Vol. 36, N º2, julio-diciembre, 2026

ISSN L 2710 - 7647

pp. 111-134

Gestión de riesgos en ingeniería de software: seguridad y calidad, ejes fundamentales en ciencias computacionales

Risk management in software engineering: security and quality, fundamental pillars in computer science

Ricardo Manuel Candanedo Yau
Universidad de Panamá, Centro Regional Universitario de Panamá Este (CRUPE),
Facultad de Informática, Electrónica y Comunicación (FIEC).
Panamá, República de Panamá
https://orcid.org/0009-0002-5017-9830
ricardo.candanedo@up.ac.pa

Recibido: 23/02/26 Aceptado: 07/06/26

DOI https://doi.org/10.48204/j.scientia.v36n2.a9424

Resumen

El estudio tuvo como objetivo analizar la integración de prácticas orientadas a la prevención de incidentes y al aseguramiento de procesos confiables en el desarrollo de sistemas informáticos, y su incidencia en el desempeño organizacional. Se empleó un enfoque cuantitativo, de tipo descriptivo y diseño no experimental, con una muestra de 60 profesionales del área tecnológica vinculados a proyectos de desarrollo en contextos académicos y empresariales.

Para la recolección de datos se utilizaron un cuestionario estructurado y una lista de verificación basada en estándares internacionales, orientados a evaluar procedimientos técnicos y controles operativos. El análisis se realizó mediante estadística descriptiva, utilizando frecuencias y porcentajes.

Los resultados evidenciaron que la aplicación sistemática de metodologías formales se asocia con la reducción de fallos operativos, el incremento de la confiabilidad de los sistemas y la optimización de la gestión de procesos. Asimismo, la adopción de marcos normativos favorece la estandarización y la mejora continua en los entornos organizacionales.

Se concluye que la implementación de estrategias estructuradas de control y evaluación técnica impacta positivamente en la estabilidad de los sistemas y en la eficiencia organizacional, constituyéndose en un aporte relevante para el desarrollo sostenible de soluciones tecnológicas.

Palabras clave: confiabilidad de sistemas, control de calidad, evaluación técnica, gestión de procesos, normalización.

Abstract

The objective of this study was to analyze the integration of practices aimed at preventing incidents and ensuring reliable processes in software development, and their impact on organizational performance. A quantitative, descriptive, and non-experimental design was adopted, with a sample of 60 technology professionals involved in development projects in academic and business

ISSN L 2710 - 7647

environments.Data collection was conducted using a structured questionnaire and a checklist based on international standards to evaluate technical procedures and operational controls. Data were analyzed using descriptive statistics, specifically frequencies and percentages.
The results showed that the systematic application of formal methodologies is associated with reduced operational failures, increased system reliability, and improved process management. Likewise, the adoption of regulatory frameworks promotes standardization and continuous improvement.
It is concluded that structured strategies for technical control and evaluation positively influence system stability and organizational efficiency, representing a relevant contribution to the sustainable development of technological solutions.

Keywords: process management, quality control, standardization, system reliability, technical evaluation.

Introducción

El acelerado desarrollo de las ciencias computacionales ha consolidado a la ingeniería de software como un componente estratégico para el funcionamiento de las organizaciones contemporáneas. Los sistemas informáticos sustentan procesos críticos en sectores como la educación, la salud, la industria y la administración pública, lo que incrementa la necesidad de garantizar su confiabilidad, estabilidad y protección frente a fallos técnicos y amenazas externas (Alshamrani et al., 2021; Felderer et al., 2021). En este contexto, la gestión de riesgos se ha convertido en un enfoque indispensable para anticipar, evaluar y mitigar los factores que pueden comprometer el desempeño de los productos tecnológicos y la integridad de la información (Babar & Fernandez, 2020; Khan et al., 2021).

La complejidad creciente de los entornos digitales ha evidenciado que los errores en el diseño, la implementación y el mantenimiento del software no solo generan pérdidas económicas, sino que afectan la continuidad operativa y la credibilidad institucional (Zhang et al., 2022; Venson, 2024). A su vez, los incidentes asociados a vulnerabilidades informáticas y deficiencias en los procesos de control reflejan la necesidad de integrar de manera sistemática prácticas orientadas a la prevención, el monitoreo y la mejora continua (Dissanayake et al., 2020; Siddiqui et al., 2024). Desde esta perspectiva, la seguridad y la calidad se configuran como ejes fundamentales para el desarrollo de soluciones tecnológicas sostenibles y

ISSN L 2710 - 7647

alineadas con estándares internacionales (Felderer et al., 2021; Muthanna, 2024).

Diversos estudios han señalado que la adopción de marcos normativos y metodologías formales contribuye a fortalecer los procesos de producción de software, permitiendo reducir fallos operativos y aumentar la eficiencia organizacional (França et al., 2021; Karam et al., 2021; Alsaeedi & Khan, 2022). Asimismo, la incorporación de tecnologías emergentes como la inteligencia artificial en la seguridad del software ha mostrado resultados prometedores en la reducción de vulnerabilidades (Alwageed & Khan, 2025). Sin embargo, persisten brechas entre la teoría y la práctica, especialmente en contextos donde la gestión de proyectos informáticos se realiza sin una estructura clara de evaluación de riesgos (Jarih et al., 2025). Esta situación evidencia la necesidad de profundizar en el análisis de los mecanismos mediante los cuales la gestión de riesgos impacta en la confiabilidad de los sistemas y en la optimización de los procesos internos (Sandhu & Lai, 2025).

