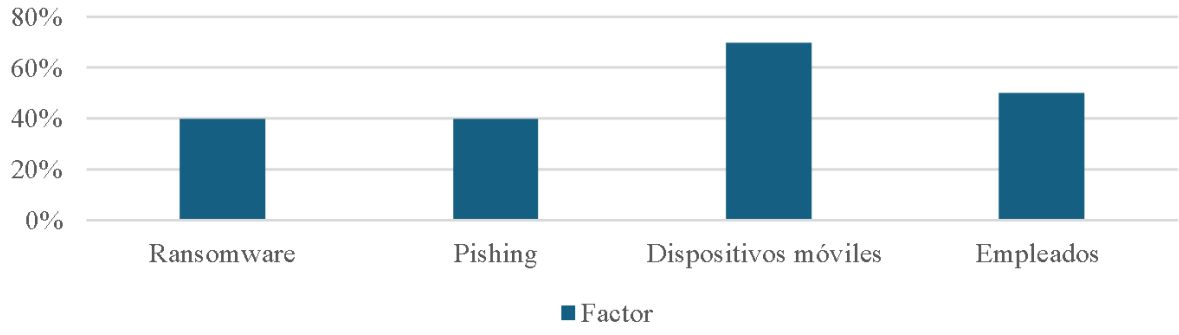
En cuanto a las desventajas, los estudios revisados coinciden en señalar que no existe un sistema de ciberseguridad que ofrezca una garantía del 100 % para la protección integral de la gerencia de proyectos, sus estrategias y la información frente a amenazas externas o delitos informáticos. Esta limitación se debe a que las prácticas delictivas en el entorno digital evolucionan constantemente, adoptando nuevas formas de operación que desafían los mecanismos existentes (Schiliro, 2023).

A ello se suma un factor recurrente identificado en las investigaciones: el elevado costo asociado tanto a la implementación como al mantenimiento de sistemas integrales de ciberseguridad. Este aspecto representa una desventaja crítica para muchas organizaciones, ya que implica la reasignación de recursos y la inversión de altos presupuestos, lo que puede dificultar la sostenibilidad financiera de estos sistemas en el largo plazo <Domínguez-Domínguez, Flores-Laguna, & Valle-López, 2023>.

Respecto a la categoría tipos de ciberamenazas registradas en las investigaciones, la Figura 3 ilustra los encontrados en los hallazgos.

Figura 3.

Tipos de Ciberamenazas.



Fuente: Elaboración propia.

De acuerdo con los hallazgos representados en la Figura 3, los dispositivos móviles constituyen uno de los principales factores de riesgo para la seguridad de la información durante el desarrollo de proyectos (Halpert, 2004). Como lo advierte Zamora (2019), estos dispositivos, que suelen ser entregados a los empleados para el almacenamiento y gestión de datos, no cuentan en muchos casos con sistemas de seguridad integral que los protejan frente a amenazas como malware o vulnerabilidades en los sistemas operativos móviles. Esta falta de protección expone datos sensibles a posibles accesos no autorizados, comprometiendo la integridad de las operaciones.

Asimismo, otro factor crítico identificado corresponde a la acción humana, particularmente la baja capacitación del personal en temas de protección de datos y gestión de riesgos. Esta carencia de formación representa una puerta de entrada a múltiples amenazas digitales. En esa misma línea, el phishing y el ransomware emergen como riesgos frecuentes y de alto impacto, ya que comprometen la seguridad mediante el cifrado malicioso de la información y su uso indebido (Darwin & Nkongolo, 2023). Estas amenazas afectan especialmente a procesos desarrollados a pequeña escala, los cuales, por lo general, no cuentan con infraestructuras técnicas ni proyecciones estratégicas que les permitan mitigar de manera efectiva dichas problemáticas (Tomašević et al., 2020).

