FIPCAEC (Edición 39) Vol. 8, No 4
Octubre-Diciembre 2023, pp. 135-157

ISSN: 2588-090X

DOI: https://doi.org/ 10.23857/fipcaec.v8i4.912

Avances en la gestión de riesgos: modelo ISO 31000 y enfoques actuales

Advances in risk management: ISO 31000 model and current approaches

Avanços na gestão de riscos: modelo ISO 31000 e abordagens atuais

Alba Isabel Maldonado-Núñez [I]
alba.maldonado@espoch.edu.ec
https://orcid.org/0000-0001-8673-0319

Gilma Gabriela Uquillas-Granizo [II]
gilma.uquillas@unach.edu.ec
https://orcid.org/0000-0002-5367-3431

Cintya Lisbeth Tello-Núñez [III]
cintya.tello@unach.edu.ec
https://orcid.org/0009-0008-8045-6273

Correspondencia: alba.maldonado@espoch.edu.ec

* **Recepción:** 30/09/2023 * **Aceptación:** 03/10/2023 *Publicación: 26/10/2023

1. Máster Universitario en Dirección y Asesoramiento Financiero, Ingeniera en Contabilidad y Auditoría CPA, Docente, Escuela Superior Politécnica de Chimborazo, Riobamba, Ecuador.
2. MBA Magister en Administración de Empresas con Mención en Gerencia de la Calidad y Productividad, Ingeniera de Empresas. Docente, Universidad Nacional de Chimborazo, Riobamba, Ecuador.
3. Máster en Contabilidad y Auditoría, Ingeniera en Contabilidad y Auditoría CPA, Docente, Universidad Nacional de Chimborazo, Riobamba, Ecuador.

Resumen

En un entorno empresarial dinámico y competitivo, la gestión efectiva de riesgos se ha convertido en una herramienta fundamental para garantizar la resiliencia y el éxito a largo plazo. La importancia de la gestión de riesgos radica en su capacidad para ayudar a las empresas u organizaciones a anticipar y prepararse para desafíos inesperados, minimizando pérdidas financieras, reputacionales, y facilitando la toma de decisiones más informadas. Esta investigación tiene el objetivo de describir la metodología ISO 31000 para la gestión de riesgos, además de identificar diversas propuestas metodológicas que pueden aplicarse en esta problemática. La investigación es de tipo documental, con un enfoque cualitativo. En los resultados se destaca que las metodologías de gestión de riesgos analizadas ofrecen diversos enfoques para abordar desafíos en identificación, evaluación y mitigación de riesgos. Destacan la importancia de un enfoque continuo y cíclico, incorporando la gestión de riesgos en la operación cotidiana. Identificación y evaluación de riesgos son pasos clave en todas las metodologías, ya sea en ámbitos estratégicos, operativos o de seguridad de la información. Planificar respuestas a riesgos es fundamental, incluyendo mitigación, aceptación, transferencia o eliminación. La comunicación y consulta con partes interesadas internas y externas son esenciales. En última instancia, estas metodologías ayudan a minimizar la incertidumbre y tomar decisiones informadas en diferentes contextos, garantizando la continuidad operativa.

Palabras Claves: Principios; Toma de decisiones; Mitigación de riesgos; Procesos; Control.

Abstract

In a dynamic and competitive business environment, effective risk management has become a critical tool to ensure long-term resilience and success. The importance of risk management lies in its ability to help companies or organizations anticipate and prepare for unexpected challenges, minimizing financial and reputational losses, and facilitating more informed decision-making. This research aims to describe the ISO 31000 methodology for risk management, in addition to identifying various methodological proposals that can be applied to this problem. The research is documentary type, with a qualitative approach. The results highlight that the risk management methodologies analyzed offer diverse approaches to address challenges in risk identification, evaluation and mitigation. They highlight the importance of a continuous and cyclical approach,

incorporating risk management into daily operations. Risk identification and evaluation are key steps in all methodologies, whether in strategic, operational or information security areas. Planning responses to risks is essential, including mitigation, acceptance, transfer or elimination. Communication and consultation with internal and external stakeholders are essential. Ultimately, these methodologies help minimize uncertainty and make informed decisions in different contexts, ensuring operational continuity.

Key Words: Beginning; Decision making; Risk mitigation; Processes; Control.