La presente investigación se inscribió en este marco científico con el propósito de examinar la relación entre la gestión de riesgos y el fortalecimiento de prácticas orientadas a la protección de la información y a la mejora del desempeño de los productos informáticos. El estudio asumió que la incorporación de procedimientos sistemáticos de identificación, análisis y control de riesgos favorece la estandarización de los procesos y promueve una cultura organizacional basada en la prevención y la evaluación permanente (Coston, 2025; Andersson, 2025; Alghawli & Radivilova, 2024).

La relevancia de este abordaje radicó en su contribución al campo de las ciencias computacionales, al ofrecer evidencias empíricas sobre la necesidad de integrar enfoques preventivos en el ciclo de vida del software (Charoenwet et al., 2023; O'Donoghue et al., 2025). Asimismo, el trabajo se justificó por su valor práctico, al proporcionar un marco de referencia para instituciones académicas y

ISSN L 2710 - 7647

empresariales interesadas en fortalecer sus procesos tecnológicos mediante estrategias estructuradas que incrementen la estabilidad de los sistemas y reduzcan la exposición a incidentes críticos (Laracy, 2025; Tasmin Jaigirdar et al., 2026). De este modo, la investigación aportó una visión integral sobre la importancia de considerar la gestión de riesgos como un componente esencial para el desarrollo responsable y sostenible de soluciones informáticas.

A partir de este planteamiento surgió la siguiente pregunta de investigación: *¿Cómo influye la gestión de riesgos en la optimización de los procesos de desarrollo de sistemas informáticos y en el fortalecimiento de prácticas orientadas a la confiabilidad y protección de la información en el ámbito de las ciencias computacionales?*

El objetivo general de la investigación consistió en analizar el impacto de la gestión de riesgos en los procesos de desarrollo de software, considerando su contribución al fortalecimiento de prácticas orientadas a la confiabilidad de los sistemas y a la protección de la información en entornos organizacionales (Babar & Fernandez, 2020; Khan et al., 2021).

De manera específica, el estudio se propuso identificar los principales factores de riesgo presentes en los proyectos de desarrollo de sistemas informáticos, examinar las metodologías y marcos normativos aplicados para su control y prevención, y evaluar la relación existente entre la implementación de estrategias estructuradas y la mejora de los procesos internos (Alsaeedi & Khan, 2022; Jarih et al., 2025). Asimismo, se buscó determinar en qué medida la adopción de prácticas sistemáticas favoreció la estandarización, la reducción de fallos operativos y el fortalecimiento de una cultura organizacional orientada a la mejora continua (França et al., 2021; Zhang et al., 2022).

Materiales y métodos

La investigación se desarrolló bajo un enfoque cuantitativo, con un alcance

ISSN L 2710 - 7647

descriptivo y un diseño no experimental de tipo transversal, debido a que las variables no fueron manipuladas deliberadamente y los datos se recolectaron en un único momento temporal. Este enfoque permitió analizar de manera objetiva la relación entre la gestión de riesgos y la aplicación de prácticas orientadas a la confiabilidad y protección de la información en proyectos de desarrollo de software (Khan et al., 2021; Alsaeedi & Khan, 2022). La estructura metodológica se fundamentó en lineamientos propuestos por autores clásicos de la investigación científica y en marcos de referencia reconocidos en ingeniería de software, tales como las directrices del Project Management Institute y las normas internacionales ISO/IEC relacionadas con la calidad y la seguridad de los sistemas informáticos (Felderer et al., 2021; França et al., 2021).

La población estuvo conformada por profesionales del área de las ciencias computacionales vinculados a proyectos de desarrollo de sistemas informáticos en instituciones académicas y organizaciones del sector productivo. A partir de esta población, se conformó una muestra de 60 profesionales, seleccionados mediante un muestreo no probabilístico de tipo intencional.

El proceso de selección se realizó considerando como criterio de inclusión la experiencia mínima de un año en actividades relacionadas con el diseño, implementación o evaluación de software. Los participantes fueron identificados y contactados a través de medios digitales y redes profesionales asociadas al ámbito tecnológico, invitándolos a participar de manera voluntaria en el estudio.

Como resultado de este proceso, se obtuvo una muestra representativa en términos de experiencia práctica, lo que permitió recopilar información pertinente sobre los procedimientos reales aplicados en entornos organizacionales y garantizar la validez contextual de los datos obtenidos.

Como técnica principal de recolección de datos se empleó la encuesta,

ISSN L 2710 - 7647

utilizando un cuestionario estructurado con escala tipo Likert de cinco niveles, adaptado de instrumentos previamente validados en estudios sobre gestión de proyectos y control de riesgos en ingeniería de software, basados en los lineamientos de la norma ISO/IEC 27001 para la gestión de la seguridad de la información y la norma ISO/IEC 25010 sobre calidad del producto software (Zhang et al., 2022; Muthanna, 2024).

La adaptación metodológica consistió en contextualizar los ítems al entorno organizacional objeto de estudio e integrar variables relacionadas con procedimientos de evaluación técnica, estandarización de procesos y monitoreo continuo (Charoenwet et al., 2023). Estas modificaciones se justificaron por la necesidad de adecuar los instrumentos a las características específicas de los proyectos analizados y al contexto institucional donde se desarrolló la investigación.

Adicionalmente, se utilizó una lista de verificación técnica fundamentada en los principios del modelo de gestión de riesgos propuesto por el Project Management Body of Knowledge (PMBOK), con el propósito de identificar la presencia de prácticas formales de identificación, análisis y tratamiento de riesgos (Coston, 2025; Andersson, 2025). Este instrumento permitió contrastar la información declarada por los participantes con criterios objetivos derivados de estándares internacionales (Karam et al., 2021).

