Revista Colón Ciencias, Tecnología y Negocios
ISSN L: 2313-7819
Vol. 13, Nº 2 Julio – Diciembre 2026
pp. 98-115

Riesgos emergentes y nuevas ciberamenazas: estrategias de mitigación mediante inteligencia de amenazas y resiliencia operativa

Emerging risks and new cyber threats: mitigation strategies through threat intelligence and operational resilience

Ricardo M. Candanedo Yau

Universidad de Panamá, Centro Regional Universitario de Panamá Este, Facultad de Informática Electrónica y Comunicación, Panamá.
ricardo.candanedo@up.ac.pa, https://orcid.org/0009-0002-5017-9830

DOI: https://doi.org/10.48204/j.colonciencias.v13n2.a9302

Resumen

El incremento de los riesgos emergentes y las nuevas ciberamenazas ha generado escenarios digitales cada vez más complejos que comprometen la estabilidad operativa y la seguridad de la información en las organizaciones. Este contexto exige estrategias integradas que articulen la inteligencia de amenazas con la resiliencia operativa. El objetivo del estudio consistió en analizar el papel de la inteligencia de amenazas y la resiliencia operativa como estrategia para la mitigación de fenómenos digitales adversos en contextos organizacionales, a partir de un enfoque teórico y documental, para esto se realizó una revisión de literatura científica mediante la consulta de bases de datos especializadas (Scopus, Web of Science, Google Scholar e IEEE Xplore). Inicialmente se identificaron 85 documentos, de los cuales 35 fueron excluidos tras aplicar criterios de pertinencia temática, actualidad y calidad metodológica, quedando una muestra final de 50 estudios para el análisis. Los autores más representativos en la temática fueron Hutchins, Cloppert y Amin; Behl y Behl; Linkov *et al*.; Tounsi y Rais; y Von Solms y Van Niekerk. Sus aportes destacaron la defensa basada en inteligencia, la resiliencia organizacional, el análisis técnico de datos y la transición desde la seguridad de la información hacia un enfoque integral de ciberseguridad.

Los resultados evidenciaron que la integración entre inteligencia de amenazas y resiliencia operativa favorece la detección temprana de incidentes, fortalece la toma de decisiones estratégicas y reduce el impacto operativo de los eventos de seguridad. Asimismo, se identificó una tendencia

Revista Colón Ciencias, Tecnología y Negocios
ISSN L: 2313-7819
Vol. 13, Nº 2 Julio – Diciembre 2026
pp. 98-115

creciente hacia el uso del monitoreo continuo y el análisis de datos como componentes clave en la gestión del riesgo digital.

Se concluye que la adopción de mecanismos estructurados de vigilancia tecnológica y continuidad de operaciones constituye un enfoque eficaz para enfrentar escenarios complejos y dinámicos, contribuyendo a una gestión de la seguridad informática integral y sostenible en contextos organizacionales.

Palabras clave: gestión del riesgo, inteligencia de amenazas, resiliencia operativa, seguridad de la información, sistemas de información

Abstract

The increase in emerging risks and new cyber threats has generated increasingly complex digital scenarios that compromise operational stability and information security in organizations. This context demands integrated strategies that combine threat intelligence with operational resilience. The objective of this study was to analyze the role of threat intelligence and operational resilience as a strategy for mitigating adverse digital phenomena in organizational contexts, using a theoretical and documentary approach. To this end, a review of scientific literature was conducted by consulting specialized databases (Scopus, Web of Science, Google Scholar, and IEEE Xplore). Initially, 85 documents were identified, of which 35 were excluded after applying criteria of thematic relevance, currency, and methodological quality, leaving a final sample of 50 studies for analysis. The most representative authors on the topic were Hutchins, Cloppert, and Amin; Behl and Behl; Linkov *et al*.; Tounsi and Rais; and Von Solms and Van Niekerk. Their contributions highlighted intelligence-based defense, organizational resilience, technical data analysis, and the transition from information security to a comprehensive cybersecurity approach.

The results showed that integrating threat intelligence and operational resilience facilitates early incident detection, strengthens strategic decision-making, and reduces the operational impact of security events. Furthermore, a growing trend toward the use of continuous monitoring and data analysis as key components of digital risk management was identified.

Revista Colón Ciencias, Tecnología y Negocios
ISSN L: 2313-7819
Vol. 13, Nº 2 Julio – Diciembre 2026
pp. 98-115

It is concluded that adopting structured technology monitoring and business continuity mechanisms is an effective approach to addressing complex and dynamic scenarios, contributing to comprehensive and sustainable cybersecurity management in various contexts.

Keywords: information security, information systems, operational resilience, risk management, threat intelligence

Introducción

El acelerado proceso de digitalización que caracteriza a las sociedades contemporáneas ha transformado de manera sustancial los modelos de producción, comunicación y gestión organizacional. La interconexión permanente de sistemas, dispositivos y plataformas ha incrementado la eficiencia operativa, pero también ha generado una superficie de exposición cada vez más amplia frente a eventos que comprometen la confidencialidad, integridad y disponibilidad de la información (Von Solms & Van Niekerk, 2013; González Díaz, 2025). En este contexto, la seguridad informática ha dejado de ser un componente exclusivamente técnico para convertirse en un eje estratégico vinculado a la continuidad de las operaciones, la sostenibilidad institucional y la confianza de los usuarios (Linkov *et al.*, 2019; Behl & Behl, 2017).

