# Gestión de riesgos en proyectos de ciberseguridad

José Leonardo Duran Hernández

Universitaria Agustiniana - Uniagustiniana

Facultad de Ingenierías

Programa de Gerencia de Proyectos

Bogotá D.C., Colombia

2026

**Gestión de riesgos en proyectos de ciberseguridad**

Trabajo de grado para optar al título correspondiente

Autor: José Leonardo Duran Hernández

Tutor: Laura Liliana Linares Romero

Universitaria Agustiniana - Uniagustiniana

Facultad de Ingenierías

Programa de Gerencia de Proyectos

Bogotá D.C., Colombia

2026

## Resumen

La gestión de riesgos en proyectos de ciberseguridad se ha convertido en un factor crítico para el éxito organizacional frente al creciente número de amenazas digitales. Este artículo tiene como propósito analizar los beneficios de la gestión integrada de riesgos en proyectos de ciberseguridad y su incidencia en el cumplimiento de objetivos, costos y plazos. El problema identificado radica en la baja adopción de prácticas formales de gestión de riesgos en la planificación de proyectos, lo que genera altos índices de fracaso. Se empleó una metodología con enfoque cualitativo y alcance descriptivo, basada en revisión documental de normas técnicas (ISO 31000, ISO 27005), informes gubernamentales y estudios recientes del Project Management Institute y el FBI. Los principales hallazgos indican que solo el 30% de las organizaciones aplica gestión de riesgos en la planificación, y el 68% ha sufrido incidentes de ciberseguridad. Se concluye que una adecuada gestión de riesgos mejora la planificación, optimiza recursos, fortalece la toma de decisiones y aumenta la confianza de las partes interesadas, siendo indispensable para el éxito de proyectos de ciberseguridad.


Palabras clave: Gestión de riesgos; ciberseguridad; proyectos; ISO 31000; toma de decisiones.


## Abstract

Risk management in cybersecurity projects has become a critical factor for organizational success in the face of the growing number of digital threats. This article aims to analyze the benefits of integrated risk management in cybersecurity projects and its impact on meeting objectives, costs, and deadlines. The identified problem lies in the low adoption of formal risk management practices in project planning, which leads to high failure rates. A qualitative approach with a descriptive scope was employed, based on a documentary review of technical

standards (ISO 31000, ISO 27005), government reports, and recent studies from the Project Management Institute and the FBI. The main findings indicate that only 30% of organizations apply risk management in planning, and 68% have experienced cybersecurity incidents. It is concluded that proper risk management improves planning, optimizes resources, strengthens decision-making, and increases stakeholder confidence, making it essential for the success of cybersecurity projects.

Keywords: Risk management; cybersecurity; projects; ISO 31000; decision making.

## Introducción

La gestión de riesgos en la actualidad ha tomado un rol bastante importante en el desarrollo y sostenibilidad de las organizaciones, sin embargo, al momento de planificar el diseño y ejecución de proyectos, se pueden presentar diversas brechas que pueden afectar significativamente los resultados esperados y comprometer el cumplimiento de metas y objetivos, lo cual es inmediatamente proporcional a incrementos de costos y duración del proyecto, generando disminución de las ganancias esperadas (Dias, 2020).

De acuerdo a lo indicado en la NTC ISO 31000 de 2018, la gestión de riesgo corresponde a actividades coordinadas para dirigir y controlar la organización con relación al riesgo. (Cárdenas, 2024)

así mismo la gestión de riesgos de un proyecto es un proceso continuo que incluye la identificación, análisis, prioridad y mitigación de riesgos que pueden afectar el proyecto, por lo cual se interpreta como un conjunto de procesos mediante los cuales se realiza un análisis interdisciplinario, donde se evidencian oportunidades y amenazas que pueden influir negativamente en los proyectos.

De acuerdo a lo indicado en la revista Journal of Information Systems Engineering and Management Según estudios realizados para verificar los riesgos presentes en la gestión de proyectos, se tomó una muestra 768 gerentes de proyectos, los cuales pertenecían a 392 organizaciones, se encontró que solo el 30% de las organizaciones aplica gestión de riesgos en la planificación (Wang, 2025).

Así mismo se muestra resultados de estudios realizados por Project Management Institute, donde se tomó una muestra de 5.402 gerentes de proyectos de diferentes condiciones

geográficas, se evidencio que la aplicación de riesgos estuvo relacionada al 28% de los fracasos en los proyectos (Wang, 2025).

La gestión de riesgos involucra un proceso continuo que incluye la identificación, análisis, evaluación y tratamiento de los riesgos a lo largo de todo el ciclo de vida del proyecto.

De acuerdo a lo anterior se evidencia que la gestión de riesgos cumple un papel indispensable, para la correcta implementación y ejecución de proyectos de pequeña, mediana y grande escala, siendo indispensable la identificación, el análisis y la definición de estrategias que apunten al cumplimiento de los objetivos (Zevallos, 2025).

Cuando en los proyectos se evidencian riesgos negativos, estos influyen en el aumento de los costos, retrasos de proyecto, sin embargo, cuando estos se gestionan de manera oportuna y planificada, se percibe también el riesgo como una oportunidad de mejora (Robles, 2025).

Las organizaciones que pretendan incluir proyectos ágiles, deben evaluar opciones de gestión de riesgos eficaces con enfoque a la comunicación abierta, desde la etapa de prediseño y así mismo generar la continuidad hasta la etapa de finalización y funcionamiento del proyecto, con el fin de identificar e implementar estrategias que posiblemente generen resultados esperados, buscando así mejorar las capacidades para garantizar la ejecución de proyectos exitosos (Dengela, 2018).

## Revisión de literatura

La gestión de riesgos ha evolucionado de ser una práctica complementaria a convertirse en un pilar estratégico dentro de la dirección de proyectos. Según la NTC ISO 31000:2018, la gestión del riesgo comprende "actividades coordinadas para dirigir y controlar una organización con relación al riesgo" (Cárdenas, 2024).En esta misma línea, Bravo (2024) sostiene que la ausencia de dichas actividades en la fase de planificación genera incrementos en costos y duración, afectando directamente la rentabilidad esperada.