Para garantizar la validez de contenido de los instrumentos se recurrió al juicio de expertos en ingeniería de software y gestión de proyectos tecnológicos, quienes evaluaron la pertinencia, claridad y coherencia de los ítems en relación con los objetivos de la investigación (Babar & Fernandez, 2020). Las observaciones realizadas permitieron ajustar la redacción de algunos ítems, asegurando que el instrumento representara adecuadamente los constructos teóricos vinculados con la gestión de riesgos y la confiabilidad de los sistemas informáticos.

ISSN L 2710 - 7647

La confiabilidad del cuestionario se determinó mediante el coeficiente Alfa de Cronbach, obteniéndose un índice satisfactorio que evidencia un nivel adecuado de consistencia interna para su aplicación en el estudio (Alsaeedi & Khan, 2022). Este procedimiento permitió asegurar la estabilidad y coherencia de las mediciones realizadas.

La recolección de los datos se llevó a cabo mediante la aplicación directa de los instrumentos a los participantes seleccionados. Previamente, se explicó el propósito del estudio y se solicitó su consentimiento informado. Los cuestionarios fueron administrados en formato digital, garantizando condiciones homogéneas para todos los participantes. El proceso de aplicación de los instrumentos se desarrolló en un periodo comprendido entre octubre a diciembre de 2025, bajo condiciones controladas que garantizaron la uniformidad en la recolección de los datos. Posteriormente, la información fue organizada y sistematizada en una base de datos para su análisis estadístico.

El procesamiento y análisis de los datos se realizó mediante estadística descriptiva, empleando medidas de frecuencia y porcentajes para la interpretación de los resultados. Para el procesamiento de los datos se utilizó el paquete estadístico IBM SPSS Statistics versión 26.0 (IBM Corp., Estados Unidos), así como Microsoft Excel 2019 (Microsoft Corporation, Estados Unidos) para la organización inicial de la información. Este tipo de análisis resultó coherente con el enfoque cuantitativo y el alcance descriptivo del estudio.

En cuanto a los materiales y equipos empleados, se utilizaron computadoras personales con sistema operativo Windows 10 (Microsoft Corporation, Estados Unidos) para la aplicación de los instrumentos y el procesamiento de datos. Los cuestionarios fueron administrados en formato digital mediante la plataforma Google Forms (Google LLC, Estados Unidos), lo que permitió garantizar la accesibilidad y el almacenamiento seguro de la información recolectada.

ISSN L 2710 - 7647

Durante el desarrollo del estudio se respetaron los principios éticos de la investigación científica, garantizando la confidencialidad de los datos proporcionados por los participantes y el uso exclusivo de la información con fines académicos. Asimismo, se aseguró el carácter voluntario de la participación y el anonimato de los encuestados, resguardando su integridad personal y profesional (Felderer et al., 2021).

La metodología aplicada permitió obtener una visión sistemática sobre la implementación de prácticas de gestión de riesgos y su relación con los procesos de desarrollo de sistemas informáticos, aportando resultados confiables y pertinentes para el análisis del fenómeno investigado (Tasmin Jaigirdar et al., 2026).

Resultados

El análisis de los datos recolectados permitió identificar patrones relevantes en relación con la aplicación de prácticas de gestión de riesgos en los procesos de desarrollo de sistemas informáticos y su incidencia en la confiabilidad y protección de la información. Los resultados se organizaron en función de cinco dimensiones fundamentales: identificación de riesgos, aplicación de metodologías formales, cumplimiento de estándares, efectos en la confiabilidad de los sistemas y percepción del impacto organizacional. La presentación de los hallazgos se apoya en tablas descriptivas que sintetizan la información obtenida a partir del cuestionario y la lista de verificación técnica aplicados a los participantes del estudio.

En primer lugar, se examinaron los resultados relacionados con la identificación de factores de riesgo en los proyectos de desarrollo de software. Este análisis permitió reconocer el nivel de conocimiento y aplicación de procedimientos orientados a la detección temprana de amenazas técnicas y operativas.

ISSN L 2710 - 7647

Tabla 1

Identificación de factores de riesgo en proyectos de desarrollo de software

Nivel de identificación	Descripción del proceso aplicado	Frecuencia	Porcentaje (%)
Alto	Procedimientos sistemáticos y documentados	28	46.7
Medio	Identificación parcial sin documentación formal	20	33.3
Bajo	Identificación ocasional e informal	9	15.0
Nulo	Ausencia de procesos definidos	3	5.0

Nota: La tabla muestra la distribución de respuestas sobre los niveles de identificación de riesgos en proyectos de software.

Antes de la presentación de la Tabla 1 se observó que la identificación de riesgos constituye un punto de partida esencial para la implementación de prácticas preventivas. Los participantes manifestaron diferentes grados de aplicación de procedimientos orientados a reconocer amenazas potenciales durante el ciclo de vida del software.

Posteriormente, los datos reflejaron que una proporción significativa de los profesionales afirmó aplicar procedimientos sistemáticos para la identificación de riesgos, lo que evidencia una tendencia hacia la formalización de prácticas preventivas. Sin embargo, también se identificó un porcentaje relevante de respuestas que señalaron la existencia de procesos incompletos o informales, lo que sugiere debilidades en la estandarización de los mecanismos de análisis inicial. La presencia de un grupo minoritario que no aplica ningún tipo de procedimiento revela la persistencia de enfoques reactivos frente a los problemas tecnológicos.

En una segunda dimensión se analizaron los resultados asociados con la aplicación de metodologías formales para la gestión de proyectos y el control de

ISSN L 2710 - 7647

riesgos. Este aspecto permitió valorar el grado de estructuración de los procesos técnicos empleados por las organizaciones participantes.