Resumo

Num ambiente empresarial dinâmico e competitivo, a gestão eficaz dos riscos tornou-se uma ferramenta crítica para garantir a resiliência e o sucesso a longo prazo. A importância da gestão de risco reside na sua capacidade de ajudar as empresas ou organizações a antecipar e preparar-se para desafios inesperados, minimizando perdas financeiras e reputacionais e facilitando uma tomada de decisão mais informada. Esta pesquisa tem como objetivo descrever a metodologia ISO 31000 para gerenciamento de riscos, além de identificar diversas propostas metodológicas que podem ser aplicadas a este problema. A pesquisa é do tipo documental, com abordagem qualitativa. Os resultados destacam que as metodologias de gestão de riscos analisadas oferecem diversas abordagens para enfrentar os desafios na identificação, avaliação e mitigação de riscos. Destacam a importância de uma abordagem contínua e cíclica, incorporando a gestão de risco nas operações diárias. A identificação e avaliação de riscos são etapas fundamentais em todas as metodologias, seja nas áreas estratégica, operacional ou de segurança da informação. Planejar respostas aos riscos é essencial, incluindo mitigação, aceitação, transferência ou eliminação. A comunicação e a consulta com as partes interessadas internas e externas são essenciais. Em última análise, estas metodologias ajudam a minimizar a incerteza e a tomar decisões informadas em diferentes contextos, garantindo a continuidade operacional.

Palavras-chave: Começo; Tomando uma decisão; Mitigação de riscos; Processos; Ao controle.

Introducción

En la actualidad, se han presenciado cambios sustanciales en el funcionamiento de la economía global, como lo refleja la recesión mundial que impacta a las naciones latinoamericanas. Estos cambios están generando transformaciones significativas en la actividad empresarial. En este dinámico entorno, se vuelve imperativo contar con una gestión de riesgos eficaz que facilite la toma de decisiones en aspectos cruciales como políticas, costos de producción, ganancias, solvencia, flujo de efectivo, financiamiento y, en términos generales, en todas las decisiones relacionadas con la dirección estratégica y la gestión de la organización. (Valencia & Narváez, 2021). El riesgo es inherente a todas las actividades económicas y debe ser parte integral de la estrategia y la toma de decisiones de una entidad, proporcionando información valiosa sobre los resultados de las decisiones.

Las organizaciones enfrentan incertidumbres diarias que, si no se manejan adecuadamente, pueden afectar sus procesos y la toma de decisiones. Aunque la gestión de riesgos no es un concepto nuevo, su complejidad ha evolucionado con el tiempo, y diversas directrices, regulaciones y recomendaciones de importantes instituciones empresariales exigen a los gerentes y líderes que ajusten sus prácticas de gestión para abordar de manera explícita los riesgos. La gestión de riesgos ofrece múltiples beneficios, como alinear el riesgo con la estrategia empresarial, reducir sorpresas operativas y pérdidas, mejorar la toma de decisiones en respuesta a riesgos, optimizar el uso de recursos, identificar y abordar riesgos interconectados en toda la empresa, vincular el crecimiento y el rendimiento con el riesgo de manera efectiva, racionalizar el capital y aprovechar oportunidades proactivamente. En general, la administración de riesgos mejora el funcionamiento del negocio, aumenta la eficacia organizacional y facilita una presentación más sólida de los riesgos (Vera & Pilco, 2008).

En la época actual de la información, la cantidad de datos producidos y guardados ha aumentado de manera exponencial, en el ámbito empresarial son fundamentales para obtener información valiosa, para la toma de decisiones informadas y adquirir conocimientos significativos (Espinoza et al., 2023). Marchesano y Scavone (2020) destacan que, para lograr informes comprensibles y útiles, es esencial contar con datos suficientes que provengan de una base de datos organizada y que permitan análisis y comparaciones. Esto se logra a través de un sistema que brinde información completa, confiable y oportuna para monitorear la exposición al riesgo y tomar decisiones

efectivas. Una gestión deficiente o la falta de gestión de riesgos conlleva problemas como: una definición imprecisa del alcance del proyecto, una planificación inadecuada de actividades y tareas, carencia de habilidades para la gestión, una perspectiva de negocio limitada, inversiones inciertas, la interrupción no planificada de trabajos, rendimientos bajos en los negocios, escasa estabilidad, escasa optimización de procesos organizacionales, un bajo nivel de integración, un uso limitado de sistemas de información, una planificación estratégica insuficiente y una capacitación inadecuada del personal (Muñoz & Cuadros, 2017).

Ciertos aspectos que pueden influenciar en la problemática actual en la gestión de riesgos de las empresas, se encuentra la escasez de información y un amplio desconocimiento de las técnicas asociadas, la falta de actualización en los planes de prevención de riesgos, programas de seguridad y protección establecidos por las organizaciones, la falta de comprensión por parte de los líderes, tanto superiores como intermedios, así como de los trabajadores, acerca de sus roles y responsabilidades en la gestión integral de riesgos, que muchas veces no se aborda como un elemento central en los procesos de gestión colaborativa (Cruz & Morejón, 2019). La gestión de riesgos tiende a ser fragmentada y carece de un enfoque integral y de una perspectiva socialmente responsable, centrándose principalmente en normativas aisladas relacionadas con la protección laboral.