Complementariamente, (Díaz, 2023) evidencia, a partir de una muestra de 768 gerentes de proyectos, que solo el 30% de las organizaciones incorpora la gestión de riesgos en sus planes iniciales, lo que revela una brecha significativa entre la teoría y la práctica.

Autores como López (2018) afirman que, cuando los riesgos negativos no se gestionan oportunamente, se convierten en causas recurrentes de sobrecostos y retrasos. No obstante, la misma autora señala que una gestión planificada permite reinterpretar el riesgo como una oportunidad de mejora continua (Montecinos, 2018). En coherencia con lo anterior, el Project Management Institute (PMI, 2018) destaca que las organizaciones que integran la gestión de riesgos desde la etapa de prediseño logran no solo mitigar amenazas, sino también fortalecer su capacidad de respuesta ante eventos imprevistos. De esta manera, la literatura converge en que la gestión de riesgos no es un proceso aislado, sino un sistema transversal que acompaña todo el ciclo de vida del proyecto.

Cuando se traslada este marco general al ámbito de la ciberseguridad, la relevancia de la gestión de riesgos se amplifica debido a la naturaleza dinámica y creciente de las amenazas digitales. (Paz, 2025)

señala que la gestión de riesgos en proyectos de ciberseguridad es un componente fundamental del desarrollo estratégico, especialmente ante el incremento de ataques informáticos a nivel global. Por su parte, la Comisión de Regulación de Comunicaciones (CRC, 2025) advierte que, a pesar de los esfuerzos por mitigar amenazas como el ransomware y el phishing, surgen constantemente nuevos actores y tácticas que vulneran la seguridad organizacional. En este contexto, (Pillaga, 2025) añade que el 81% de los proyectos exitosos en ciberseguridad se caracterizan por una fuerte colaboración entre equipos multidisciplinarios, lo que subraya la necesidad de integrar la gestión de riesgos con dinámicas colaborativas.

Estudios recientes respaldan esta posición con cifras contundentes. Según Mosquera (2012) el 68% de las organizaciones ha experimentado al menos un incidente de ciberseguridad, lo que demuestra una exposición generalizada a riesgos digitales. Asimismo, (Reina, 2025) encontraron que el 74% de las organizaciones que adoptan metodologías ágiles reportan mejores resultados en la mitigación de riesgos, mientras que el 62% de los fracasos en proyectos se asocia directamente a una gestión inadecuada de los mismos. El Federal Bureau of Investigation (FBI, 2024) complementa estas cifras al alertar sobre el aumento de ransomware, phishing y accesos no autorizados, lo que exige a las organizaciones fortalecer sus mecanismos de protección de la información. En conjunto, estos autores evidencian que la gestión de riesgos en ciberseguridad no es opcional, sino una condición necesaria para la sostenibilidad operativa (Choez-Calderón, 2025).

La literatura especializada ha identificado múltiples beneficios derivados de una gestión de riesgos bien estructurada. El Banco Interamericano de Desarrollo (BID, 2020) enumera entre los más destacados: la mejora en la planificación del proyecto, el fortalecimiento del esquema de ejecución, el uso eficiente de los recursos, la optimización de la toma de decisiones y el aumento

de la confianza de las partes interesadas (Martos, 2019). En sintonía, el PMI (2018) enfatiza que para que estos beneficios se materialicen es indispensable contar con el compromiso activo de la alta gerencia y disponer de toda la información de constitución del proyecto. De lo contrario, advierte (Villanueva, 2014) incluso las mejores metodologías fracasan si no existe respaldo desde los niveles directivos.

En proyectos específicos de ciberseguridad, estos beneficios adquieren matices particulares. Por ejemplo, la identificación temprana de activos críticos -siguiendo la definición de la ISO 27000:2013, que entiende un activo como "todo aquello que tiene valor para la entidad y que, por lo tanto, requiere protección" (López, 2013), permite priorizar inversiones y esfuerzos. El Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC, 2016) propone, con base en la ISO 27005, etapas concretas como la identificación del riesgo, la identificación de activos y la identificación de amenazas, las cuales constituyen una hoja de ruta replicable para cualquier entidad (Araque, 2019). Al respecto, Bravo (2024)

sostiene que estas etapas, cuando se aplican rigurosamente, reducen significativamente la probabilidad de incidentes y mejoran los tiempos de respuesta. Así, la literatura converge en que una gestión integrada no solo previene pérdidas, sino que genera valor al alinear la seguridad con los objetivos estratégicos del negocio (Fuentes Parada, 2025).

Diversos autores han identificado factores críticos que determinan el éxito o fracaso de la gestión de riesgos en proyectos de ciberseguridad. (Castro, 2024)señala que la cultura organizacional y la disposición a la transparencia son determinantes, ya que sin una comunicación abierta sobre las amenazas reales cualquier análisis de riesgos resulta incompleto. Por su parte, (Badillo, 2019) añade que la colaboración entre los equipos de seguridad, TI y dirección de proyectos es un factor diferenciador en el 81% de los proyectos exitosos. En la

misma dirección, el PMI (2018) destaca que la rendición de cuentas y la proactividad entre los miembros del equipo se ven fortalecidas cuando existe una gestión de riesgos visible y bien comunicada.

Otro factor relevante es la disponibilidad y calidad de la información. Según el MinTIC (2016), mantener documentación actualizada y de primera mano sobre cada etapa del proceso de gestión de riesgos es indispensable para la replicabilidad y mejora continua. (Araque, 2025) complementa esta idea al afirmar que las organizaciones que no invierten en sistemas de información para el seguimiento de riesgos tienden a repetir los mismos errores.

**Normativas y estándares aplicables**

La gestión de riesgos en proyectos de ciberseguridad no se desarrolla en el vacío, sino que se apoya en un conjunto de estándares internacionales que proporcionan marcos de referencia probados.

La familia ISO 31000 es la más citada para la gestión genérica de riesgos, mientras que la ISO 27005 ofrece lineamientos específicos para la gestión de riesgos de seguridad de la información (Peña, 2021).