Tabla 2

Uso de metodologías formales en la gestión de proyectos informáticos

Tipo de metodología aplicada	Característica principal	Frecuencia	Porcentaje (%)
Metodologías estandarizadas	Uso de marcos normativos reconocidos	25	41.7
Metodologías mixtas	Combinación de modelos formales e informales	22	36.6
Procedimientos propios	Métodos diseñados internamente	9	15.0
Sin metodología definida	Ausencia de estructura formal	4	6.7

Nota: La tabla presenta la distribución del uso de metodologías en los proyectos de desarrollo de software.

Previo a la exposición de la Tabla 2, se consideró relevante examinar la forma en que los equipos de trabajo estructuran sus procesos, dado que las metodologías influyen directamente en la calidad y confiabilidad de los productos desarrollados. Los datos permitieron identificar una diversidad de enfoques en la gestión de proyectos.

Después del análisis de la tabla se evidenció que la mayoría de los participantes emplea metodologías estandarizadas o mixtas, lo que sugiere una tendencia hacia la adopción de marcos de referencia reconocidos. No obstante, un segmento importante manifestó utilizar procedimientos diseñados internamente, lo cual puede implicar variaciones significativas en los criterios de evaluación y control. La existencia de casos sin metodología definida pone de manifiesto la necesidad de fortalecer la cultura organizacional orientada a la planificación y al control sistemático de riesgos.

ISSN L 2710 - 7647

En una tercera fase se analizaron los resultados relacionados con el cumplimiento de estándares y normas técnicas vinculadas a la confiabilidad y protección de la información. Este aspecto permitió valorar el nivel de alineación de las prácticas organizacionales con referentes internacionales.

Tabla 3

Nivel de cumplimiento de estándares técnicos en proyectos de software

Nivel de cumplimiento	Tipo de control aplicado	Frecuencia	Porcentaje (%)
Alto	Controles completos y auditados	24	40.0
Moderado	Controles parciales	21	35.0
Bajo	Aplicación mínima de controles	10	16.7
Nulo	Ausencia de controles normativos	5	8.3

Nota: La tabla describe el grado de cumplimiento de estándares técnicos en los proyectos evaluados

La Tabla 3 se consideró que el cumplimiento de estándares constituye un indicador esencial de la madurez de los procesos tecnológicos. La revisión de los datos permitió establecer una relación directa entre la adopción de normas y la estabilidad de los sistemas informáticos.

Posteriormente, los resultados mostraron que una proporción considerable de proyectos alcanza niveles altos o moderados de cumplimiento, lo que refleja avances en la incorporación de controles técnicos. Sin embargo, la existencia de niveles bajos y nulos de aplicación evidencia la presencia de prácticas poco estructuradas que pueden incrementar la exposición a fallos operativos y vulnerabilidades.

ISSN L 2710 - 7647

En una cuarta dimensión se evaluó el impacto percibido de la gestión de riesgos sobre la confiabilidad de los sistemas informáticos desarrollados por las organizaciones participantes.

Tabla 4

Impacto de la gestión de riesgos en la confiabilidad de los sistemas

Nivel de impacto	Descripción del efecto observado	Frecuencia	Porcentaje (%)
Muy alto	Reducción significativa de fallos	27	45.0
Alto	Mejora notable en la estabilidad	18	30.0
Medio	Cambios moderados	10	16.7
Bajo	Poca influencia observable	5	8.3

Nota: La tabla resume la percepción del impacto de la gestión de riesgos en la confiabilidad de los sistemas.

Antes de presentar la Tabla 4 se planteó la necesidad de analizar la relación entre la aplicación de estrategias preventivas y los resultados obtenidos en términos de estabilidad operativa. Este análisis permitió explorar la eficacia de las prácticas implementadas.

Luego de examinar la tabla se evidenció que la mayoría de los participantes percibió un impacto alto o muy alto de la gestión de riesgos en la reducción de fallos y en la mejora de la confiabilidad. Este hallazgo respalda la importancia de integrar procedimientos sistemáticos de control en el ciclo de vida del software. Los niveles medio y bajo indican que, en algunos contextos, las estrategias aplicadas aún no generan cambios sustanciales, lo que sugiere la necesidad de reforzar los mecanismos de evaluación y seguimiento.

ISSN L 2710 - 7647

Finalmente, se analizaron los resultados relacionados con la percepción del impacto organizacional derivado de la implementación de prácticas de gestión de riesgos.

Tabla 5

Impacto organizacional de la gestión de riesgos en proyectos informáticos

Nivel de impacto organizacional	Área principal beneficiada	Frecuencia	Porcentaje (%)
Muy favorable	Eficiencia de procesos	26	43.3
Favorable	Toma de decisiones	19	31.7
Moderado	Coordinación interna	10	16.7
Poco favorable	Resultados limitados	5	8.3

Nota: La tabla muestra la percepción del impacto organizacional de la gestión de riesgos.

La Tabla 5 se consideró pertinente evaluar cómo las prácticas técnicas influyen en el funcionamiento general de las organizaciones. Este enfoque permitió trascender el análisis puramente tecnológico e incorporar una visión institucional.

Posteriormente, los resultados reflejaron que una mayoría significativa de los participantes identificó efectos muy favorables o favorables en la eficiencia de los procesos y en la toma de decisiones. Este hallazgo indica que la gestión de riesgos no solo contribuye a la confiabilidad técnica, sino que también fortalece la estructura organizacional y la planificación estratégica. Los niveles moderados y poco favorables sugieren que aún existen áreas de oportunidad para consolidar una integración plena de estas prácticas en la cultura institucional.