Durante la última década, se ha evidenciado una evolución significativa en la naturaleza de los incidentes digitales, caracterizada por su mayor sofisticación, persistencia y capacidad de adaptación. Estas transformaciones han dado lugar a un escenario en el que los mecanismos tradicionales de protección resultan insuficientes para enfrentar fenómenos cada vez más complejos (Tounsi & Rais, 2018; Saeed *et al.*, 2023). Diversos estudios señalan que las amenazas actuales no solo explotan vulnerabilidades tecnológicas, sino también debilidades organizacionales, humanas y procedimentales, lo que exige un enfoque integral basado en la anticipación, la gestión del riesgo y la capacidad de recuperación operativa (Cantillo Velásquez *et al.*, 2025; Darus *et al.*, 2025).

Revista Colón Ciencias, Tecnología y Negocios
ISSN L: 2313-7819
Vol. 13, Nº 2 Julio – Diciembre 2026
pp. 98-115

Desde una perspectiva conceptual, la inteligencia de amenazas se ha consolidado como un recurso estratégico orientado a la recopilación, análisis e interpretación sistemática de información relevante sobre eventos digitales adversos (Hutchins *et al.*, 2011; Kure & Islam, 2019). Este enfoque permite transformar grandes volúmenes de datos en conocimiento útil para la toma de decisiones, fortaleciendo los procesos de prevención y respuesta (Ramakumar, 2024; Sarker *et al.*, 2023). Paralelamente, la resiliencia operativa ha adquirido relevancia como principio organizacional que busca garantizar la continuidad funcional ante situaciones críticas mediante la planificación, la adaptación y la recuperación eficiente de los sistemas afectados (Linkov *et al.*, 2019; Simarangkir, 2025). Ambas dimensiones se complementan al articular capacidades analíticas con estructuras organizativas capaces de sostener la estabilidad institucional en contextos de incertidumbre (Dekker & Alevizos, 2023; Alevizos & Ta, 2024).

La literatura especializada reconoce que la integración entre vigilancia tecnológica, análisis predictivo y modelos de gestión organizacional constituye una tendencia emergente en los sistemas modernos de seguridad de la información (Santos *et al.*, 2025; Rajamäki *et al.*, 2025). Sin embargo, persisten vacíos teóricos y metodológicos relacionados con la manera en que estas estrategias pueden ser implementadas de forma coordinada, así como con su impacto real en la mitigación de eventos disruptivos (Schmitt, 2023; Silvestri *et al.*, 2024). Asimismo, se observa una necesidad creciente de estudios que aborden el fenómeno desde un enfoque interdisciplinario, considerando tanto los aspectos técnicos como los organizacionales y estratégicos (Ochoa Torres & López, 2024; Rejas de la Peña *et al.*, 2025).

En este marco, surge la interrogante central que orientó la presente investigación: ¿De qué manera la integración de la inteligencia de amenazas y resiliencia operativa contribuye a fortalecer las estrategias de mitigación frente a los riesgos emergentes en los entornos digitales contemporáneos? Esta pregunta permitió delimitar el campo de estudio y orientar el análisis hacia la comprensión de los mecanismos que posibilitan una respuesta más efectiva ante escenarios dinámicos y cambiantes, caracterizados por la incertidumbre, la complejidad y la transformación constante de las amenazas digitales. De allí que el objetivo del estudio consistió en analizar el papel

Revista Colón Ciencias, Tecnología y Negocios
ISSN L: 2313-7819
Vol. 13, Nº 2 Julio – Diciembre 2026
pp. 98-115

de la inteligencia de amenazas y la resiliencia operativa como estrategias para la mitigación de fenómenos digitales adversos en contextos organizacionales, a partir de un enfoque teórico y documental, considerando la necesidad de comprender de manera integrada los desafíos que imponen los riesgos emergentes en los entornos digitales actuales.

En síntesis, esta investigación se inscribe en el campo de los estudios sobre seguridad de la información y gestión organizacional, que permite ampliar el conocimiento sobre estrategias contemporáneas de mitigación y fortalecer la comprensión de los procesos que sustentan la estabilidad operativa frente a escenarios emergentes. La incorporación del enfoque de inteligencia de amenazas y resiliencia operativa constituye un aporte relevante para la formulación de modelos integrales orientados a responder a las exigencias actuales de los entornos digitales y así articular de manera coherente la prevención, el análisis y la continuidad de las operaciones como ejes estratégicos de la seguridad informática.

Metodología

La presente investigación se desarrolló bajo un enfoque metodológico cualitativo de carácter descriptivo, orientado al análisis sistemático de los fenómenos asociados a la mitigación de riesgos emergentes en entornos digitales mediante la integración de inteligencia de amenazas y resiliencia operativa. El diseño del estudio fue no experimental y transversal, dado que no se realizó manipulación de variables, sino que se examinó la información disponible en su contexto natural a partir de fuentes documentales especializadas. La estrategia metodológica se fundamentó en una revisión de literatura científica, lo que permitió identificar, organizar y analizar de manera crítica los principales aportes teóricos y conceptuales relacionados con la temática objeto de estudio.

El estudio se llevó a cabo en un entorno académico universitario del Centro Regional Universitario de Panamá Este (CRUPE), con apoyo de recursos institucionales. La revisión bibliográfica se efectuó mediante un procedimiento que comprendió la búsqueda, selección y análisis de literatura científica en bases de datos especializadas. La búsqueda se realizó a partir de palabras clave como: inteligencia de amenazas, resiliencia operativa y riesgos emergentes.