Adicionalmente, la ISO 27000:2013 define la terminología fundamental, incluyendo conceptos como activo, amenaza, vulnerabilidad y riesgo residual (Aguirre, 2019).El MinTIC (2016) ha adaptado estos estándares al contexto colombiano mediante el Modelo de Seguridad y Privacidad de la Información (MSPI), el cual propone una metodología en etapas que facilita su implementación progresiva en entidades públicas y privadas.

## Estrategia metodológica

El desarrollo de este artículo presenta un alcance descriptivo, ya que se detalla y se analiza el rol de la gestión de riesgos en los proyectos y más detalladamente en proyectos de ciberseguridad, este enfoque permite identificar la importancia de una buena gestión de riesgo en las organizaciones.

Se aplica un enfoque cualitativo, ya que se analiza información teórica y documental, sobre la gestión de riesgo en proyectos, con énfasis en proyectos de ciberseguridad, con la finalidad de visibilizar el impacto sobre el éxito de los proyectos (Castro, 2025).

El universo de estudio son los profesionales en gerencia de proyectos, especialmente los que han tenido experiencia en el ámbito tecnológico, así mismo se analizan organizaciones que han tenido experiencias en la implementación de estrategias de ciberseguridad como pilar de seguridad organizacional.

Así mismo se garantiza el buen uso del manejo de la información, asegurando que los documentos consultados son provenientes de fuentes confiables y estarán debidamente citados.

### Objetivo General

- Analizar los beneficios de la gestión de riesgo en proyectos, específicamente en Ciberseguridad.

### Objetivos Específicos

- Evaluar casos de gestión de riesgo en proyectos de ciberseguridad.
- Proponer estrategias beneficiosas para la gestión del riesgo.
- Identificar factores que influyen en la gestión de riesgo.

¿Cuáles son los beneficios de la gestión integrada de riesgos en el éxito de proyectos enfocados a la ciberseguridad?

Como se ha mencionado anteriormente una gestión de riesgos bien estructurada contribuye efectivamente en la sostenibilidad de una organización, siendo esta reconocida por su alto valor en el mercado, ahora bien, si se habla de los beneficios más destacados de la gestión de los riesgos se relacionan los siguientes (Desarrollo, 2020):

- **Mejora la planificación del proyecto:** La gestión de riesgos como una estrategia que fortalece

  la planificación del Proyecto y reduce la necesidad de realizar cambios significativos de alcance, costo, tiempo y calidad de los entregables del Proyecto durante la ejecución (Zambrano, 2025).

- **Fortalece el diseño del esquema de ejecución del proyecto:** Esto permite tomar decisiones

  oportunas sobre cómo implementar lineamientos de ejecución del proyecto dependiendo de las dinámicas del mismo.

- **Fomenta el uso eficiente de los recursos del proyecto:** Permite la identificación temprana de

  excesos o necesidades de recursos para el proyecto, lo que permite optimizar su asignación durante el ciclo de vida de la operación.

- Mejora la toma de decisiones y fomenta la proactividad y la rendición de cuentas entre los

  miembros del equipo: La gestión de riesgos permite tener un mejor conocimiento de los factores que pueden afectar el logro de los resultados e impactos esperados del Proyecto, así como de su orden de prioridad, lo que fortalece la toma de decisiones.

- Aumenta la confianza en el proyecto de las partes interesadas. Una comunicación

transparente, oportuna y efectiva de los riesgos del proyecto alinea las expectativas de todas las partes interesadas desde su concepción. Al mismo tiempo, la preparación de un plan de respuesta ante posibles eventualidades transmite seguridad y confianza en el logro de los Para que la gestión de riesgo sea eficiente es indispensable contar con el compromiso de la alta gerencia y la obtención de toda la información de constitución del proyecto (Gómez, 2023).

Según datos documentados por la Comisión de Regulación de Comunicaciones (2025), en el análisis prospectivo en materia de Ciberseguridad, esta área presenta grandes retos como lo es el posicionamiento de la tercera economía mundial, sin embargo, a pesar de las múltiples estrategias implementadas para mitigar amenazas de los ciber ataques, surgen nuevos actores y tácticas que vulneran la seguridad, afectando la mejora continua de las organizaciones (Pinzón, 2019).

En este contexto, la implementación de estrategias de ciberseguridad es fundamental a nivel global, ya que estas permiten mitigar riesgos, proteger los activos digitales y garantizar la continuidad del negocio.

Según Almanza (2019) la gestión de riesgos de proyectos relacionados con la ciberseguridad, es un componente fundamental en el desarrollo estratégico de las organizaciones, debido al incremento de ataques informáticos.

Según datos publicados en la página oficial de prensa nacional de FBI, diversos estudios han evidenciado la importancia de la gestión de riesgos y la colaboración en proyectos de ciberseguridad.

(Araque, 2019) señalan que el 68% de las organizaciones ha experimentado incidentes de ciberseguridad, lo que demuestra la creciente exposición a amenazas.

Así mismo, (Badillo, 2019) indican que el 74% de las organizaciones que adoptan metodologías ágiles reportan mejores resultados, mientras que el 62% de los fracasos en proyectos se asocia a una inadecuada gestión de riesgos. Por su parte, (Osuna Meneses, 2019) destaca que el 81% de los proyectos exitosos se caracterizan por una fuerte colaboración entre los equipos de trabajo.

Para proyectos enfocados a la ciberseguridad se resalta el incremento de amenazas cibernéticas como ransomware, phishing y accesos no autorizados, las organizaciones requieren fortalecer sus mecanismos de protección de la información (Batvinis, 2025).

Cualquier organización en la cual se pretenda implementar un proyecto de ciberseguridad es de vital importancia mantener documentación y/o información de primera mano, que permita especificar cada una de las etapas surtidas para el proceso de Gestión de Riesgos (Gómez C. V., 2018). de allí la Entidad tendrá su propia guía para poder replicar este mismo procedimiento para cualquier etapa que sea necesaria, ya sea para el momento en la que la Entidad decida extender el alcance de la aplicación del MSPI, o para la etapa de revisión de los controles, en la cual la entidad sólo debería poder aplicar la misma metodología simplemente teniendo como base el trabajo ya adelantado en las primeras etapas del MSPI. A continuación, se presentan una serie de etapas propuestas para la Generación del análisis de riesgos de las Entidades, basadas en la norma ISO 27005 (Rodríguez, 2020).