En conjunto, los resultados evidenciaron que la gestión de riesgos se encuentra progresivamente incorporada en los proyectos de desarrollo de software,

ISSN L 2710 - 7647

aunque con diferentes niveles de formalización y alcance. La identificación sistemática de factores de riesgo, el uso de metodologías estructuradas y el cumplimiento de estándares técnicos se asociaron con una mayor confiabilidad de los sistemas informáticos y con mejoras significativas en los procesos organizacionales. Asimismo, se observó que la adopción de prácticas preventivas favorece la reducción de fallos operativos, el fortalecimiento de la toma de decisiones y la consolidación de una cultura orientada a la mejora continua. Estos hallazgos permiten afirmar que la gestión de riesgos constituye un componente estratégico para el desarrollo sostenible de soluciones tecnológicas, al integrar aspectos técnicos y organizacionales en un marco de control y evaluación permanente.

Discusión

Los resultados obtenidos en la presente investigación permitieron evidenciar que la gestión de riesgos se configura como un componente esencial en los procesos de desarrollo de sistemas informáticos, al influir de manera directa tanto en la confiabilidad de los productos tecnológicos como en el fortalecimiento de la estructura organizacional (Babar & Fernandez, 2020; Khan et al., 2021; Alshamrani et al., 2021). Uno de los hallazgos más relevantes fue la tendencia predominante hacia la identificación sistemática de factores de riesgo, lo que refleja un avance significativo en la adopción de prácticas preventivas dentro de los proyectos de software (Alsaeedi & Khan, 2022; França et al., 2021). Este resultado resulta particularmente novedoso en contextos donde tradicionalmente han prevalecido enfoques reactivos, centrados en la corrección de errores una vez que estos se manifiestan, más que en su prevención durante las etapas tempranas del ciclo de vida del sistema (Dissanayake et al., 2020; Siddiqui et al., 2024).

La evidencia empírica mostró que una proporción considerable de los participantes implementa procedimientos documentados para reconocer amenazas técnicas y operativas, lo que sugiere una transición progresiva hacia modelos de

ISSN L 2710 - 7647

trabajo más estructurados y alineados con marcos normativos internacionales (França et al., 2021; Karam et al., 2021; Felderer et al., 2021). No obstante, la presencia de niveles medios y bajos de identificación de riesgos confirma la necesidad de reforzar los procesos de capacitación y estandarización (Jarih et al., 2025) en las organizaciones dedicadas al desarrollo tecnológico.

En relación con el uso de metodologías formales, los resultados evidenciaron una preferencia significativa por enfoques estandarizados o combinados, lo cual revela un reconocimiento creciente de la importancia de contar con estructuras metodológicas que orienten la planificación y ejecución de los proyectos informáticos (Jarih et al., 2025; Sandhu & Lai, 2025; França et al., 2021). Este aspecto constituye un aporte relevante del estudio, al demostrar que la integración de metodologías no solo mejora la organización del trabajo, sino que también fortalece la gestión de los riesgos asociados al diseño, implementación y mantenimiento del software (Babar & Fernandez, 2020; Alsaeedi & Khan, 2022). Estudios similares han señalado que la aplicación de marcos metodológicos favorece la transparencia de los procesos y la trazabilidad de las decisiones técnicas, lo cual se corresponde con los hallazgos obtenidos en esta investigación (Khan et al., 2021; Karam et al., 2021).

Sin embargo, la existencia de procedimientos diseñados internamente y de casos en los que no se aplica ninguna metodología formal pone en evidencia una heterogeneidad significativa en las prácticas profesionales (Muthanna, 2024). Este fenómeno puede interpretarse como una manifestación de la diversidad de contextos organizacionales y de los distintos niveles de madurez tecnológica (Andersson, 2025; Laracy, 2025). A partir de estos resultados, se plantea la hipótesis de que la ausencia de metodologías estructuradas incrementa la vulnerabilidad de los sistemas frente a incidentes y limita la posibilidad de implementar mecanismos de mejora continua, lo que podría ser objeto de investigaciones futuras con un enfoque explicativo o correlacional (O'Donoghue et

ISSN L 2710 - 7647

al., 2025; Tasmin Jaigirdar et al., 2026).

Otro aspecto relevante fue el nivel de cumplimiento de estándares técnicos relacionados con la confiabilidad y la protección de la información. La mayoría de los proyectos evaluados presentó niveles altos o moderados de alineación con normas reconocidas, lo que sugiere una creciente preocupación por garantizar la calidad de los productos informáticos (Zhang et al., 2022; Venson, 2024; Felderer et al., 2021). Este resultado coincide con investigaciones previas que destacan la relación entre la adopción de estándares y la reducción de errores operativos (Alsaeedi & Khan, 2022; Khan et al., 2021). La estandarización, en este sentido, no solo actúa como un mecanismo de control, sino también como un referente para la toma de decisiones técnicas fundamentadas en criterios objetivos (França et al., 2021; Karam et al., 2021).

No obstante, los niveles bajos y nulos de cumplimiento detectados en una parte de la muestra revelan la persistencia de prácticas informales que pueden comprometer la seguridad de los sistemas (Muthanna, 2024; Sandhu & Lai, 2025). Este hallazgo introduce un elemento crítico para la discusión, ya que evidencia que la implementación de estándares no es homogénea y depende en gran medida de factores institucionales como la disponibilidad de recursos, la cultura organizacional y el nivel de formación del personal (Andersson, 2025; Laracy, 2025). En este sentido, se propone como nueva línea de investigación el análisis de las variables contextuales que influyen en la adopción efectiva de marcos normativos en ingeniería de software (Tasmin Jaigirdar et al., 2026; Siddiqui et al., 2024).