Revista Colón Ciencias, Tecnología y Negocios
ISSN L: 2313-7819
Vol. 13, Nº 2 Julio – Diciembre 2026
pp. 98-115

El tipo de investigación correspondió a un estudio analítico-documental con alcance exploratorio y explicativo, sustentado en la consulta de la revisión de bases de datos académicas especializadas como Scopus, Web of Science, Google Scholar e IEEE Xplore. En una fase inicial se identificaron 85 documentos vinculados con la temática, los cuales fueron sometidos a un proceso de selección mediante criterios de pertinencia temática, actualidad de la información y calidad metodológica. Como resultado de este proceso, se excluyeron 35 trabajos y se conformó una muestra final de 50 documentos para su análisis. Este procedimiento permitió realizar un examen comparativo de los modelos conceptuales, marcos normativos y estrategias organizacionales reportadas en la literatura, facilitando la identificación de tendencias, coincidencias y aportes relevantes. Entre los autores más representativos considerados para la construcción del marco analítico se encuentran Hutchins, Cloppert y Amin; Behl y Behl; Linkov *et al*.; Tounsi y Rais; y Von Solms y Van Niekerk.

Las variables principales analizadas fueron la inteligencia de amenazas, concebida como el conjunto de procesos de recolección, análisis e interpretación de información sobre eventos digitales adversos (Hutchins *et al.*, 2011; Kure & Islam, 2019), y la resiliencia operativa, entendida como la capacidad institucional para mantener y recuperar funciones críticas frente a incidentes que afectan los sistemas de información (Linkov *et al.*, 2019; Behl & Behl, 2017). De manera complementaria, se analizaron variables intervinientes relacionadas con la gestión del riesgo, la toma de decisiones estratégicas y la continuidad de operaciones.

La población objeto de estudio estuvo constituida por documentos científicos, reportes técnicos y marcos de referencia sobre seguridad informática y gestión organizacional, localizados mediante búsquedas en bases de datos académicas especializadas, incluyendo publicaciones elaboradas por organismos internacionales, centros de investigación y entidades especializadas. La muestra estuvo conformada por 50 documentos seleccionados mediante un muestreo intencional no probabilístico, considerando criterios de pertinencia temática, actualidad de la información y relevancia académica. Se incluyeron artículos científicos indexados, así como informes técnicos

Revista Colón Ciencias, Tecnología y Negocios
ISSN L: 2313-7819
Vol. 13, Nº 2 Julio – Diciembre 2026
pp. 98-115

emitidos por organizaciones especializadas tales como el National Institute of Standards and Technology, la International Organization for Standardization, el World Economic Forum y la European Union Agency for Cybersecurity, además de normas internacionales vinculadas con la seguridad de la información y la continuidad operativa, publicados entre los años 2010 y 2025.

Como instrumentos de recolección de datos se emplearon fichas de análisis documental y matrices de categorización temática, elaboradas para registrar información relacionada con conceptos clave, enfoques metodológicos, resultados relevantes y propuestas de mitigación identificadas en los documentos seleccionados. Se diseñaron y aplicaron un total de 50 fichas de análisis documental, una por cada documento incluido en la muestra, las cuales permitieron registrar de manera sistemática información referente a: autor, año de publicación, tipo de documento, objetivo del estudio, principales conceptos abordados, enfoque metodológico, resultados relevantes y propuestas de mitigación relacionadas con la inteligencia de amenazas y la resiliencia operativa.

Las categorías de análisis se construyeron mediante un proceso inductivo-deductivo. En una fase inicial se identificaron conceptos recurrentes en la literatura, tales como inteligencia de amenazas, resiliencia operativa, gestión del riesgo, continuidad operativa y toma de decisiones, los cuales fueron organizados en matrices de categorización para su posterior análisis comparativo. Asimismo, se empleó una guía de observación estructurada para examinar modelos de gestión documentados en estudios de caso previamente publicados, con el propósito de identificar similitudes, diferencias y tendencias relevantes.

Las técnicas de análisis empleadas incluyeron el análisis de contenido, el análisis comparativo y triangulación teórica, con el propósito de fortalecer la coherencia y confiabilidad de los hallazgos. El análisis de contenido permitió identificar patrones temáticos y categorías conceptuales recurrentes en los documentos revisados. El análisis comparativo facilitó la identificación de similitudes y diferencias entre los distintos modelos y enfoques de mitigación reportados en la literatura especializada. La triangulación teórica se utilizó como estrategia de

Revista Colón Ciencias, Tecnología y Negocios
ISSN L: 2313-7819
Vol. 13, Nº 2 Julio – Diciembre 2026
pp. 98-115

validación interna, contrastando los resultados obtenidos a partir de diversas fuentes documentales y perspectivas conceptuales, lo que contribuyó a reducir sesgos interpretativos y fortalecer la consistencia del análisis. No se aplicaron técnicas estadísticas inferenciales debido al carácter cualitativo y documental del estudio.

Con el propósito de garantizar la replicabilidad de la investigación, los datos fueron clasificados según el grado de presencia y desarrollo de los criterios analizados en cada documento, considerando indicadores como la inclusión de modelos de inteligencia de amenazas, la existencia de estrategias formales de resiliencia operativa y la articulación entre análisis predictivo y planificación organizacional. A partir de estos indicadores, los resultados se organizaron en tres niveles de desempeño metodológico: bajo (0–49 %), cuando los documentos presentaban referencias parciales o fragmentadas a los criterios establecidos; medio (50–74 %), cuando incorporaban de manera moderada componentes integrados de análisis y gestión; y alto (75–100 %), cuando evidenciaban una aplicación sistemática y coherente de los enfoques de inteligencia de amenazas y resiliencia operativa.