CONCLUSIONES

Las investigaciones en ciberseguridad en la gerencia o gestión de proyectos entre 2012 y 2023 en el contexto Latinoamericano, en su mayoría están publicadas en Colombia y Perú, debido a que en estos países se han desarrollado procesos encaminados a la intervención sobre la incidencia continua de delitos informáticos reportados por entidades públicas y privadas, que, como consecuencia, han puesto en evidencia este problema y lo han sistematizado para adquirir insumos en pro de la formulación de una política nacional de seguridad de la información. Así mismo, esto se ha logrado a raíz de que las organizaciones académicas a través de sus procesos de monitoreo sobre las tendencias laborales, las necesidades de formación en su campo de acción con los negocios e infraestructura informática han motivado a las universidades a integrarlas dentro de su currículo, en procesos de formación posgradual y complementaria.

Por otro lado, la mayoría de investigaciones según su fecha de publicación fueron realizadas después o en el marco de la pandemia Covid -19, debido a que se observó una mutación de los delitos informáticos en áreas financieras y operativas de las empresas o departamento que son responsables de manejar información operativa y financiera de los proyectos.

Dentro de las categorías halladas en los estudios publicados, se identifica que la mayoría aborda la confidencialidad y disponibilidad de la información, exponiendo los riesgos y estrategias que se pueden ejecutar para contrarrestar los factores internos y externos que las comprometen, pero no en temas de integración que es responsabilidad con el manejo y capacitación de los colaboradores o funcionarios con los sistemas de información. Por último, los riesgos más comunes hallados en estos estudios son el Phishing, el Ransomware y la baja formación de los empleados en la manipulación y seguridad de la información y en consenso a los aparatos electrónicos e interfaces de navegación.

REFERENCIAS

Álvarez, M.A. A., & Ladino, D. *A. H. 2021). Análisis preliminar de la ciberseguridad asociada al sistema financiero en algunos países de Latinoamérica y la contribución de la informática forense. Cuaderno de investigaciones: semilleros andina, 1*(14).

Álvarez-Valenzuela, D., & Hevia Angulo, A. (2020). *Protección legal para la búsqueda y notificación de vulnerabilidades de ciberseguridad en Chile. Revista chilena de derecho y tecnología, 9*(2), 1-4.

Angelini, M., Bonomi, S., and Palma, A. (2022). A Methodology to Support Automatic Cyber Risk Assessment Review. arXiv (Cornell University). *https://doi.org/10.48550/arxiv.2207.03269*

Ayo, S. C. et al. (2018). Information Security Risks Assessment: A Case Study. arXiv (Cornell University). *https://doi.org/10.48550/arxiv.1812.04659*

Borrero, R. C. (2015). Estado actual de la política pública de ciberseguridad y ciberdefensa en Colombia. Revista de Derecho, Comunicaciones y Nuevas Tecnologías, (14), 4.

Caamaño Fernández, E.E. y Gil Herrera, R. J. (2020). Prevención de riesgos por ciberseguridad desde la auditoria forense: conjugando el talento humano organizacional. NOVUM, revista de Ciencias Sociales Apliacadas, / (10), 61-80.

Campos, J. *L. S. (2022). Vigencia Ontológica de la Ciberseguridad en el Marco de la Seguridad Informática Chilena. Convenio De Budapest. Aula Virtual, 3*(6), 132-148.

Cano, J., & Almanza, A. (2021). Reflexiones y retos para la academia en la formación de profesionales de seguridad/ciberseguridad en Colombia: 2010-2020. ISLA 2021 Proceedings. 7. *https://aisel.aisnet.org/isla2021/7/*

Cerna Arqueros, K. W., & Peña Villena, C. R. (2023). Estado del arte de la ciberseguridad para la prevención y detección temprana de la delincuencia cibernética en Perú (2018-2022) [Tesis de posgrado, Universidad Nacional de Trujillo]. Repositorio Institucional de la Universidad Nacional de Trujillo. *https://repositorio.unitru.edu.pe/*

https://dspace.unitru.edu.pe/items/e912abcf-c616-472a-9adc-d87f20181bc8

De Franco, M. F., & Solórzano, J. L. V. (2020). Paradigmas, enfoques y métodos de investigación: Análisis teórico. *Mundo Recursivo, 3*(1), 1-24.