La gestión de riesgos es esencial en cualquier modelo de gestión empresarial, sin importar el tamaño o la naturaleza de la organización, porque todas las empresas operan en entornos cambiantes. Los analistas de riesgos deben identificar y comprender las incertidumbres y determinar la magnitud de los riesgos en diferentes aspectos. Las empresas a nivel global, al identificar incertidumbres en sus procesos, pueden agregar valor a sus servicios, lo que les permite mantener su sostenibilidad. La evaluación de riesgos en las empresas abarca diversos ámbitos, como el normativo, administrativo, archivístico, tecnológico y organizacional (Bodero et al., 2022a). Gestionar estas incertidumbres implica crear posibles escenarios de riesgo. La valoración de la gestión de riesgos se basa principalmente en las variables de reacción y probabilidad de impacto (Bodero et al., 2022b). Las tradicionales metodologías de gestión, como la administración clásica, científica, de calidad y estratégica, por sí solas, ya no son adecuadas para enfrentar las nuevas demandas de un entorno empresarial dinámico y lleno de incertidumbre. Por lo tanto,

muchas empresas están adoptando la gestión de riesgos como un nuevo enfoque administrativo, lo que se refleja en la creación de roles como el director de riesgos (Martínez & Blanco, 2017).

Contar con un modelo que posibilite la Gestión de Riesgos puede anticipar una perspectiva significativa en la gestión de proyectos, estar preparados de manera proactiva para afrontar las posibles amenazas que puedan influir en el resultado final de los proyectos es esencial para cualquier empresa u organización (Rodas, 2017). Por lo tanto, identificar y examinar las metodologías actuales que se utilizan para la gestión de riesgos se vuelve de vital importancia. Esto permite a las organizaciones identificar y aplicar las mejores prácticas disponibles, adaptando su enfoque a las particularidades de su contexto y, al mismo tiempo, asegurando una gestión de riesgos efectiva y precisa que contribuya al éxito de sus proyectos y al resguardo de los intereses de la empresa y los clientes. Esta investigación tiene el objetivo de describir la metodología ISO 31000 para la gestión de riesgos, además de identificar diversas propuestas metodológicas que pueden aplicarse en esta problemática.

Metodología

La investigación de tipo documental, porque se basa en la revisión y análisis exhaustivo de documentos científicos, fuentes bibliográficas y literatura existente sobre la gestión de riesgos. La metodología se centra en la recopilación, síntesis y análisis de información ya publicada y documentada en diversas fuentes, con el objetivo de obtener una comprensión profunda del tema de la gestión de riesgos y de las metodologías utilizadas en este campo. En esta modalidad de investigación, se utiliza un enfoque cualitativo, que se caracteriza por su énfasis en comprender y analizar fenómenos, en este caso, relacionados con la gestión de riesgos, a través de la revisión y análisis de documentos científicos y fuentes bibliográficas. La investigación comienza formulando preguntas clave, y a partir de ahí, se procede con una exhaustiva revisión bibliográfica y análisis documental para identificar aspectos relevantes vinculados a los riesgos, como los tipos de riesgos y los principios asociados. Además, se exploran las metodologías utilizadas en la gestión de riesgos en diversos ámbitos, tales como empresarial, gubernamental o seguridad de la información. En particular, se destaca la norma ISO 31000 como una de las metodologías más ampliamente adoptada, se presentan y describen en detalle sus principales procesos. También se exponen diversas metodologías propuestas por diferentes autores, junto con sus respectivos procesos, con

el objetivo de proporcionar una visión completa y actualizada sobre la gestión de riesgos en diferentes contextos.

La combinación de este enfoque cualitativo con una revisión detallada y un análisis crítico de la literatura existente en el campo de la gestión de riesgos proporciona una visión integral y actualizada que resulta valiosa tanto para la comunidad científica como para profesionales en búsqueda de una comprensión profunda y actualizada de este tema crucial en la gestión organizacional.

Resultados

La gestión de riesgos desempeña un papel fundamental en la toma de decisiones estratégicas y operativas en todos los ámbitos de la vida, ya sea en el mundo de los negocios, la administración pública, la inversión financiera o incluso en nuestras actividades cotidianas. La habilidad para identificar, evaluar y mitigar riesgos es crucial para alcanzar objetivos y salvaguardar intereses. En este contexto, resulta esencial comprender los diversos tipos de riesgos a los que nos enfrentamos. Por medio de la revisión bibliográfica realizada se presentan los principales tipos de riesgos que pueden afectar a organizaciones y empresas, destacando su importancia y cómo la gestión de riesgos adecuada puede marcar la diferencia entre el éxito y el fracaso.