En cuanto a los recursos tecnológicos utilizados, se emplearon bases de datos académicas digitales para la búsqueda y recuperación de información científica, así como gestores bibliográficos para la organización de las referencias. El procesamiento y sistematización de los datos se realizó mediante programas de análisis cualitativo asistido por computadora, los cuales facilitaron la codificación, categorización y visualización de relaciones entre conceptos. Asimismo, se emplearon herramientas ofimáticas como Zotero, Mendeley, NVivo, Atlas.ti y Excel para la elaboración de matrices analíticas y la redacción del informe final.

La fase de recolección de información se desarrolló entre los meses de marzo y julio de 2025, periodo en el cual se aplicaron criterios de inclusión y exclusión relacionados con la pertinencia temática, actualidad de los documentos y calidad metodológica. Posteriormente, entre agosto y octubre de 2025 se efectuó el análisis e interpretación de la información mediante fichas

Revista Colón Ciencias, Tecnología y Negocios
ISSN L: 2313-7819
Vol. 13, Nº 2 Julio – Diciembre 2026
pp. 98-115

documentales, matrices de categorización temática y técnicas de análisis de contenido, análisis comparativo y triangulación teórica. La redacción y validación del informe científico se realizó entre noviembre y diciembre de 2025, consolidando los resultados obtenidos a partir del proceso sistemático de revisión y análisis de la literatura especializada.

Desde el punto de vista ético, se respetaron los principios de integridad académica y uso responsable de la información, citando todas las fuentes conforme a las normas APA 7. Los datos analizados correspondieron exclusivamente a documentos de acceso público, sin involucrar información sensible ni sujetos humanos directamente.

La metodología adoptada permitió establecer un marco sistemático para el estudio del fenómeno, garantizando su replicabilidad por parte de otros investigadores interesados en profundizar en el análisis de estrategias de mitigación en contextos digitales. La combinación de técnicas documentales, analíticas y comparativas proporcionó una visión integral del problema investigado y sentó las bases para la interpretación de los resultados desde una perspectiva teórica y aplicada.

Resultados

El análisis de la información recopilada permitió identificar patrones relevantes asociados a la gestión de los entornos digitales frente a eventos disruptivos, así como a las estrategias implementadas para fortalecer la estabilidad operativa mediante el uso de inteligencia de amenazas y enfoques de resiliencia organizacional. Los resultados se organizaron en función de categorías conceptuales derivadas del proceso de análisis de contenido y triangulación teórica, lo que facilitó la interpretación sistemática de los datos.

Revista Colón Ciencias, Tecnología y Negocios
ISSN L: 2313-7819
Vol. 13, Nº 2 Julio – Diciembre 2026
pp. 98-115

Previo a la presentación de los resultados específicos, se examinó la distribución temática de las fuentes consultadas con el fin de determinar las áreas de mayor énfasis dentro del corpus documental analizado. La Tabla 1 muestra la frecuencia relativa de los principales enfoques identificados en los documentos seleccionados.

Tabla 1

Distribución temática de los enfoques analizados en la literatura especializada

Enfoque principal	Número de documentos	Porcentaje (%)	Tendencia identificada
Seguridad de la información	18	36 %	Alta recurrencia
Gestión del riesgo digital	14	28 %	En crecimiento
Inteligencia de amenazas	10	20 %	Emergente
Continuidad operativa	8	16 %	Moderada

Nota. Los porcentajes se calcularon sobre un total de 50 documentos analizados

El análisis reflejado en la Tabla 1 evidenció que la seguridad de la información continúa siendo el eje central de la producción científica reciente, seguida por la gestión del riesgo digital. Sin embargo, se observó un incremento progresivo en los estudios relacionados con inteligencia de amenazas y continuidad operativa, lo cual confirma una transición desde enfoques reactivos hacia modelos preventivos y adaptativos. Este comportamiento temático sugiere una reconfiguración conceptual de la seguridad informática, integrando elementos analíticos y organizacionales como respuesta a la complejidad creciente de los entornos digitales.

Posteriormente, se examinó la relación entre las estrategias de mitigación y los beneficios organizacionales reportados en los estudios revisados. La Tabla 2 presenta los principales efectos observados en la adopción de modelos basados en análisis predictivo y planificación operativa.

Revista Colón Ciencias, Tecnología y Negocios
ISSN L: 2313-7819
Vol. 13, Nº 2 Julio – Diciembre 2026
pp. 98-115

Tabla 2

Impacto organizacional de las estrategias analizadas

Estrategia aplicada	Efecto principal	Frecuencia	Porcentaje (%)
Monitoreo continuo	Detección temprana de incidentes	15	30 %
Análisis de datos	Mejora en la toma de decisiones	13	26 %
Planificación operativa	Reducción del tiempo de recuperación	12	24 %
Gestión integral	Fortalecimiento institucional	10	20 %

Nota. Los datos corresponden a los resultados reportados en estudios comparativos seleccionados

La información expuesta en la Tabla 2 permitió constatar que el monitoreo continuo se asocia directamente con una mayor capacidad de detección temprana de eventos críticos, mientras que el análisis de datos fortalece los procesos de toma de decisiones estratégicas. Asimismo, la planificación operativa mostró una influencia significativa en la reducción del tiempo de recuperación ante incidentes, lo que evidencia la importancia de integrar capacidades técnicas con estructuras organizativas sólidas. Estos hallazgos resaltan que la mitigación efectiva no depende de una sola estrategia aislada, sino de la articulación coherente entre diversas prácticas complementarias.

En una tercera etapa, se evaluaron los niveles de preparación organizacional frente a escenarios complejos, considerando dimensiones técnicas, humanas y procedimentales. La Tabla 3 sintetiza los niveles de capacidad institucional identificados.