Darwin, V., and Nkongolo, M. (2023). Data Protection for Data Privacy-A South African Problem?. arXiv (Cornell University).

Domínguez-Domínguez, R., Flores-Laguna, O. A., and Valle-López, J. d. (2023). Evaluation of an information security management system at a Mexican higher education institution. arXiv (Cornell University). *https://doi.org/10.48550/arxiv.2306.11050*

Efthymiopoulos, M. P. (2019). A cyber-security framework for development, defense and innovation at NATO. *Journal of Innovation and Entrepreneurship, 8*(1). *https://doi.org/10.1186/s13731-019-0105-z*

Feito, M. A.; Núñez, E. V.; López, P. B.; Agüero, R. R. & Marcos, C. R. (2023). El papel de la ciberseguridad en la era post-pandemia [Formación complementaria, Universidad de Educación a Distancia]. Repositorio institucional. *https://contenidosdigitales.uned.es/fez/view/intecca:GICCU-65080f9b21a8909017addbf5v*

Flores Mori, C. E. (2023). Incremento de los delitos informáticos a consecuencia de la pandemia del Covid-19 en la ciudad de Trujillo entre 2020-2021 [Tesis de posgrado, Universidad Cesar Vallejo]. Repositorio institucional. *https://repositorio.ucv.edu.pe/handle/20.500.12692/124989*

Gurumendi Párraga, D. *J. (2023). La importancia de tener Instituciones Educativas ciberseguras post pandemia. Journal of Alternative Perspectives in the Social Sciences, 11*(4).

Gupta, M. et al. (2023). From ChatGPT to ThreatGPT: Impact of Generative AI in Cybersecurity and Privacy. arXiv (Cornell University). *https://doi.org/10.48550/arxiv.2307.00691*

Halpert, B. (2004). *Mobile device security. Proceedings of the 1st annual conference on Information security curriculum development, 99*-101. *https://doi.org/10.1145/1059524.1059545*

Hernández González, O. (2021). *Aproximación a los distintos tipos de muestreo no probabilístico que existen. Revista Cubana de Medicina General Integral, 37*(3).

Huberts, L. *W. J. C. (2018). Integrity: What it is and why it is important. Public Integrity, 20*(sup1), S18–S32. *https://doi.org/10.1080/10999922.2018.1477404*

Humblet, M. et al. (2015). How to Assess Data Availability, Accessibility and Format for Risk Analysis?. *Transboundary and Emerging Diseases, 63*(6), e173-e186. *https://doi.org/10.1111/tbed.12328*

Inoguchi Rojas, A., & Macha Moreno, E. *L. (2017). Gestión de la ciberseguridad y prevención de los ataques cibernéticos en las PYMES del Perú, 2016* [Tesis de posgrado, Universidad de Lima]. Repositorio Institucional de la Universidad de Lima. *https://revistas.ulima.edu.pe/index.php/Advocatus/article/view/5114*

Jiménez Almeira, G. A. Morales Lince, M. P. & Patiño Sánchez, I. (2022). Ciberseguridad: una mirada a los métodos y estrategias de anticipación al avance del cibercrimen en Colombia y la región. En P. A. Sierra-Zamora, T. L. Fonseca-Ortiz, & F. Coronado-Camero (Eds.), De los delitos transnacionales, las Fuerzas Armadas y el tratamiento jurídico de la seguridad y defensa nacionales (pp. 137-155). Sello Editorial ESDEG. *https://doi.org/10.25062/9786287602120.04*

Kamal, A. H. A. et al. (2020). Risk Assessment, Threat Modeling and Security Testing in SDLC. arXiv (Cornell University). *https://doi.org/10.48550/arxiv.2012.07226*