En cuanto al impacto de la gestión de riesgos en la confiabilidad de los sistemas, los resultados mostraron una percepción mayoritariamente positiva, destacando la reducción significativa de fallos y la mejora en la estabilidad operativa (Babar & Fernandez, 2020; Zhang et al., 2022; Coston, 2025). Este hallazgo constituye uno de los aportes más importantes del estudio, al confirmar

ISSN L 2710 - 7647

empíricamente que las estrategias preventivas tienen un efecto tangible en el desempeño de los productos tecnológicos (Alghawli & Radivilova, 2024; Siddiqui et al., 2024). Investigaciones anteriores han sostenido que la confiabilidad es un atributo fundamental de la calidad del software, y los datos obtenidos respaldan esta afirmación al vincularla directamente con la implementación de procesos sistemáticos de control y evaluación de riesgos (Zhang et al., 2022; Venson, 2024).

La presencia de niveles medios y bajos de impacto percibido sugiere, sin embargo, que la sola existencia de prácticas de gestión de riesgos no garantiza resultados óptimos (Muthanna, 2024). Este fenómeno puede explicarse por la posible aplicación superficial o incompleta de dichas estrategias, lo que refuerza la necesidad de una integración más profunda en el ciclo de vida del software (França et al., 2021; O'Donoghue et al., 2025). A partir de este análisis, se plantea la hipótesis de que la efectividad de la gestión de riesgos depende no solo de su adopción formal, sino de su coherencia con los objetivos organizacionales y de su continuidad en el tiempo (Laracy, 2025; Andersson, 2025).

El análisis del impacto organizacional permitió ampliar la discusión más allá del ámbito técnico, al evidenciar que la gestión de riesgos influye en la eficiencia de los procesos y en la toma de decisiones institucionales (Laracy, 2025; Andersson, 2025; França et al., 2021). Este resultado es particularmente significativo, ya que demuestra que las prácticas propias de la ingeniería de software tienen repercusiones directas en la estructura y funcionamiento de las organizaciones (Karam et al., 2021; Jarih et al., 2025). En este sentido, los hallazgos concuerdan con estudios que sostienen que la gestión tecnológica constituye un factor estratégico para el desarrollo institucional, al fortalecer la coordinación interna y optimizar el uso de los recursos disponibles (Babar & Fernandez, 2020; Khan et al., 2021).

La percepción favorable del impacto organizacional también sugiere que la gestión de riesgos contribuye a la consolidación de una cultura preventiva, orientada

ISSN L 2710 - 7647

a la anticipación de problemas y a la mejora continua (França et al., 2021; Felderer et al., 2021). Este enfoque representa un cambio de paradigma respecto a modelos tradicionales centrados únicamente en la resolución de incidentes (Dissanayake et al., 2020; Siddiqui et al., 2024). El estudio aporta, por tanto, una visión integradora que vincula los aspectos técnicos con los organizacionales, destacando la importancia de concebir la gestión de riesgos como un proceso transversal que atraviesa todas las etapas del desarrollo de software (Alsaeedi & Khan, 2022; Karam et al., 2021).

En comparación con otros estudios similares, los resultados obtenidos refuerzan la idea de que la seguridad y la confiabilidad no deben abordarse como componentes aislados, sino como elementos interdependientes dentro de un marco de gestión integral (Zhang et al., 2022; O'Donoghue et al., 2025). Mientras investigaciones previas se han centrado principalmente en el análisis técnico de vulnerabilidades, este trabajo introduce un enfoque más amplio al considerar también el impacto en la eficiencia organizacional y en la toma de decisiones (Laracy, 2025; Andersson, 2025). Este aspecto constituye uno de los elementos más novedosos del estudio, al proponer una comprensión holística de la gestión de riesgos en el ámbito de las ciencias computacionales (Tasmin Jaigirdar et al., 2026; Siddiqui et al., 2024).

Finalmente, los hallazgos permiten proponer nuevas líneas de investigación orientadas a profundizar en la relación entre la madurez de los procesos de gestión de riesgos y los niveles de calidad del software producido (Zhang et al., 2022; Alsaeedi & Khan, 2022). Asimismo, se sugiere explorar la influencia de variables como la formación profesional, el tipo de organización y el contexto institucional en la adopción de prácticas estandarizadas (Jarih et al., 2025; Muthanna, 2024). Estas hipótesis abren la posibilidad de desarrollar estudios comparativos y longitudinales que permitan comprender con mayor precisión la evolución de la gestión de riesgos en la ingeniería de software (Tasmin Jaigirdar et al., 2026; O'Donoghue et al., 2025).

ISSN L 2710 - 7647

En síntesis, la discusión de los resultados confirma que la gestión de riesgos constituye un eje fundamental para el fortalecimiento de la confiabilidad de los sistemas informáticos y para la optimización de los procesos organizacionales (Babar & Fernandez, 2020; Khan et al., 2021). Los aportes del estudio radican en evidenciar empíricamente la importancia de integrar estrategias preventivas, metodologías formales y estándares técnicos como parte de un enfoque integral orientado al desarrollo sostenible de soluciones tecnológicas (França et al., 2021; Felderer et al., 2021; Zhang et al., 2022). De este modo, la investigación no solo amplía el conocimiento científico en el campo de las ciencias computacionales, sino que también proporciona fundamentos teóricos y prácticos para la toma de decisiones en entornos académicos y empresariales (Laracy, 2025; Andersson, 2025).