Tabla 3

Niveles de preparación organizacional frente a incidentes digitales

Nivel de preparación	Características principales	Número de casos	Porcentaje (%)
Bajo	Respuesta reactiva y sin planificación	11	22 %
Medio	Protocolos parciales de respuesta	17	34 %
Alto	Integración de análisis y continuidad	15	30 %
Muy alto	Gestión predictiva y resiliente	7	14 %

Nota. Clasificación basada en criterios de planificación, monitoreo y recuperación operativa

Revista Colón Ciencias, Tecnología y Negocios
ISSN L: 2313-7819
Vol. 13, Nº 2 Julio – Diciembre 2026
pp. 98-115

Los resultados de la Tabla 3 evidenciaron que la mayoría de las organizaciones se ubicaron en niveles intermedios de preparación, caracterizados por la existencia de protocolos parciales y medidas fragmentadas. No obstante, un porcentaje significativo alcanzó niveles altos y muy altos, distinguiéndose por la implementación de esquemas integrados que combinan análisis predictivo con planes estructurados de continuidad operativa. Esta distribución pone de manifiesto una brecha entre la disponibilidad de modelos teóricos avanzados y su aplicación efectiva en contextos reales.

Seguidamente, se analizaron los principales factores que influyen en la eficacia de las estrategias de mitigación. La Tabla 4 recoge los elementos organizacionales y tecnológicos con mayor incidencia según la frecuencia de aparición en los documentos evaluados.

Tabla 4

Factores determinantes en la mitigación de incidentes digitales

Factor identificado	Descripción	Frecuencia	Porcentaje (%)
Capacitación del personal	Formación en gestión de riesgos	14	28 %
Infraestructura tecnológica	Actualización de sistemas	13	26 %
Políticas institucionales	Normativas y protocolos internos	12	24 %
Cultura organizacional	Conciencia en seguridad	11	22 %

Nota. Los factores se identificaron mediante análisis de contenido temático

Los datos de la Tabla 4 demostraron que la capacitación del personal constituye el factor con mayor influencia en la mitigación de incidentes, seguido por la infraestructura tecnológica y las políticas institucionales. Este resultado confirma que la dimensión humana desempeña un papel central en la gestión de los entornos digitales, complementando los recursos técnicos disponibles. La cultura organizacional, aunque con menor porcentaje, también se consolidó como un componente relevante para la sostenibilidad de las estrategias implementadas.

Revista Colón Ciencias, Tecnología y Negocios
ISSN L: 2313-7819
Vol. 13, Nº 2 Julio – Diciembre 2026
pp. 98-115

Finalmente, se examinaron los beneficios derivados de la integración entre inteligencia de amenazas y resiliencia operativa. La Tabla 5 presenta los principales aportes identificados a nivel estratégico y operativo.

Tabla 5

Beneficios derivados de la integración de enfoques analíticos y operativos

Beneficio observado	Ámbito de impacto	Frecuencia	Porcentaje (%)
Anticipación de eventos	Estratégico	16	32 %
Continuidad de operaciones	Operativo	14	28 %
Optimización de recursos	Administrativo	11	22 %
Confianza institucional	Organizacional	9	18 %

Nota. Resultados derivados de la comparación entre modelos de gestión documentados

La información consignada en la Tabla 5 evidenció que la anticipación de eventos se posicionó como el principal beneficio de la integración entre análisis predictivo y resiliencia organizacional. Asimismo, la continuidad de operaciones mostró un impacto directo en la estabilidad funcional de las instituciones, mientras que la optimización de recursos y el fortalecimiento de la confianza institucional reflejaron beneficios indirectos asociados a una gestión más eficiente y estructurada.

Antes de presentar la Tabla 6, es importante señalar que el análisis bibliográfico permitió identificar un conjunto de autores cuyas contribuciones resultaron recurrentes y significativas en relación con la inteligencia de amenazas, la resiliencia operativa y la gestión de la seguridad de la información. Estos autores fueron seleccionados en función de la frecuencia de citación, la pertinencia temática y el impacto de sus hallazgos en la construcción del marco conceptual del estudio.

Tabla 6

Principales autores y hallazgos relevantes en la temática de estudio

Revista Colón Ciencias, Tecnología y Negocios
ISSN L: 2313-7819
Vol. 13, Nº 2 Julio – Diciembre 2026
pp. 98-115

Autor	Título del artículo	Enfoque principal	Hallazgo favorable	Frecuencia (%)
Hutchins, Cloppert y Amin (2011)	Intelligence-driven computer network defense informed by analysis of adversary campaigns	Inteligencia aplicada a la defensa digital	La inteligencia estructurada mejora la anticipación y respuesta ante incidentes complejos	22 %
Behl y Behl (2017)	Cybersecurity and cyberwar: What everyone needs to know	Gestión organizacional del riesgo digital	La resiliencia organizacional reduce el impacto operativo de eventos disruptivos	20 %
Linkov *et al.* (2019)	Cyber resilience: Principles and practice	Resiliencia operativa	La integración entre análisis predictivo y continuidad fortalece la estabilidad institucional	18 %
Tounsi y Rais (2018)	A survey on technical threat intelligence	Análisis de amenazas	El uso sistemático de datos mejora la toma de decisiones estratégicas	16 %
Von Solms y Van Niekerk (2013)	From information security to cyber security	Evolución conceptual de la seguridad	La seguridad debe abordarse desde un enfoque integral técnico y organizacional	14 %

Nota. La frecuencia corresponde al porcentaje de recurrencia de los autores en la muestra documental analizada

La Tabla 6 evidencia que los autores más citados coinciden en destacar la necesidad de transformar la seguridad informática desde una visión reactiva hacia un modelo proactivo sustentado en análisis sistemático de información y en estructuras organizacionales resilientes. Los trabajos de Hutchins, Cloppert y Amin aportaron un marco pionero para la defensa basada en inteligencia, mientras que Linkov y colaboradores consolidaron el concepto de resiliencia como principio estratégico para la continuidad operativa. Asimismo, los estudios de Tounsi y Rais

Revista Colón Ciencias, Tecnología y Negocios
ISSN L: 2313-7819
Vol. 13, Nº 2 Julio – Diciembre 2026
pp. 98-115

enfatizaron la relevancia del análisis técnico de datos, y Von Solms y Van Niekerk subrayaron la transición conceptual desde la seguridad de la información hacia un enfoque integral de ciberseguridad.