Riesgo estratégico: Los riesgos estratégicos son aquellos que están vinculados a factores que pueden impactar significativamente la dirección y el éxito a largo plazo de una organización. Estos riesgos se relacionan con las preferencias cambiantes de los clientes, la evolución de la tecnología y las barreras normativas o políticas que pueden afectar el entorno empresarial (Palacio-Fierro et al., 2016). Se centran en la adaptación a las necesidades cambiantes de los clientes, la capacidad de mantenerse a la vanguardia en términos tecnológicos y la capacidad de enfrentar desafíos regulatorios o políticos que podrían influir en la estrategia y la viabilidad a largo plazo de la empresa. Estos riesgos requieren una gestión proactiva y una comprensión profunda de los factores externos que pueden moldear la dirección de la organización.

Riesgo operativo: El riesgo operativo se refiere a las posibles pérdidas que una empresa puede enfrentar debido a una amplia gama de eventos, ya sean internos o externos. Palma (2011) expresa que el riesgo operativo se divide en cuatro categorías principales: personas, relacionado con

pérdidas por errores humanos y problemas interpersonales; procesos internos, que abarca la posibilidad de pérdidas debido a fallas en procesos y políticas; tecnología de información, que involucra pérdidas por fallos tecnológicos; y eventos externos, que incluyen pérdidas debido a factores fuera del control de la empresa, como desastres naturales o cambios en leyes y regulaciones. También se incluyen riesgos asociados con la negligencia, el fraude, los problemas tecnológicos y otros factores que pueden afectar negativamente las operaciones y los resultados de una organización.

Riesgo financiero: El riesgo financiero abarca diversas categorías, incluyendo el riesgo de mercado, crédito, operacional, legal y de liquidez. El riesgo de mercado se relaciona con factores externos, como precios, costos y variables macroeconómicas, mientras que el riesgo de crédito es importante para las empresas no financieras debido a su impacto en la estabilidad financiera y la continuidad de las operaciones. El riesgo operacional comprende una amplia gama de eventos relacionados con la ejecución de procesos empresariales, como fraudes, fallos informáticos y errores de gestión, incluyendo el riesgo de modelo (Rodríguez et al., 2013). Además, se deben considerar los riesgos competitivos, que se asocian con amenazas estratégicas, como la competencia de nuevos rivales o productos alternativos, así como el deterioro de activos intangibles clave para la competitividad de la empresa, como su reputación y lealtad de empleados y clientes.

Riesgos de tecnología: La gestión de riesgos informáticos y tecnológicos se refiere a la práctica de identificar, evaluar y mitigar los riesgos asociados con el uso de tecnología de la información y sistemas informáticos, con el objetivo de proteger la seguridad, confidencialidad e integridad de los datos, así como garantizar la continuidad del acceso a la información. En la actualidad, el crecimiento de sistemas informáticos se ha convertido en un pilar del avance tecnológico. Los usuarios confían sus datos personales y financieros a diversas plataformas en línea. Por lo tanto, la seguridad de la información en internet es de vital importancia (Espinoza et al., 2022). Esto implica la identificación de amenazas, evaluación de su probabilidad e impacto, implementación de controles de seguridad, desarrollo de planes de respuesta a incidentes y la planificación de la continuidad del negocio, con el fin de minimizar los posibles daños y asegurar un funcionamiento eficiente en el entorno tecnológico ((Arévalo et al., 2017). Para garantizar el cumplimiento de las dimensiones fundamentales de seguridad de la información, como la confidencialidad, integridad y disponibilidad, es crucial implementar metodologías integradas de gestión de riesgos.

Principios de la gestión de riesgo

1. Crear valor: Contribuye a la creación y preservación del valor empresarial, mejorando el rendimiento a través de la revisión de procesos y la gestión efectiva para el logro de objetivos.

2. Se integra a los procesos de la organización, formando parte integral de la planificación tanto operativa como estratégica.

3. Se integra en la toma de decisiones, al proporcionar información oportuna para identificar prioridades y acciones adecuadas.

4. Es explícito frente a la incertidumbre, identificando riesgos para aumentar ganancias y reducir pérdidas.

5. Se aplica sistemáticamente y estructuradamente, garantizando eficiencia, consistencia y confiabilidad en los resultados.

6. Se basa en la mejor información disponible, considerando toda la información relevante y reconociendo sus limitaciones.

7. Es adaptable a recursos humanos, financieros y temporales, así como al entorno interno y externo de la organización.

8. Integra factores humanos y culturales, reconociendo su influencia en el logro de los objetivos.

9. Es transparente e inclusivo, involucrando a stakeholders y promoviendo la comunicación y consulta en la gestión del riesgo.