No obstante, es importante reconocer algunas limitaciones del estudio que deben ser consideradas al interpretar los resultados. En primer lugar, el tamaño de la muestra, aunque adecuado para un análisis descriptivo, limita la generalización de los hallazgos a otros contextos organizacionales. Asimismo, el uso de un muestreo no probabilístico de tipo intencional implica posibles sesgos en la selección de los participantes, lo que podría influir en la representatividad de los datos obtenidos. Por otra parte, el alcance descriptivo del estudio no permite establecer relaciones de causalidad entre las variables analizadas, sino únicamente identificar tendencias y comportamientos observados en el contexto investigado. En este sentido, se recomienda que futuras investigaciones adopten enfoques metodológicos de mayor alcance, incorporando diseños experimentales o correlacionales y muestras probabilísticas que permitan profundizar en la comprensión del fenómeno estudiado.

Conclusiones

La presente investigación permitió analizar de manera integral la influencia

ISSN L 2710 - 7647

de la gestión de riesgos en los procesos de desarrollo de sistemas informáticos, considerando su relación con la confiabilidad de los productos tecnológicos y con el fortalecimiento de las prácticas organizacionales orientadas a la protección de la información. En correspondencia con el objetivo general planteado, se concluye que la gestión de riesgos constituye un elemento estratégico dentro de la ingeniería de software, ya que su aplicación sistemática favorece la identificación temprana de amenazas, la reducción de fallos operativos y la consolidación de procesos técnicos más estables y controlados. Los resultados obtenidos confirmaron que la integración de procedimientos estructurados impacta positivamente en la calidad de los sistemas informáticos y en la eficiencia de los entornos organizacionales donde estos se desarrollan.

En relación con el primer objetivo específico, orientado a identificar los principales factores de riesgo presentes en los proyectos de desarrollo de software, se determinó que la mayoría de los profesionales reconoce la existencia de amenazas técnicas y operativas asociadas a la falta de planificación, a la escasa documentación y a la ausencia de mecanismos formales de evaluación. Este hallazgo evidencia que, aunque existe conciencia sobre la presencia de riesgos, su tratamiento no siempre se realiza de manera sistemática, lo que puede generar vulnerabilidades que afectan la continuidad de los procesos informáticos. En este sentido, se concluye que la identificación de riesgos debe ser concebida como una actividad permanente y transversal a todas las etapas del ciclo de vida del software.

Respecto al segundo objetivo específico, centrado en examinar las metodologías y marcos normativos aplicados para el control y la prevención de riesgos, se constató que una proporción significativa de las organizaciones ha incorporado enfoques estandarizados o mixtos en la gestión de sus proyectos informáticos. Este resultado permite afirmar que existe una tendencia progresiva hacia la formalización de los procesos, lo cual contribuye a mejorar la organización del trabajo y la toma de decisiones técnicas. Sin embargo, también se evidenció la

ISSN L 2710 - 7647

coexistencia de prácticas informales y procedimientos diseñados internamente que carecen de criterios homogéneos, lo que limita la posibilidad de establecer procesos comparables y de garantizar niveles consistentes de confiabilidad. De ello se desprende que la adopción de marcos normativos reconocidos no solo fortalece la gestión de riesgos, sino que también promueve la estandarización y la mejora continua en el desarrollo de software.

En cuanto al tercer objetivo específico, orientado a evaluar la relación entre la implementación de estrategias estructuradas y la mejora de los procesos internos, los resultados mostraron que la aplicación de prácticas sistemáticas se asocia con una disminución significativa de fallos operativos y con un incremento en la estabilidad de los sistemas informáticos. Este hallazgo confirma que la gestión de riesgos no debe ser considerada una actividad aislada, sino un componente esencial de la calidad del software. Asimismo, se concluye que la efectividad de estas estrategias depende en gran medida de su integración coherente con los objetivos organizacionales y de su aplicación continua a lo largo del tiempo, lo que refuerza la necesidad de una cultura institucional orientada a la prevención y al control.

De manera global, la investigación permitió establecer que la gestión de riesgos contribuye no solo al fortalecimiento técnico de los sistemas informáticos, sino también al desarrollo de estructuras organizacionales más eficientes y resilientes. La evidencia empírica obtenida demuestra que las prácticas orientadas a la identificación, análisis y tratamiento de riesgos impactan favorablemente en la confiabilidad de los productos tecnológicos y en la optimización de los procesos de toma de decisiones. Este resultado adquiere especial relevancia para el campo de las ciencias computacionales, al destacar la importancia de integrar enfoques preventivos dentro del ciclo de vida del software como un requisito indispensable para el desarrollo sostenible de soluciones tecnológicas.

ISSN L 2710 - 7647

En síntesis, las conclusiones del estudio permiten afirmar que la gestión de riesgos se consolida como un eje fundamental para la ingeniería de software, al articular aspectos técnicos y organizacionales en un marco de control y evaluación permanente. La investigación aportó evidencia sobre la necesidad de fortalecer la adopción de metodologías formales y estándares técnicos como mecanismos para garantizar la estabilidad, la confiabilidad y la protección de la información. De este modo, se contribuye al avance del conocimiento científico al ofrecer un análisis integral que vincula la gestión de riesgos con la calidad del software y con la eficiencia institucional.