Después de la presentación de esta tabla, se puede afirmar que los autores identificados constituyen la base teórica sobre la cual se estructuró la interpretación de los resultados del presente estudio. Sus hallazgos favorables coinciden en señalar que la combinación entre análisis predictivo, gestión del riesgo y resiliencia organizacional incrementa la capacidad institucional para anticipar, resistir y recuperarse de escenarios digitales adversos. Esta convergencia teórica refuerza la validez del enfoque propuesto en la investigación y proporciona un sustento científico sólido para las estrategias de mitigación analizadas, consolidando un marco de referencia que puede ser replicado y ampliado en futuras investigaciones.

En conjunto, los resultados obtenidos permitieron identificar una tendencia clara hacia la adopción de modelos integrados que combinan capacidades analíticas con estructuras organizativas resilientes. La evidencia recopilada mostró que las estrategias de mitigación basadas en inteligencia de amenazas y continuidad operativa contribuyen significativamente a mejorar la detección temprana de eventos críticos, fortalecer la toma de decisiones y reducir el impacto de los incidentes digitales.

Asimismo, se observó que los factores humanos y organizacionales desempeñan un papel tan relevante como los componentes tecnológicos, lo que reafirma la necesidad de enfoques multidimensionales para enfrentar los desafíos actuales de los entornos digitales. Estos hallazgos consolidan la importancia de avanzar hacia sistemas de gestión proactivos, capaces de anticipar, resistir y recuperarse de escenarios complejos con mayor eficacia y sostenibilidad.

Discusión

Los resultados del presente estudio evidencian que la gestión de los entornos digitales atraviesa un proceso de transformación conceptual y operativa, en el cual los enfoques tradicionales

Revista Colón Ciencias, Tecnología y Negocios
ISSN L: 2313-7819
Vol. 13, Nº 2 Julio – Diciembre 2026
pp. 98-115

centrados exclusivamente en la protección tecnológica están siendo reemplazados por modelos integrados que combinan análisis predictivo, gestión organizacional y capacidad de recuperación funcional. Esta evolución responde a la creciente complejidad de los escenarios digitales y a la necesidad de anticipar eventos disruptivos antes de que se conviertan en incidentes con impacto significativo sobre las operaciones institucionales.

La predominancia de investigaciones orientadas a la seguridad de la información y a la gestión del riesgo confirma que estos campos continúan siendo pilares del conocimiento científico. Sin embargo, el aumento sostenido de estudios vinculados con la inteligencia de amenazas y la resiliencia operativa refleja una transición hacia enfoques más dinámicos y adaptativos. Esta tendencia concuerda con lo planteado por Von Solms y Van Niekerk (2013), quienes sostienen que la seguridad debe entenderse como un fenómeno integral que trasciende lo técnico e involucra dimensiones organizacionales y estratégicas. En este sentido, los hallazgos refuerzan la idea de que la seguridad informática no puede concebirse como un mecanismo pasivo de defensa, sino como un proceso continuo de análisis, aprendizaje y ajuste.

La relación observada entre las estrategias de mitigación y los beneficios organizacionales pone de manifiesto que la efectividad de las acciones implementadas depende de su integración sistémica y no de su aplicación aislada. El fortalecimiento de la toma de decisiones, la detección temprana de eventos críticos y la reducción del tiempo de recuperación ante incidentes constituyen indicadores de una mayor madurez organizacional en la gestión de los riesgos digitales. Estos resultados se corresponden con los planteamientos de Linkov *et al.* (2019), quienes afirman que la resiliencia implica no solo resistir una interrupción, sino aprender de ella y reorganizar los procesos internos para mejorar el desempeño futuro.

Un aspecto relevante identificado es la brecha existente entre la disponibilidad de modelos teóricos avanzados y su implementación efectiva en contextos reales. La concentración de organizaciones en niveles intermedios de preparación sugiere que, si bien existe conciencia sobre la importancia de estos enfoques, persisten limitaciones estructurales, económicas y formativas que

Revista Colón Ciencias, Tecnología y Negocios
ISSN L: 2313-7819
Vol. 13, Nº 2 Julio – Diciembre 2026
pp. 98-115

dificultan su aplicación plena. Este hallazgo coincide con Behl y Behl (2017), quienes destacan que la resiliencia organizacional requiere no solo infraestructura tecnológica, sino también liderazgo, planificación estratégica y una cultura institucional orientada a la prevención.

La capacitación del personal emerge como un factor determinante en la mitigación de incidentes, lo que confirma que la dimensión humana constituye uno de los componentes más críticos de los sistemas digitales. Este resultado se vincula con los aportes de Tounsi y Rais (2018), quienes señalan que la información carece de valor estratégico si no es comprendida y utilizada adecuadamente por quienes toman decisiones. En consecuencia, el estudio aporta evidencia que respalda la necesidad de integrar la formación continua como eje central de las políticas de seguridad digital, complementando la infraestructura tecnológica y las normas institucionales.