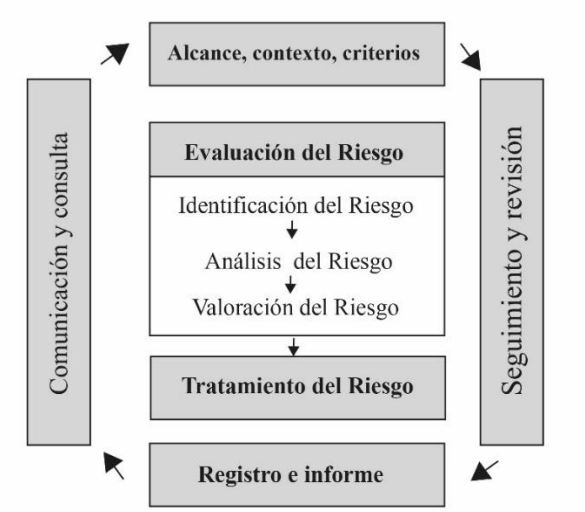
10. Es dinámico, repetitivo y sensible a los cambios en el entorno empresarial, adaptándose a la evolución de los riesgos.

11. Facilita la mejora continua de las organizaciones, impulsando inversiones a largo plazo en su gestión de riesgos.

Según la revisión bibliográfica realizada la metodología más utilizada y referente en materia de gestión de riesgos son las normas ISO 31000. La norma ISO 31000 es una herramienta ampliamente reconocida a nivel internacional para la gestión de riesgos. Se considera como la base en la que se apoyan todos los sistemas de gestión cuando se trata de incorporar riesgos y oportunidades como elementos esenciales. Esta norma actúa como un instrumento que promueve la adquisición de ventajas competitivas para cualquier organización que la implementa (Contreras, 2020).

Además, ofrece las instrucciones esenciales para llevar a cabo una gestión de riesgos efectiva. En este sentido, indican que el marco de trabajo de la gestión de riesgos es un conjunto de componentes que establecen los principios y las pautas que la organización necesita para desarrollar, implementar, supervisar, revisar y mejorar constantemente su gestión de riesgos (Soler et al., 2020). La norma es completa y se puede utilizar en una amplia gama de industrias y para todo tipo de riesgos, ofreciendo un respaldo más efectivo a las organizaciones en la gestión constante de los riesgos a los que se enfrentan (Díaz, 2017). Esta norma destaca que las organizaciones operan en un entorno incierto y, en ocasiones, deben gestionar los riesgos de manera preventiva. Para lograr esto, es esencial implementar un sistema de gestión que garantice una gestión adecuada de los riesgos, lo que mejora la capacidad de la organización para identificar amenazas y oportunidades. De esta manera, se incrementa la probabilidad de alcanzar los objetivos organizacionales. La norma ISO 31000 proporciona orientación y elementos de apoyo para la gestión de riesgos. Esto se logra mediante la identificación sistemática de riesgos, facilitando el análisis, la evaluación y la definición de estrategias para abordarlos (Díaz, 2017).

Lizararzaburu et al. (2017) enfatiza que es esencial aplicar esta normativa considerando la dirección general de la empresa, la administración de la organización, la circulación de información y las políticas internas de la asociación. La gestión de riesgos se posiciona como un elemento fundamental en las empresas, que no solo influye en el avance de los procedimientos y la detección de amenazas, sino también en su influencia en la gestión de la excelencia en la calidad. En la Figura 1 se presenta el proceso para la gestión de riesgos que establece la norma ISO 31000.



FIPCAEC (Edición. 39) Vol. 8, No 4, Octubre-Diciembre 2023, pp. 135-157, ISSN: 2588-090X

Figura 1. Proceso Gestión del Riesgo Norma ISO 31000

Fuente: International Organization for Standardization (ISO,2018).

Comunicación y consulta: La comunicación y la consulta desempeñan un papel crucial en todo el proceso de gestión de riesgos. Implican la realización de actividades de retroalimentación y el intercambio constante de información. Este intercambio de información tiene como objetivo enriquecer los procesos, realizar ajustes y mejoras, y aplicar medidas preventivas o correctivas de manera oportuna. En otras palabras, se busca evitar la espera de la entrega de informes o la ocurrencia de daños a la organización para tomar medidas (Castañeda, 2018). La comunicación efectiva y la consulta con partes interesadas son esenciales para una gestión de riesgos proactiva y eficiente, permitiendo una respuesta adecuada a las amenazas y oportunidades en tiempo real.

Alcance, contexto y criterios: En esta fase se reconoce la necesidad de adaptar enfoques específicos a diversos sectores y aplicaciones debido a sus particularidades. El establecimiento del contexto se destaca como un paso crítico, involucrando la identificación de objetivos, consideración del entorno, reconocimiento de partes interesadas y diversidad de criterios de riesgo. Esto proporciona la base para comprender y evaluar la naturaleza y complejidad de los riesgos (Brito, 2018). Se deben definir criterios coherentes para evaluar la importancia de los riesgos, teniendo en cuenta factores como las causas y consecuencias. Es importante identificar de manera exhaustiva los riesgos y vincular esta etapa con los objetivos y procesos organizacionales, asegurando una comprensión completa de las amenazas y oportunidades.