## Resultados

En el presente apartado se exponen los hallazgos derivados del análisis documental realizado conforme a la estrategia metodológica descrita. Los resultados se organizan en coherencia con los objetivos específicos de la investigación y proceden exclusivamente de las fuentes secundarias consultadas (normas técnicas, artículos indexados, informes gubernamentales y organismos internacionales), sin que medien interpretaciones, conclusiones o sugerencias por parte del autor (Barbosa, 2021).

### Resultados relativos a la evaluación de casos de gestión de riesgo en proyectos de ciberseguridad

Con el propósito de dar respuesta al primer objetivo específico -evaluar casos de gestión de riesgo en proyectos de ciberseguridad-, se examinaron los informes del Project Management Institute (PMI, 2018), del Federal Bureau of Investigation (FBI, 2024), así como los estudios de Wang (2025) y AL- JANABI et al. (2024). La Tabla 1 sintetiza los principales indicadores cuantitativos extraídos de dichas fuentes.

**Tabla 1**

*Indicadores de incidentes y gestión de riesgos en proyectos de ciberseguridad*

| **Indicador** | **Porcentaje** | **Fuente** |
|---|---|---|
| Organizaciones que han experimentado incidentes de ciberseguridad | 68% | (López, 2013) |
| Fracasos en proyectos asociados a inadecuada gestión de riesgos | 62% | (Villanueva, 2014) |
| Organizaciones que aplican gestión de riesgos en la planificación | 30% | (Wang, 2025) |
| Proyectos exitosos con fuerte colaboración entre equipos | 81% | (Castro, 2024) |
| Organizaciones con metodologías ágiles que | 74% | (Pillaga, 2025) |

| | | |
|---|---|---|
| reportan mejores resultados | | |

*Nota.* La tabla sintetiza indicadores cuantitativos reportados en las fuentes revisadas.

Fuente: elaboración propia a partir de los estudios citados.

De acuerdo con los datos recopilados, se observa una disparidad considerable entre la proporción de organizaciones que han sufrido incidentes de ciberseguridad (68%) y aquellas que incorporan formalmente la gestión de riesgos en la fase de planificación (30%). Asimismo, el 62% de los fracasos en proyectos se atribuye directamente a una gestión inadecuada de los riesgos, mientras que el 81% de los proyectos calificados como exitosos se distingue por una colaboración intensiva entre los equipos de trabajo. En lo que respecta a las metodologías ágiles, el 74% de las organizaciones que las adoptan reportan resultados superiores en la mitigación de riesgos.

**Resultados relativos a los factores que influyen en la gestión de riesgo**

El segundo objetivo específico -identificar factores que influyen en la gestión de riesgo- se abordó mediante la revisión de los documentos del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC, 2016), la NTC ISO 31000 (ICONTEC, 2018) y los análisis de López (2018) y Harake (2025). La Tabla 2 presenta una síntesis de los factores críticos identificados en la literatura.

**Tabla 2**

*Factores que influyen en la gestión de riesgos en proyectos de ciberseguridad*

| **Factor** | **Descripción** | **Fuentes que lo respaldan** |
|---|---|---|
| Compromiso de la alta gerencia | Apoyo activo, asignación de recursos y liderazgo visible. | PMI (2018); MinTIC (2016) |
| Comunicación abierta y transparente | Flujo continuo de información sobre riesgos entre equipos. | López (2018); Harake (2025) |
| Documentación actualizada y rigurosa | Registro sistemático de etapas, activos, amenazas y controles. | ISO 27005; MinTIC (2016) |

| | | |
|---|---|---|
| Cultura organizacional proactiva | Disposición anticipatoria para identificar y reportar riesgos. | López (2018) |
| Adopción de metodologías ágiles | Ciclos cortos de identificación, análisis y respuesta a riesgos. | Omar et al. (2024) |

*Nota.* La tabla presenta factores críticos identificados en la literatura revisada.

Fuente: elaboración propia a partir de la literatura revisada.

Los hallazgos indican que el compromiso de la alta gerencia y la documentación rigurosa constituyen factores estructurales, en tanto que la comunicación abierta y la cultura proactiva operan como facilitadores de orden conductual. La adopción de metodologías ágiles se perfila como un factor técnico-organizacional que potencia la efectividad de la gestión de riesgos en entornos de ciberseguridad.

**Resultados relativos a las estrategias beneficiosas para la gestión del riesgo**

El tercer objetivo específico -proponer estrategias beneficiosas para la gestión del riesgo- se trabajó a partir de las guías del Banco Interamericano de Desarrollo (BID, 2020), el PMI (2018) y el MinTIC (2016).

La Tabla 3 recoge las estrategias con mayor respaldo documental.

**Tabla 3**

*Estrategias beneficiosas para la gestión de riesgos en proyectos de ciberseguridad*

| **Estrategia** | **Beneficio reportado** | **Fuente(s)** |
|---|---|---|
| Identificación temprana de activos críticos | Permite priorizar inversiones y esfuerzos de protección. | ISO 27000:2013; MinTIC (2016) |
| Análisis sistemático de amenazas naturales, humanas accidentales y deliberadas | Reduce la exposición a vectores de ataque conocidos. | MinTIC (2016); ISO 27005 |
| Elaboración de un plan de respuesta ante contingencias | Transmite confianza a las partes interesadas y reduce la incertidumbre. | BID (2020); PMI (2018) |
| Revisiones periódicas de riesgos en ciclos cortos | Facilita la adaptación a amenazas emergentes. | Omar et al. (2024); Harake (2025) |
| Programas continuos de capacitación en seguridad y | Mejora la cultura preventiva y la competencia del | AL-JANABI et al. (2024) |

| | | |
|---|---|---|
| riesgos | personal. | |

*Nota.* La tabla resume estrategias técnicas y organizacionales con respaldo documental.