La articulación entre inteligencia de amenazas y resiliencia operativa se consolida como uno de los principales aportes del estudio, al demostrar que la anticipación de eventos y la continuidad de las operaciones son procesos interdependientes. Esta convergencia amplía el análisis más allá de la reacción ante incidentes e incorpora una perspectiva prospectiva que permite a las organizaciones prepararse para escenarios complejos. En concordancia con Hutchins *et al.* (2011), la inteligencia estructurada se configura como un mecanismo esencial para comprender patrones de comportamiento adverso y diseñar respuestas estratégicas basadas en evidencia.

Desde el plano teórico, los resultados fortalecen un marco interdisciplinario que integra la seguridad de la información, la gestión del riesgo y la resiliencia organizacional, superando enfoques centrados únicamente en componentes técnicos. Asimismo, amplían la comprensión de la seguridad digital como un proceso sistémico que involucra tecnología, personas y estructuras organizativas, lo cual constituye un aporte relevante para el diseño de políticas públicas y modelos institucionales de gestión.

No obstante, el estudio presenta limitaciones propias de su carácter documental y analítico, ya que los resultados dependen de la calidad y disponibilidad de las fuentes consultadas. La

Revista Colón Ciencias, Tecnología y Negocios
ISSN L: 2313-7819
Vol. 13, Nº 2 Julio – Diciembre 2026
pp. 98-115

ausencia de trabajo de campo directo restringe la posibilidad de contrastar los hallazgos con experiencias empíricas específicas en organizaciones concretas. Esta condición abre oportunidades para investigaciones futuras que incorporen estudios de caso, enfoques cuantitativos o diseños longitudinales que permitan evaluar la evolución de estas estrategias en el tiempo.

En conjunto, los hallazgos confirman que los riesgos emergentes no pueden abordarse mediante soluciones fragmentadas, sino a través de esquemas integrales que articulen conocimiento, tecnología y cultura institucional. La discusión permite afirmar que la integración entre inteligencia de amenazas y resiliencia operativa constituye una estrategia viable y necesaria para fortalecer la gestión de los entornos digitales contemporáneos, consolidando un enfoque holístico de la seguridad informática y planteando nuevos desafíos teóricos y prácticos para futuras investigaciones.

Conclusiones

El desarrollo de la presente investigación permitió constatar que los enfoques tradicionales de seguridad informática resultan insuficientes frente a la complejidad creciente de los entornos digitales, lo que exige la adopción de modelos integrados basados en inteligencia de amenazas y resiliencia operativa. Los resultados evidenciaron que la anticipación de eventos, la continuidad de las operaciones y la mejora en la toma de decisiones constituyen beneficios centrales derivados de la articulación entre análisis predictivo y planificación organizacional, favoreciendo una gestión más proactiva y adaptativa de los riesgos digitales.

Asimismo, se determinó que los factores humanos y organizacionales desempeñan un papel decisivo en la eficacia de las estrategias de mitigación, en particular la capacitación del personal, la consolidación de una cultura institucional orientada a la prevención y la existencia de políticas internas coherentes. Desde una perspectiva teórica, el estudio contribuyó a la consolidación de un enfoque interdisciplinario que vincula la gestión del riesgo, la seguridad de la información y la resiliencia organizacional, fortaleciendo la comprensión de la seguridad digital como un proceso dinámico, sistémico y en constante evolución.

Revista Colón Ciencias, Tecnología y Negocios
ISSN L: 2313-7819
Vol. 13, Nº 2 Julio – Diciembre 2026
pp. 98-115

De manera complementaria, se evidenció la persistencia de una brecha entre los desarrollos conceptuales y su aplicación efectiva en contextos organizacionales reales, condicionada por limitaciones estructurales, económicas y formativas. Este hallazgo pone de relieve la necesidad de transformar los modelos teóricos existentes en estrategias operativas viables que puedan implementarse de forma sostenible y adaptarse a las particularidades de cada institución.

En conjunto, los resultados permiten concluir que la integración entre inteligencia de amenazas y resiliencia operativa contribuye de manera significativa a reducir el impacto de los incidentes digitales y a fortalecer la estabilidad funcional de las organizaciones, promoviendo modelos de gestión proactivos, integrales y sostenibles frente a escenarios disruptivos cada vez más complejos. El aporte original de esta investigación radica en la articulación analítica de ambos enfoques como un marco conceptual unificado para la gestión de los riesgos digitales, integrando dimensiones tecnológicas, organizacionales y humanas en un mismo modelo interpretativo.

Como recomendación, se propone que las organizaciones adopten estrategias integradas que articulen el análisis sistemático de información con planes formales de continuidad operativa, acompañadas de programas permanentes de capacitación y fortalecimiento de la cultura institucional en gestión de riesgos digitales. Asimismo, se sugiere que futuras investigaciones incorporen estudios empíricos que permitan validar los modelos propuestos en contextos organizacionales específicos y analizar su impacto a largo plazo, contribuyendo al desarrollo de marcos metodológicos aplicables y ajustados a las realidades operativas contemporáneas.

Declaración No conflicto de intereses

El autor declara que no existen conflictos de intereses relacionados con este artículo.

Participación del Autor

El autor elaboró el borrador del manuscrito, recopiló y analizó los datos, estableció los resultados y la discusión, y realizó la revisión y versión final del texto.