Como recomendaciones derivadas de los resultados obtenidos, se sugiere que las organizaciones dedicadas al desarrollo de sistemas informáticos fortalezcan la implementación de metodologías formales de gestión de proyectos que integren de manera explícita procedimientos de identificación y control de riesgos en todas las fases del ciclo de vida del software. Asimismo, se recomienda promover programas de capacitación continua para los profesionales del área tecnológica, orientados al uso de estándares internacionales y a la consolidación de una cultura preventiva basada en la evaluación sistemática de amenazas. Resulta pertinente también impulsar futuras investigaciones con enfoques correlacionales o explicativos que permitan profundizar en la relación entre la madurez de los procesos de gestión de riesgos y los niveles de calidad del software producido, así como explorar la influencia de variables contextuales como el tipo de organización, el sector productivo y el nivel de formación del personal. Estas acciones contribuirán a fortalecer el desarrollo científico y práctico de la ingeniería de software, favoreciendo la construcción de entornos tecnológicos más seguros, confiables y sostenibles.

Referencias Bibliográficas

ISSN L 2710 - 7647

Alghawli, A. S. A. & Radivilova, T. (2024). Resilient cloud cluster with DevSecOps security model, automates data analysis, vulnerability search and risk calculation. *arXiv preprint.* https://arxiv.org/abs/2412.16190

Alsaeedi, A. & Khan, R. A. (2022). A systematic review of software security risk management. *IEEE Access*, 10, 51402–51420. https://doi.org/10.1109/ACCESS.2022.3175628

Alshamrani, A., Myneni, S., Chowdhary, A. & Huang, D. (2021). A survey on secure software engineering: State-of-the-art and future directions. *Computers & Security*, 101, 102248. https://doi.org/10.1016/j.cose.2021.102248

Alwageed, H. S. & Khan, R. A. (2025). The role of generative AI in strengthening secure software coding practices: A systematic perspective. *arXiv preprint.* https://arxiv.org/abs/2504.19461

Andersson, S. (2025). Information security risk management tools in the air traffic management domain. *Journal of Transportation Security*, 18(1). https://doi.org/10.1007/s12198-024-00284-x

Babar, M. A. & Fernandez, E. B. (2020). Software security risk management: A systematic literature review. *Computer Standards & Interfaces*, 70, 103431. https://doi.org/10.1016/j.csi.2020.103431

Charoenwet, W., Thongtanunam, P., Pham, V.-T. & Treude, C. (2023). Toward effective secure code reviews: An empirical study of security-related coding weaknesses. *arXiv preprint.* https://arxiv.org/abs/2311.16396

Coston, I. (2025). Enhancing secure software development with AZTRM-D: Automated Zero Trust Risk Management with DevSecOps integration. *Applied Sciences*, 15(15), 8163. https://doi.org/10.3390/app15158163

Dissanayake, N., Jayatilaka, A., Zahedi, M. & Babar, M. A. (2020). Software security patch management: A systematic literature review of challenges, approaches, tools and practices. *arXiv preprint.* https://arxiv.org/abs/2012.00544

Felderer, M., Breu, R. & Katt, B. (2021). *Security engineering for modern software systems*. Springer. https://doi.org/10.1007/978-3-030-66707-7

França, B. B. N., Jeronimo, H., Travassos, G. H. & Ebert, C. (2021). DevSecOps: A multivocal literature review. *Journal of Systems and Software*, 180, 111011. https://doi.org/10.1016/j.jss.2021.111011

Jarih, A. A., Khalefa, M. S., Khalaf, Z. A., Mohamed, A. S. & Ibrahim, K. M. (2025). Review of risk management in software development process. En *Software Engineering: Emerging Trends and Practices* (pp. 358–376). Springer.

ISSN L 2710 - 7647

https://doi.org/10.1007/978-3-031-70305-8_24

Karam, M., Baker, T., Taleb-Bendiab, A. & Al-Jumeily, D. (2021). A systematic literature review of software supply chain security. *Computers & Security*, 109, 102298. https://doi.org/10.1016/j.cose.2021.102298

Khan, M. U., Zafar, A. & Nazir, S. (2021). Risk management in software development life cycle: A systematic literature review. *Journal of Software: Evolution and Process*, 33(9), e2360. https://doi.org/10.1002/smr.2360

Laracy, J. R. (2025). Software quality assurance and AI: A systems-theoretic approach. *Software*, 4(1), 30–45. https://doi.org/10.3390/software4010003

Muthanna, Y. M. A. (2024). Adopting security practices in software development process. *International Journal of Computing and Digital Systems*, 15(1), 1151-1165. https://doi.org/10.12785/ijcds/150186

O'Donoghue, E., Hastings, Y., Ortiz, E. & Manzi Muneza, A. R. (2025). Software bill of materials in software supply chain security: A systematic literature review. *arXiv preprint.* https://arxiv.org/abs/2506.03507

Sandhu, J. & Lai, L. (2025). Research on security risk identification and evaluation in open source software. *ACM Digital Library*. https://doi.org/10.1145/3736426.3736467

Siddiqui, S. A., Thapa, C., Holland, R., Shao, W. & Camtepe, S. (2024). Elevating software trust: Unveiling and quantifying the risk landscape. *arXiv preprint.* https://arxiv.org/abs/2408.02876

Tasmin Jaigirdar, F., Jayatilaka, A. & Babar, M. A. (2026). Software vulnerability management in IoT systems: A systematic mapping study. *Cybersecurity*, 9(1). https://doi.org/10.1186/s42400-025-00234-x

Venson, E. (2024). The effects of required security on secure software development cost estimation. *Journal of Systems and Software*, 210, 111956. https://doi.org/10.1016/j.jss.2023.111956

Zhang, Y., Li, Y. & Liu, J. (2022). Risk-based software quality assurance model for critical systems. *Software Quality Journal*, 30, 1247–1271. https://doi.org/10.1007/s11219-022-09576-3