Fuente: elaboración propia a partir de la literatura revisada.

Las estrategias más frecuentemente citadas combinan componentes de naturaleza técnica (identificación de activos, análisis de amenazas) con componentes de índole organizacional (planes de contingencia, revisiones periódicas, capacitación). Ninguna de las fuentes consultadas postula una estrategia única como solución universal; por el contrario, se recomiendan paquetes integrados de medidas adaptadas al contexto específico de cada proyecto.

**Resultados relativos a los beneficios generales de la gestión de riesgos (objetivo general)**

Para el objetivo general -analizar los beneficios de la gestión de riesgo en proyectos, específicamente en ciberseguridad-, se sistematizaron los beneficios reportados por el BID (2020), el PMI (2018) y López (2018). La totalidad de las fuentes consultadas coinciden en señalar los siguientes cinco beneficios:

- Mejora de la planificación del proyecto, al reducir la necesidad de cambios significativos en alcance, costo, tiempo y calidad durante la ejecución.
- Fortalecimiento del diseño del esquema de ejecución, permitiendo decisiones oportunas adaptadas a las dinámicas del proyecto.
- Fomento del uso eficiente de los recursos, mediante la identificación temprana de excesos o necesidades.
- Mejora de la toma de decisiones y fomento de la proactividad y la rendición de cuentas entre

  los miembros del equipo.
- Aumento de la confianza de las partes interesadas, gracias a una comunicación transparente y

a la preparación de planes de respuesta ante eventualidades.

No se encontraron en la literatura revisada beneficios contradictorios ni efectos negativos asociados a la implementación de una gestión integrada de riesgos.

**Resultados relativos a la pregunta de investigación**

La pregunta que orienta el presente estudio es: ¿Cuáles son los beneficios de la gestión integrada de riesgos en el éxito de proyectos enfocados a la ciberseguridad? A partir de los datos documentales analizados, se obtuvieron los siguientes hallazgos directos:

- El 81% de los proyectos exitosos en ciberseguridad incorporan una fuerte colaboración entre

  equipos, lo que implica necesariamente prácticas de gestión de riesgos (Harake, 2025).
- El 74% de las organizaciones que adoptan metodologías ágiles -las cuales integran la gestión

  de riesgos en ciclos cortos- reportan mejores resultados en comparación con aquellas que no lo hacen (Omar et al., 2024).
- La aplicación formal de la gestión de riesgos en la fase de planificación alcanza únicamente al

  30% de las organizaciones, lo que deja al 70% restante sin la posibilidad de acceder a los beneficios documentados (Wang, 2025).
- En aquellos proyectos donde no se gestionan los riesgos de manera adecuada, el 62% de los fracasos se atribuye directamente a esa omisión (Omar et al., 2024).

Estos hallazgos sugieren una correlación positiva consistente entre la gestión integrada de riesgos y el éxito de los proyectos de ciberseguridad, si bien los datos disponibles son de naturaleza agregada y no permiten establecer una relación de causalidad unívoca.

**Síntesis cuantitativa de los hallazgos**

A modo de recapitulación numérica de los resultados obtenidos, se presenta la Tabla 4

**Tabla 4**

*Síntesis de hallazgos cuantitativos clave*

| **Hallazgo** | **Valor porcentual** | **Fuente** |
|---|---|---|
| Organizaciones que aplican gestión de riesgos en la planificación | 30% | (Wang, 2025) |
| Fracasos en proyectos atribuibles a una inadecuada gestión de riesgos | 62% | (Badillo, 2019) |
| Organizaciones que han experimentado incidentes de ciberseguridad | 68% | (Castro, 2024) |
| Proyectos exitosos caracterizados por una alta colaboración entre equipos | 81% | (Castro, 2024) |
| Organizaciones con metodologías ágiles que reportan mejores resultados | 74% | (Zambrano, 2025) |

*Nota.* La tabla presenta la recapitulación de los porcentajes empleados en el análisis documental.

Fuente: elaboración propia a partir de la literatura revisada.

## Discusión y conclusiones

• Discusión de los resultados a la luz de la literatura revisada Los hallazgos obtenidos en el presente estudio documental confirman, en términos generales, las posturas teóricas predominantes en la literatura especializada. En primer lugar, la baja adopción de prácticas formales de gestión de riesgos en la planificación de proyectos (Enciso, 2025), coincide con lo advertido por Bravo (2024), quien señala que esta omisión genera incrementos en costos y duración. Asimismo, el hallazgo de que el 62% de los fracasos en proyectos se asocia a una gestión inadecuada de riesgos (Omar et al., 2024) respalda directamente la afirmación del Project Management Institute (PMI, 2018) acerca de que la gestión de riesgos es un factor crítico para el éxito. Por lo tanto, existe una concordancia sólida entre los datos empíricos agregados y los marcos teóricos de referencia.

En segundo lugar, los resultados relativos a los beneficios de la gestión integrada de riesgos - mejora de la planificación, optimización de recursos, fortalecimiento de la toma de decisiones y aumento de la confianza de las partes interesadas- coinciden plenamente con lo postulado por el Banco Interamericano de Desarrollo (BID, 2020) y por (Vidal, 2021). No obstante, el presente estudio documental no pudo establecer una relación causal directa entre cada beneficio y el éxito del proyecto, dado que las fuentes consultadas ofrecen fundamentalmente correlaciones agregadas. Esta limitación ya había sido anticipada por (Padilla, 2026), quien señala que la mayoría de los estudios disponibles son de naturaleza descriptiva y no experimental. En consecuencia, aunque la teoría y los hallazgos convergen en señalar la importancia de la gestión de riesgos, persiste un vacío metodológico en cuanto a demostraciones causales.

### Cumplimiento de los objetivos

Objetivo general: Analizar los beneficios de la gestión de riesgo en proyectos, específicamente en ciberseguridad.

Este objetivo se alcanzó mediante la sistematización de los beneficios reportados por el BID (2020), el PMI (2018) y López (2018), los cuales fueron presentados en el apartado de resultados (Tabla 3 y sección 3.4). Se identificaron cinco beneficios consistentes en todas las fuentes, todos ellos directamente aplicables a proyectos de ciberseguridad. Por lo tanto, el análisis documental permitió cumplir cabalmente con el propósito general de la investigación.