Evaluación del riesgo: Este proceso implica la comparación de las evaluaciones de riesgo estimadas con los estándares de evaluación y aceptación de riesgos que se han establecido previamente en el contexto. En otras palabras, se trata de evaluar el riesgo calculado en función de un criterio de riesgo dado para determinar la significancia de dicho riesgo. La magnitud del riesgo se expresa en términos numéricos y se basa en factores como el valor de los activos de información, el impacto de la amenaza y la amplitud de la vulnerabilidad. Una vez que los riesgos han sido identificados, el marco de trabajo debe incorporar una metodología de análisis de riesgo. En el análisis de riesgo cualitativo, se utiliza una escala de atributos para describir la magnitud de las

posibles consecuencias (por ejemplo, baja, media y alta) y la probabilidad de que estas consecuencias ocurran.

Tratamiento del riesgo: El manejo de los riesgos implica la toma de decisiones en relación a las diversas amenazas presentes, de acuerdo a la estrategia de la organización. En este proceso, es esencial elegir medidas de control con el propósito de mitigar, aceptar y retener, evitar o transferir los riesgos. Además, es necesario elaborar un plan detallado que especifique cómo se abordarán y gestionarán dichos riesgos.

Seguimiento y revisión: El proceso de seguimiento y revisión en la gestión de riesgos debe ser planificado y someterse a una supervisión regular, ya sea de manera periódica o puntual, con responsabilidades claramente definidas. Estos procesos deben abarcar todos los aspectos de la gestión de riesgos para lograr varios objetivos, como verificar la eficacia y eficiencia de los controles, recopilar información adicional para mejorar la comprensión de los riesgos, analizar eventos, cambios, tendencias, éxitos y fracasos, identificar riesgos emergentes y detectar cambios en el contexto interno y externo que puedan requerir la revisión de las estrategias de tratamiento de riesgos y prioridades (Brito, 2018). Los resultados del seguimiento y revisión se deben registrar y utilizar tanto internamente como externamente.

Registro e informe o comunicación del riesgo: La comunicación del riesgo se trata del intercambio de información sobre riesgos entre todas las partes involucradas, tanto dentro como fuera de la organización. Sin una comunicación efectiva del riesgo, no se puede prever las consecuencias de un evento adverso (Rojas et al., 2018). Implica mantener una relación constante entre los niveles de dirección de la organización y los empleados, permitiendo que estos aporten ideas de mejora y estén al tanto de los cambios en el entorno que podrían afectar negativamente los objetivos de la organización.

Barboza (2015) presenta un compendio de las herramientas que pueden utilizarse para la gestión de Riesgos según la Norma ISO 31010. Las cuales son: Lluvia de ideas, entrevistas estructuras o semiestructuradas, Método Delphi, Listas de verificación, Análisis de principios peligrosos, Estudios de peligros y operatividad (HAZOP), Análisis de peligros y puntos críticos de control (HACCP), Valoración de riesgos ambientales, Estructura: “¿Qué sucedería si?” (SWIFT), Análisis de escenarios, Análisis de escenarios, Análisis de impacto del negocio, Análisis de causa raíz, Análisis del modo y efecto de la falla (AMEF), Análisis del árbol de falla, Análisis del árbol de

eventos, Análisis de causa y consecuencia, Análisis de causa y efecto, Análisis de niveles de protección (LOPA), Árbol de decisión, Análisis de confiabilidad humana, Análisis de corbata de lazo, Confiabilidad centrada en mantenimiento, Análisis de condiciones insidiosas (análisis transitorio), Análisis de Markov, Simulación Monte- Carlo, Estadística Bayesiana y Redes de Bayes, Curvas FN, Índice de riesgo, Matriz de consecuencia y probabilidad, Análisis costo beneficio, Análisis de decisión multicriterio

La gestión del riesgo empresarial se ha convertido en una estrategia fundamental para las organizaciones, los altos mandos de las organizaciones disponen de diversas herramientas y metodologías que desempeñan un papel crucial en la gestión de riesgos empresariales. Esto es esencial para los líderes y ejecutivos, porque los ayuda y encamina de manera estratégica a alcanzar los objetivos organizacionales (Hasper et al., 2017). En la Tabla 1 se presentan diversas metodologías para la gestión de riesgos en distintos contextos, junto con sus respectivos procesos. Estas metodologías han sido identificadas a través de una exhaustiva revisión bibliográfica. La tabla proporciona una visión general de las diferentes aproximaciones y enfoques que se han propuesto para abordar la gestión de riesgos en una amplia gama de escenarios, lo que resulta valioso para aquellos que buscan comprender y seleccionar la metodología más adecuada para sus necesidades específicas.