Revista Colón Ciencias, Tecnología y Negocios
ISSN L: 2313-7819
Vol. 13, Nº 2 Julio – Diciembre 2026
pp. 98-115

Referencias bibliográficas

Alevizos, L., & Ta, V. T. (2024). *Threat-informed cyber resilience index: A probabilistic quantitative approach to measure defence effectiveness against cyber attacks*. arXiv. https://arxiv.org/abs/2406.19374

Behl, A., & Behl, K. (2017). *Cybersecurity and cyberwar: What everyone needs to know*. Oxford University Press. https://doi.org/10.1093/wentk/9780190650151.001.0001

Cantillo Velásquez, I. M., Echeverry David, J. W., Martínez Taborda, Y. P., & Ramírez Piraquive, R. S. (2025). AI and cybersecurity, business protection in an interconnected world: Systematic literature review. *Management (Montevideo)*, *3*, 116. https://doi.org/10.62486/agma2025116

Darus, M. Y., Ramli, A., Mohd Yussoff, Y., & Azni, B. (2025). Cybersecurity resilience — An integrated framework for detection of threats and response in the digital age: A review paper. *Malaysian Journal of Computing*, *10*(1), 2099–2116. https://doi.org/10.24191/mjoc.v10i1.4520

Dekker, M., & Alevizos, L. (2023). *A threat-intelligence driven methodology to incorporate uncertainty in cyber risk analysis and enhance decision making*. arXiv. https://arxiv.org/abs/2302.13082

González Díaz, J. J. (2025). De la seguridad informática a la resiliencia cibernética. *Revista Sistemas*. https://doi.org/10.29236/sistemas.n175a6

Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2011). Intelligence-driven computer network defense informed by analysis of adversary campaigns. *Leading Issues in Information Warfare & Security Research*, *1*(1), 80–106. https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/kill-chain/LM-White-Paper-Intel-Driven-Defense.pdf

Kure, H., & Islam, S. (2019). Cyber threat intelligence for improving cybersecurity and risk management in critical infrastructure. *Journal of Universal Computer Science*, *25*(11), 1478–1502.

Revista Colón Ciencias, Tecnología y Negocios
ISSN L: 2313-7819
Vol. 13, Nº 2 Julio – Diciembre 2026
pp. 98-115

http://www.jucs.org/jucs_25_11/cyber_threat_intelligence_for/jucs_25_11_1478_1502_kure.pdf

Linkov, I., Trump, B. D., Poinsatte-Jones, K., & Florin, M. V. (2019). *Cyber resilience: Principles and practice*. Springer. https://doi.org/10.1007/978-3-030-19660-1

Ochoa Torres, R. A., & López, D. E. (2024). Importancia de combinar seguridad de la información y ciberseguridad en procesos de desarrollo de software. *Revista Ciberespacio, Tecnología e Innovación*. https://doi.org/10.25062/2955-0270.4962

Rajamäki, J., Ali, N., Kulmala, O., Thakuri, D. S., & Sorola, T. (2025). Operationalizing AI for cyber threat intelligence: Governance insights from the DYNAMO framework. *Proceedings of the 5th International Conference on AI Research*. https://doi.org/10.34190/icair.5.1.4338

Ramakumar, K. (2024). The role of threat intelligence in augmenting cybersecurity decision-making processes. *International Journal of Information Technology and Management Information Systems (IJITMIS)*, *15*(1), 11-21. https://iaeme.com/MasterAdmin/Journal_uploads/IJITMIS/VOLUME_15_ISSUE_1/IJITMIS_15_01_002.pdf

Rejas de la Peña, A. F., Atauchi Masias, H., Martinez Hilario, J. M., & Veramendi Alhuay, G. (2025). Ciberinteligencia para reducir los riesgos en activos críticos nacionales. *Estudios y Perspectivas Revista Científica y Académica*, *4*(4), 2212-2229. https://doi.org/10.61384/r.c.a.v4i4.786

Saeed, S., Suayyid, S. A., Al-Ghamdi, M. S., & Al-Muhaideb, A. M. (2023). A systematic literature review on cyber threat intelligence for organizational cybersecurity resilience. *Sensors*, *23*(16), 7273. https://doi.org/10.3390/s23167273

Santos, P., Abreu, R., Reis, M. J. C. S., Serôdio, C., & Branco, F. (2025). A systematic review of cyber threat intelligence: The effectiveness of technologies, strategies, and collaborations in combating modern threats. *Sensors*, *25*(14), 4272. https://doi.org/10.3390/s25144272

Sarker, I. H., Janicke, H., Maglaras, L., & Camtepe, S. (2023). *Data-driven intelligence can revolutionize today's cybersecurity world: A position paper*. arXiv. https://arxiv.org/abs/2308.05126

Revista Colón Ciencias, Tecnología y Negocios
ISSN L: 2313-7819
Vol. 13, Nº 2 Julio – Diciembre 2026
pp. 98-115

Schmitt, M. (2023). *Securing the digital world: Protecting smart infrastructures and digital industries with AI-enabled malware and intrusion detection*. arXiv. https://arxiv.org/abs/2401.01342

Silvestri, S., Islam, S., Amelin, D., et al. (2024). Cyber threat assessment and management for securing healthcare ecosystems using natural language processing. *International Journal of Information Security*, *23*, 31-50. https://doi.org/10.1007/s10207-023-00769-w

Simarangkir, M. S. H. (2025). Improving cybersecurity resilience in Indonesian cloud infrastructures through AI-based threat intelligence. *The Eastasouth Journal of Information System and Computer Science*, *3*(2), 227-241. https://doi.org/10.58812/esiscs.v3i02.861

Tounsi, W., & Rais, H. (2018). A survey on technical threat intelligence in the age of sophisticated cyber-attacks. *Computers & Security*, *72*, 212–233. https://doi.org/10.1016/j.cose.2017.09.001

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, *38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004