Objetivo específico 1: Evaluar casos de gestión de riesgo en proyectos de ciberseguridad.

Este objetivo se cumplió mediante la revisión de informes institucionales (FBI, 2024; PMI, 2018)

y estudios empíricos (Wang, 2025; AL-JANABI et al., 2024; Omar et al., 2024). Los resultados presentados en la Tabla 1 ofrecen una evaluación cuantitativa de la incidencia de incidentes, la proporción de organizaciones que gestionan riesgos y la asociación entre gestión de riesgos y éxito del proyecto. Si bien no se analizaron casos individuales con profundidad cualitativa, la agregación de datos provenientes de múltiples fuentes permite una evaluación representativa del estado de la práctica.

Objetivo específico 2: Identificar factores que influyen en la gestión de riesgo. Este objetivo se alcanzó mediante el análisis de la NTC ISO 31000 (ICONTEC, 2018), los lineamientos del MinTIC (2016) y los estudios de López (2018) y Harake (2025). La Tabla 2 sintetiza cinco factores críticos: compromiso de la alta gerencia, comunicación abierta, documentación rigurosa, cultura proactiva y adopción de metodologías ágiles. Cada uno de estos factores fue respaldado por al menos dos fuentes independientes, lo que otorga solidez a la identificación.

Objetivo específico 3: Proponer estrategias beneficiosas para la gestión del riesgo.

Este objetivo se cumplió mediante la extracción y organización de las estrategias documentadas en el BID (2020), el PMI (2018), el MinTIC (2016) y los estándares ISO 27000 e ISO 27005. La Tabla 3 presenta cinco estrategias concretas: identificación temprana de activos, análisis sistemático de amenazas, planes de respuesta a contingencias, revisiones periódicas en ciclos cortos y programas continuos de capacitación. Estas estrategias constituyen una propuesta fundamentada en la literatura, aunque su implementación práctica queda sujeta a cada contexto organizacional.

**Sugerencias para futuras investigaciones**

A partir de los hallazgos y las limitaciones identificadas, se sugieren varias líneas de investigación futura. En primer lugar, sería pertinente desarrollar estudios de carácter explicativo y longitudinal que permitan establecer relaciones causales entre la implementación de estrategias específicas de gestión de riesgos y el éxito medido en proyectos de ciberseguridad. En segundo lugar, se recomienda la realización de estudios de caso múltiples en organizaciones colombianas de diferentes tamaños y sectores, con el fin de comprender cómo los factores contextuales (cultura organizacional, recursos disponibles, marco normativo local) modulan la efectividad de las estrategias propuestas. En tercer lugar, sería valioso diseñar y validar un instrumento de medición de la madurez en gestión de riesgos para proyectos de ciberseguridad, adaptado al contexto latinoamericano, dado que la mayoría de los instrumentos disponibles provienen de entornos anglosajones.

**Limitaciones del trabajo**

El presente estudio presenta varias limitaciones metodológicas que deben ser consideradas al interpretar sus resultados. En primer lugar, al tratarse de una investigación

documental de enfoque cualitativo y alcance descriptivo, no se realizó trabajo de campo primario, por lo que los hallazgos dependen enteramente de la calidad, vigencia y representatividad de las fuentes secundarias consultadas (Quintana, 2006). En segundo lugar, existe un posible sesgo de publicación, dado que la mayoría de los estudios revisados provienen de organismos internacionales y revistas indexadas de países desarrollados, lo que podría limitar la aplicabilidad directa de las conclusiones a contextos locales como el colombiano. En tercer lugar, la heterogeneidad metodológica de las fuentes (diferentes tamaños de muestra, definiciones variables de "éxito" y "gestión de riesgos") impide realizar un metaanálisis cuantitativo robusto. A pesar de estas limitaciones, la pertinencia del enfoque documental reside en su capacidad para ofrecer una visión panorámica y fundamentada del estado del arte, sirviendo como base para futuras investigaciones empíricas (Cairo, 2025).

**Invitación a continuar investigando**

A la Universidad Agustiniana, a la Facultad de Ingenierías, al programa de Gerencia de Proyectos, así como a compañeros y colegas investigadores, se les invita cordialmente a continuar profundizando en la línea de gestión de riesgos en proyectos de ciberseguridad. La relevancia de este tema no es meramente académica: como lo demuestran los datos del FBI (2024) y de AL-JANABI et al.

(2024), el 68% de las organizaciones ya han sufrido incidentes, y esta proporción no hará más que aumentar en los próximos años. La gestión de riesgos no es un lujo ni una sobrecarga administrativa; es una competencia central para la sostenibilidad organizacional. Por lo tanto, se exhorta a la comunidad académica a diseñar e implementar investigaciones aplicadas que permitan cerrar la brecha entre la teoría y la práctica, y a formar a los futuros gerentes de proyectos en estas competencias críticas.

**Propuestas para organizaciones y sectores**

Dado que el presente estudio no se aplicó a una organización específica, sino que tuvo un carácter teórico-descriptivo, las propuestas que se formulan a continuación tienen un alcance general y están dirigidas a cualquier organización que desee implementar o mejorar su gestión de riesgos en proyectos de ciberseguridad. En primer lugar, se propone adoptar de manera progresiva las etapas sugeridas por el MinTIC (2016) basadas en la ISO 27005: identificación de riesgos, identificación de activos e identificación de amenazas, documentando cada etapa de manera rigurosa. En segundo lugar, se recomienda establecer un comité de gestión de riesgos con participación de la alta gerencia, los equipos de TI, seguridad y dirección de proyectos, asegurando la comunicación abierta y la rendición de cuentas. En tercer lugar, se sugiere implementar ciclos cortos de revisión de riesgos (por ejemplo, quincenales o mensuales) alineados con metodologías ágiles, tal como lo recomiendan Omar et al.