Tabla 1. Metodologías para la Gestión de Riesgos

Autor	**Fases de la Gestión de Riesgos**
Gestión de riesgos en encadenamientos productivos sostenibles (Pérez & Vega, 2021)	**Fase I. Manejo inicial** Paso 1. Preparación del equipo de trabajo Paso 2. Diagnóstico de la gestión de riesgos logísticos **Fase II. Identificación de los riesgos** Paso 3. Análisis las actividades logísticas entre proveedores a clientes Paso 4. Clasificación de los riesgos según brechas en el servicio al cliente. **Fase III. Evaluación de los riesgos**

	Paso 5. Estimación de los riesgos Paso 6. Determinación del nivel de prioridad **Fase IV. Tratamiento y prevención del riesgo** Paso 7. Tratamiento del riesgo Paso 8. Elaboración del Plan de prevención de riesgos Paso 9. Estrategia de mejora de la gestión de riesgos del servicio al cliente e incremento de valor.
Gestión de riesgos mediante el ciclo PHVA (Planificar-Hacer-Verificar-Actuar) (Rojas et al., 2018).	**Planificar** Comunicación y consulta Establecimiento del contexto **Hacer** Identificación de riesgos Valoración de los riesgos **Verificar** Evaluación de los riesgos Determinación del nivel de vulnerabilidad de la Organización **Actuar** Tratamiento de los riesgos Seguimiento y revisión Comunicación del riesgo
Metodología basada en FD AFNOR X50-117 Gestión de riesgos de un proyecto (Muñoz & Cuadros, 2017).	1. **Conceptualización del riesgo:** Se lleva a cabo un proceso de lluvia de ideas y análisis de los riesgos estratégicos que están relacionados con el proyecto en cuestión, marcando el inicio del proyecto. 2. **Planificación de la respuesta al riesgo:** Aquí se definen los riesgos por fase y se establecen indicadores para evaluarlos adecuadamente.

	3. **Ejecución de la respuesta a los riesgos:** Durante esta fase, se revisan los riesgos previamente identificados y se toman medidas de acuerdo con el plan de respuesta establecido. 4. **Terminación:** Se crea un informe final de riesgos que incluye información sobre los riesgos que ocurrieron, cómo se mitigaron, el cumplimiento de objetivos y se analizan las lecciones aprendidas, tanto los éxitos como las fallas del proyecto. Para mejorar la identificación de riesgos, recomienda sistematizar los siguientes aspectos: el origen de los riesgos, la fase en la que pueden ocurrir, las posibles consecuencias y una evaluación de los mismos. En esta evaluación, cada riesgo recibe una calificación tanto para su impacto como para su probabilidad.
Metodología de gestión de riesgos de proyectos para pequeñas empresas (Marcelino-Sádaba et al., 2014**)**	**Definición del proyecto** Análisis del entorno del proyecto 5. Definición de objetivos del proyecto 6. Identificación de riesgos estratégicos asociados al proyecto **7. Planificación de proyecto** 8. Definición de un plan de gestión de riesgos 9. Identificación de riesgos operacionales 10. Análisis y evaluación de riesgos **11. Ejecución y control del proyecto** 12. Seguimiento y control del estado de los riesgos 13. Comunicación de riesgos del proyecto **14. Cierre y evaluación final del proyecto** Informe de resultados del proyecto Lecciones aprendidas

FIPCAEC (Edición. 39) Vol. 8, No 4, Octubre-Diciembre 2023, pp. 135-157, ISSN: 2588-090X

Ciclo Deming considerando la ISO 27005 Ciclo PDCA (Arévalo et al., 2017)	**Plan:** Identificar los Activos de información y sus requerimientos de seguridad asociados. - Evaluar los riesgos de seguridad de la información. - Seleccionar los controles relevantes para gestionar los riesgos inaceptables **Do:** Implementar Controles-Gestionar Operaciones. **Check:** Monitorear el Rendimiento - Evaluar el Rendimiento **Act:** Acciones Preventivas - Acciones Correctivas
Norma ISO 27001 Sistema de Gestión de la Seguridad de la Información (SGSI) - Evaluación de Riesgos (International Organization for Standardization, 2018).	**1. Identificar los Activos de Información y sus responsables,** **2. Identificar las Vulnerabilidades de cada activo: aquellas** **3. Identificar las amenazas: Aquellas cosas que puedan suceder y** **4. Identificar los requisitos legales y contractuales** **5. Identificar los riesgos:** **6. Cálculo del riesgo:** **7. Plan de tratamiento del riesgo:** Asumir el riesgo Reducir el riesgo Eliminar el riesgo Transferir el riesgo
Modelos de Gestión de Riesgos de Seguridad de la Información. (MGRSI) (Zevallos, 2019)	**Establecimiento del contexto:** Se toman en cuenta la cultura organizacional, los recursos de la organización, así como los procesos y objetivos organizacionales. **Definición de alcance:** Es esencial tener en cuenta aspectos tanto internos como externos, considerar a las partes interesadas y evaluar los requisitos, interfaces y dependencias entre actividades **Identificación de activos:** implica la creación de un inventario que se utiliza para categorizarlos en función de su importancia para la organización, permitiendo así la asignación de niveles de