Kamanzi, A., and Romania, M. (2019). *Rethinking Confidentiality in Qualitative Research in the Era of Big Data. American Behavioral Scientist, 63*(6), 743-758. *https://doi.org/10.1177/0002764219826222*

Kesswani, N., and Kumar, S. (2015). *Maintaining Cyber Security. Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research, 161*-164. *https://doi.org/10.1145/2751957.2751976*

Khatri, S., Cherukuri, A. K., and Kamalov, F. (2023). Global Pandemics Influence on Cyber Security and Cyber Crimes. arXiv (Cornell University).

https://doi.org/10.48550/arxiv.2302.12462

Kumar, R. *L. (2004). A Framework for Assessing the Business Value of Information Technology Infrastructures. Journal of Management Information Systems, 21*(2), 11-32. *https://doi.org/10.1080/07421222.2004.11045801*

Lezama, C. *R. Q. (2023). Ciberdefensa y ciberseguridad en el Perú: realidad y retos en torno a la capacidad de las FF. AA. para neutralizar ciberataques que atenten contra la seguridad nacional. Revista de Ciencia e Investigación en Defensa-CAEN, 4*(1), 55-76.

Lingham, A. D. et al. (2020). Implementation of Security Features in Software Development Phases. arXiv (Cornell University).

https://doi.org/10.48550/arxiv.2012.13108

Libién, H. *R. P. (2019). Cibercriminalidad y ciberseguridad en México. Ius Comitialis, 2*(4), 47-69.

Mendivil Caldentey, J., Sanz Urquijo, B. & Gutiérrez Almazor, M. (2022). *Formación y concienciación en ciberseguridad basada en competencias: una revisión sistemática de literatura. Pixel-Bit: Revista de Medios y Educación, 63*, 197-225.

Morán Maldonado, N. M. (2021). Estado de la ciberseguridad en las empresas del sector público del Ecuador: Una revisión sistemática [Tesis de posgrado, Universidad Politécnica Salesiana]. Repositorio Institucional de la Universidad Politécnica Salesiana. *https://dspace.ups.edu.ec/bitstream/123456789/20243/1/UPS-GT003204.pdf*

Nkongolo, M., Mennega, N., and Zyl, I. v. (2023). Cybersecurity Career Requirements: A Literature Review. arXiv

(Cornell University). *https://doi.org/10.48550/arxiv.2306.09599*

Obando-Ibarra, C., Garcés-Giraldo, L. F., Quiroz-Fabra, J., Benjumea-Arias, M., Valencia-Arias, A., Zavala, L. R. & Patiño-Vanegas, C. (2022). *Evaluación de riesgos en ciberseguridad: una revisión bibliométrica. Revista Ibérica de Sistemas e Tecnologias de Informação (E49), 396*-409.

Ospina Díaz, M. R., & Sanabria Rangel, P. *E. (2020). Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia. Revista Criminalidad, 62*(2), 199-217.

Pattnaik, N. et al. (2023). It's more than just money: The real-world harms from ransomware attacks. arXiv (Cornell University). *https://doi.org/10.48550/arxiv.2307.02855*

Poma, A., & Vargas, R. (2019). *Problemática en ciberseguridad como protección de sistemas informáticos y redes sociales en el Perú y en el mundo. Sciéndo, 22*(4), 275-282.

Ramesh, P., and Maheswari, D. (2012). Survey of cyber crime activities and preventive measures. Proceedings of the Second International Conference on Computational Science, Engineering and Information Technology, 301-305. *https://doi.org/10.1145/2393216.2393267*

Rivera, O. M. & Contreras, J. *V. A. (2022). El fenómeno de las ciberamenazas: afectaciones a la ciberseguridad del Ejército nacional de Colombia. Revista Perspectivas en Inteligencia, 14*(23), 63-95.