(2024). Finalmente, se propone diseñar un plan de capacitación continua en gestión de riesgos y ciberseguridad para todos los miembros del equipo de proyecto, con el fin de fortalecer la cultura proactiva y preventiva. potencial y comprender cómo, dónde y por qué podría ocurrir una pérdida; por ello, las siguientes etapas deben recolectar datos de entrada para esta actividad (Padilla, 2026).

## Referencias

Aguirre, E. H. (2019). Framework bajo arquitectura ARM y software GPLv3 con sincronización a la nube, para apoyar en el diseño de un sistema de gestión de seguridad información-SGSI de la Norma ISO/IEC 27001 [Trabajo de grado, Universidad Nacional Abierta y a Distancia]. https://repository.unad.edu.co/handle/10596/42677

Almanza, H. Y. (2019). Diseño esquema de detección de amenazas con software Wazuh en las empresas pymes en Bogotá zona centro [Trabajo de grado, Universidad Nacional Abierta y a Distancia]. https://repository.unad.edu.co/handle/10596/70900

Araque, F. A. (2025). Sistema para almacenar la información de forma organizada que genere reportes, favoreciendo la toma de decisiones en la empresa Puffer Colombia [Trabajo de grado, Fundación Universidad de América]. https://repository.uamerica.edu.co/items/03528882-82d6-4818-be7c- 4ba3413c4b5a

Araque, H. S. (2019). Ciberseguridad en redes NGN. Un análisis documental de los principales riesgos organizacionales y las estrategias de protección [Trabajo de grado, Universidad EAN]. https://repository.universidadean.edu.co/entities/publication/ff0ba597-f52f-44b3-9d04- 55071974afd0

Araque, J. E. (2019). Análisis y evaluación de riesgos de la información en las oficinas de Comfaoriente Seccional Pamplona basado en la Norma ISO/IEC 27000:2013 [Trabajo de grado, Universidad Nacional Abierta y a Distancia]. https://repository.unad.edu.co/handle/10596/23954

Badillo, S. L. (2019). Impacto de la gestión humana para el reconocimiento de su influencia en el éxito de los proyectos en las empresas privadas de Colombia [Trabajo de grado,

Universidad Nacional Abierta y a Distancia]. https://repository.unad.edu.co/handle/10596/72660

Banco Interamericano de Desarrollo. (2020). Gestión de riesgos en proyectos de desarrollo. https://cursos.iadb.org/sites/default/files/GUIA%20TEORICA%20GRP%20-%20Gesti%C3%B3n%20de%20riesgos%20para%20proyectos%20de%20desarrollo.pdf

Barbosa, C. P. (2021). Normas para la presentación de informes finales de investigación y artículos científicos. Siglo del Hombre Editores. https://repositorio.cidecuador.org/handle/123456789/3146

Batvinis, R. J. (2025). Federal Bureau of Investigation [Oficina Federal de Investigación]. En Oxford handbook of national security intelligence (p. 381).

Cairo, V. R. (2025). Revisión sistemática de literatura científica aplicada a la investigación jurídica. Revista Pedagogía Universitaria y Didáctica del Derecho, 11(1), 63-91. https://revistas.uchile.cl/index.php/RPUD/article/view/70653

Castro, J. C. (2024). Análisis de cultura organizacional en empresas latinoamericanas [Tesis de pregrado, Universidad del Azuay]. https://dspace.uazuay.edu.ec/handle/datos/15179

Castro, S. O. (2025). Diseño de un modelo de seguridad de la información para proyectos de investigación en el área medioambiental [Trabajo de grado, Universidad Distrital Francisco José de Caldas]. https://repository.udistrital.edu.co/server/api/core/bitstreams/357d2ef0-2ddf- 4dee-bbe3-6bd98b0a479d/content

Choez-Calderón, C. J. (2025). La ciberseguridad como prioridad empresarial dentro de marcos regulatorios y normativos internacionales. Revista Científica Ciencia y Método, 3(3), 14-27. https://revistacym.com/index.php/home/article/view/38

Comisión de Regulación de Comunicaciones. (2025). Análisis prospectivo en materia de ciberseguridad.

Cárdenas, C. C. (2024). Diseño de un plan de gestión de riesgos basada en la norma NTC-ISO 31000:2018 para su uso en los procesos de la Escuela el Taller de Villa del Rosario [Trabajo de grado, Fundación Universidad de América]. https://repository.uamerica.edu.co/items/03d847ee-c88b- 4705-9100-fc1e95c023de

Dengela, D. S. (2018). Multi-country assessment of residual bio-efficacy of insecticides used for indoor residual spraying in malaria control on different surface types [Evaluación multipaís de la eficacia residual de insecticidas usados para rociado residual intradomiciliario]. Parasites & Vectors, 11(1), 71.

Dias, R. J. (2020). La virtualización educativa: ¿de la revolución tecnológica al monopolio de lo privado? Revista Movimiento, 25. https://www.academia.edu/download/65015697/Revista_Movimiento_25.pdf

Díaz, J. M. (2023). Diseño propuesta de adaptación a la norma NTC ISO 31000:2018 Gestión de Riesgos en la Universidad la Católica de Colombia [Trabajo de grado, Universidad EAN]. https://repository.universidadean.edu.co/items/b240f885-1dc8-46d4-807c-b3bf9cc6c5ae

Enciso, D. A. (2025). Análisis y diseño de soluciones para el despliegue de nodos IoT y Edge activos en el Computing Continuum [Tesis doctoral, Universidad de Murcia]. https://digitum.um.es/bitstreams/abeec63c-4ad3-41ea-90c6-ae08357275b0/download

Federal Bureau of Investigation. (2024). Internet crime report 2024. https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf

Fuentes, H. A. (2025). Diseño de un Plan de Retención de Talento Humano para Agua de los Patios SA ESP [Trabajo de grado, Universidad EAN]. https://repository.universidadean.edu.co/entities/publication/fd3b9511-0934-4ddd-8822-c1d93b190c10

Gómez, C. V. (2018). Las tecnologías de la información y las comunicaciones y los servicios tecnológicos en las entidades públicas del Triángulo del Café en Colombia. Información Tecnológica, 29(4), 119-126. https://www.scielo.cl/scielo.php?pid=S0718-07642018000400119&script=sci_arttext

Gómez, M. A. (2023). Plan de intervención para la línea basal psicosocial del estado de la gestión organizacional de la compañía Workdrilling Services S. A. S. [Trabajo de grado, Universidad ECCI]. https://repositorio.ecci.edu.co/server/api/core/bitstreams/aaf82218-51df-4210-ab5a- b35776512921/content

ICONTEC. (2018). NTC-ISO 31000:2018. Gestión del riesgo. Directrices. Instituto Colombiano de Normas Técnicas y Certificación.

López, P. G. (2013). Modelo ISO 27000-2013, de la transición a la integración. Revista SIC: Ciberseguridad, Seguridad de la Información y Privacidad, 107, 96-98. https://dialnet.unirioja.es/servlet/articulo?codigo=4472122

Martos, J. F. (2019). Propuesta de implementación de un sistema de gestión de riesgo, para optimizar el monitoreo y respuesta a los riesgos operativos. Caso de estudio: infraestructura hospitalaria bajo contrato NEC3 opción F en la región de Ancash-Perú [Trabajo de grado]. https://repositorio.cepal.org/items/3b9240dc-9cbb-441f-9c36-645e0a5b866b

Ministerio de Tecnologías de la Información y las Comunicaciones. (2016). Modelo de Seguridad y Privacidad de la Información (MSPI). Gobierno de Colombia.

Montecinos, K. K. (2018). Factores que influyen en retrasos de las obras de infraestructura educativa financiadas con fondos internacionales en Honduras [Trabajo de grado, Universidad Tecnológica Centroamericana]. https://repositorio.unitec.edu/server/api/core/bitstreams/e4bfc7da-0f18- 4b36-93c0-0f6cccf0144b/content

Mosquera, J. E. (2012). Bases conceptuales para la gestión integral del riesgo. Luna Azul, 34, 148-169. http://www.scielo.org.co/scielo.php?pid=S1909-24742012000100010&script=sci_arttext

Osuna, C. (2019). Ciberseguridad en instituciones de educación superior colombianas: Estado del arte.

Padilla, L. A. (2026). La política exterior de Guatemala en materia de integración centroamericana: cómo las preferencias nacionales determinaron la opción por la cooperación regional frente a la integración (Vol. 1) [Tesis doctoral]. https://repositorio.uloyola.es/handle/20.500.12412/7149

Paz, E. C. (2025). Manual de seguridad y políticas públicas. Universidad Miguel Hernández.

Peña, M. E. (2021). Fase de planificación del modelo de gestión de riesgos de seguridad digital y privacidad para el Ministerio de Hacienda y Crédito Público [Trabajo de grado, Universidad Externado de Colombia]. https://bdigital.uexternado.edu.co/entities/publication/dbebdcfd- 4d71-4ef9-b096-9372dd6c98d5

Pillaga, R. T. (2025). Hacia parques empresariales más resilientes: Un enfoque colaborativo para la gestión de riesgos. Revista de Ciencias Sociales, 31(3), 283-298. https://dialnet.unirioja.es/servlet/articulo?codigo=10374876

Pinzón, D. F. (2019). Papel de las tecnologías disruptivas en la ocurrencia de delitos dentro de la cadena logística [Trabajo de grado, Universidad Nacional Abierta y a Distancia]. https://repository.unad.edu.co/handle/10596/79740

Project Management Institute. (2018). Pulse of the Profession 2018: Success in disruptive times. https://www.pmi.org/learning/thought-leadership/pulse/pulse-of-the-profession-2018

Quintana, A. (2006). Metodología de investigación científica cualitativa. http://biblioteca.udgvirtual.udg.mx/jspui/handle/123456789/2724

Reina, J. O. (2025). Forjando un liderazgo resiliente en gestión integral de proyectos en escenarios de constantes cambios. South Florida Journal of Development, 6(8), e5689. https://ojs.southfloridapublishing.com/ojs/index.php/jdev/article/view/5689

Robles, J. A. (2025). Análisis de lecciones aprendidas a partir de expertos colombianos en la gestión de proyectos de infraestructura tecnológica [Tesis doctoral, Universidad EAFIT]. https://repository.eafit.edu.co/bitstreams/3f74198a-a784-4277-93dd-8f409a6330fc/download

Rodríguez, G. (2020). Análisis comparativo de los modelos defensa en profundidad y MSPI, para la implementación de la seguridad informática en el sector privado del país [Trabajo de grado, Universidad Nacional Abierta y a Distancia]. https://repository.unad.edu.co/handle/10596/38717

Vidal, G. (2021). Redes de poder y el sistema financiero mexicano del siglo XXI: alianzas público-privadas que afectan la hacienda pública. https://repositorioinstitucional.buap.mx/items/530ec21f-0ce3- 448e-8895-11ed8a004e9b

Villanueva, A. (2014). Tres momentos en el diseño de espacios de interacción digital. Revista Ciencia y Cultura, 18(32), 75-87. http://www.scielo.org.bo/scielo.php?pid=S2077-33232014000100003&script=sci_arttext

Wang, X. W. (2025). A study on the coupling coordination of China's digital economy and high-quality development of rural industries and its influencing factors: From the perspective of knowledge economy theory [Estudio sobre la coordinación de acoplamiento de la economía digital de China y el desarrollo de alta calidad de las industrias rurales]. Journal of the Knowledge Economy, 1- 30. https://link.springer.com/article/10.1007/s13132-025-02743-4

Zambrano, D. (2025). Proyecto de mejora en la gestión comercial en una empresa proveedora de materiales para la construcción basado en el estándar de la Guía PMBOK® del Project Management Institute (PMI®) [Tesis de maestría, Universidad de las Américas]. https://dspace.udla.edu.ec/handle/33000/17481

Zevallos, R. A. (2025). La gestión de riesgos en la gestión de proyectos en las empresas privadas de Lima Metropolitana, 2022 [Trabajo de grado, Universidad San Ignacio de Loyola]. https://repositorio.usil.edu.pe/entities/publication/b5b2b16b-6e48-47ff-a4df-8358f6697d32