Rodríguez-Medina, L. et al. (2019). *International Ties at Peripheral Sites: Co-producing Social Processes and Scientific Knowledge in Latin America. Science as Culture, 28*(4), 562-588. *https://doi.org/10.1080/09505431.2019.1629409*

Romero, J. C. (2021). Ciberseguridad: Evolución y tendencias. bie3: Boletín IEEE, (23), 460-494.

Salazar-Lazo, C. & Ávila-Correa, B., (2023). *Estándares de ciberseguridad aplicables a los sistemas informáticos sanitarios para proteger los datos personales. 593 Digital Publisher CEIT, 9*(1), 88 - 102, *https://doi.org/10.33386/593dp.2024.1.2156*

Salmela, H. (2008). *Analysing Business Losses Caused by Information Systems Risk: A Business Process Analysis Approach. Journal of Information Technology, 23*(3), 185-202. *https://doi.org/10.1057/palgrave.jit.2000122*

Senabre, S., Soto, I., & Munera, J. (2021). *Fortaleciendo la ciberresiliencia del sector financiero. Evolución y tendencias. Revista de Estabilidad Financiera, 14*. *Sistemas e Tecnologías de Informação (E49), 396*-409.

Schiliro, F. (2023). Building a Resilient Cybersecurity Posture: A Framework for Leveraging Prevent, Detect and Respond Functions and Law Enforcement Collaboration. arXiv (Cornell University). *https://doi.org/10.48550/arxiv.2303.10874*

Sviatun, O. *V. et al. (2021). Combating Cybercrime: Economic and Legal Aspects. Wseas transactions on business and economics, 18*, 751-762. *https://doi.org/10.37394/23207.2021.18.72*

Tomašević, I. et al. (2020). *Lean in High-Mix/Low-Volume industry: a systematic literature review. Production Planning & Control, 32*(12), 1004-1019. *https://doi.org/10.1080/09537287.2020.1782094*

Valores, A. (2019). Ciberseguridad en Colombia [Tesis de posgrado, Universidad Piloto de Colombia]. Repositorio institucional. *http://repository.unipiloto.edu.co/handle/20.500.12277/6370*

Valoyes Mosquera, A. (2019). Ciberseguridad en Colombia [Seminario, Universidad Piloto de Colombia]. Universidad Piloto de Colombia.

Villamil, X. A. C., Jara, M. L. B., Venegas, J. C. P., & Aguilar, J. *A. Q. (2020). Ciberseguridad y ciberdefensa en Colombia: Un posible modelo a seguir en las relaciones cívico-militares. Revista Científica General José María Córdova 18(30), 357*-377.

Waters, R. V., and Ahmed, S. *A. (2020). Beyond the spreadsheets: quality project management. Performance Improvement, 59*(10), 16-29. *https://doi.org/10.1002/pfi.21940*

Yao, D., and Garcia de Soto, B. (2022). *A preliminary Swot evaluation for the applications of ML to Cyber Risk Analysis in the Construction Industry. IOP Conference Series: Materials Science and Engineering 1218(1), 012017*. *https://doi.org/10.1088/1757-899x/1218/1/012017*

Yang, S. et al. (2022). SoK: MEV Countermeasures: Theory and Practice. arXiv (Cornell University). *https://doi.org/10.48550/arxiv.2212.05111*

Younas, A. et al. (2023). *Proposing the 'Miracle' Narrative Framework for Providing Thick Description in Qualitative Research. International Journal of Qualitative Methods, 22*. *https://doi.org/10.1177/16094069221147162*

Zamora, L. R. V. (2019). Enfoques y diseños de investigación social: cuantitativos, cualitativos y mixtos. *Educación Superior 18(27), 96*-99.

Zhou, S. et al. (2022). *Adversarial Attacks and Defenses in Deep Learning: From a Perspective of Cybersecurity. ACM Computing Surveys, 55*(8), 1-39. *https://doi.org/10.1145/3547330*