FIPCAEC (Edición. 39) Vol. 8, No 4, Octubre-Diciembre 2023, pp. 135-157, ISSN: 2588-090X

	protección correspondientes en base a sus características y roles en los procesos. **Identificación de riesgos** **Análisis de riesgos** **Estimación de riesgos** Probabilidad de ocurrencia Impacto Niveles de Riesgo **Declaración de Aplicabilidad:** tiene como objetivo mantener un registro y describir el control de las medidas de seguridad relevantes y aplicables, basándose en los resultados de procesos de evaluación y tratamiento, requisitos regulatorios. **Tratamiento de riesgos** **Revisión del cumplimiento** Medición de eficacia de controles Acciones correctivas Registro e informe Monitoreo, seguimiento y revisión Comunicación y consulta
Modelo de Gestión de Riesgos Project Management Institute PMBOK (Rodas, 2017).	**Inicio** **Planificación** 1.Planificar la Gestión de los riesgos 2.Identificar los riesgos 3.Realizar análisis cualitativo de los riesgos 4.Realizar análisis cuantitativo de los riesgos 5.Planificar la respuesta a los riesgos **Ejecución** **Monitoreo** **Control**

	6.Controlar los riesgos **Cierre**
Componente 300 Evaluación de Riesgos (Fiscalía General del estado, 2016)	**300-01 Identificación del Riesgo** **300-02 Plan de mitigación de Riesgos** - Análisis de los factores externos e internos que implican la exposición al riesgo - Inventario de eventos o los riesgos que afectan el cumplimiento de los objetivos de la institución - Valoración de los riesgos desde la perspectiva de la probabilidad y el impacto - Plan de mitigación de riesgos institucionales que incluyan objetivos, estrategias de gestión y metas, asignación de responsabilidad para cada unidad. **300-03 Valoración de los Riesgos** **300-04 Respuesta al Riesgo**
Guía para la gestión de riesgos de seguridad de la información. (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2016)	**Establecimiento del contexto** 1.Consideraciones Generales - Levantamiento de información inicial 2. Establecer criterios básicos para la Gestión del Riesgo 3. Definir alcance y límites de la Gestión del Riesgo 4.Establecer una organización para la operación del SGRSI **Valoración del Riesgo** 5. Identificar Activos de Información 6. Identificar las amenazas y las vulnerabilidades 7. Identificar los controles existentes 8. Identificar consecuencias 9. Valorar las consecuencias 10. Valorar los incidentes 11. Determinar el nivel de estimación del riesgo

12. Evaluar el riesgo

Tratamiento del Riesgo

13. Seleccionar controles Aceptación del Riesgo
14. Aceptar el riesgo Comunicación del Riesgo
15. Comunicar el riesgo Monitoreo y Revisión del Riesgo
16. Monitorear y revisar los riesgos

En este análisis de diversas metodologías de gestión de riesgos, se destacan algunos procesos que se repiten y son fundamentales en la mayoría de los enfoques. Estos procesos clave incluyen la identificación de riesgos, su valoración, la planificación de respuestas, el monitoreo y revisión, así como la comunicación y consulta. Estos elementos se consideran esenciales para comprender, evaluar y gestionar los riesgos en diferentes contextos, ya sea en proyectos, seguridad de la información, gestión de proyectos, o en el ámbito general de la gestión de riesgos. Independientemente de la metodología específica utilizada, estos procesos son universales en la gestión de riesgos y proporcionan un marco sólido para la toma de decisiones informadas y la mitigación de riesgos. Cada metodología agrega sus propias particularidades y enfoques adicionales, pero estos procesos fundamentales siguen siendo consistentes en la gestión de riesgos en diversos dominios y son esenciales para lograr una gestión efectiva de los riesgos.

Conclusiones

Las diferentes metodologías de gestión de riesgos presentadas en este análisis ofrecen una amplia gama de enfoques y procesos para abordar los desafíos asociados con la identificación, evaluación y mitigación de riesgos en distintos contextos. Estas metodologías demuestran que, independientemente de la industria o el ámbito en el que se apliquen, existen principios fundamentales que guían una gestión efectiva de riesgos.

En primer lugar, es evidente que la gestión de riesgos es un proceso continuo y cíclico. Todas las metodologías presentadas, desde la gestión de riesgos en encadenamientos productivos sostenibles hasta la seguridad de la información y la gestión de riesgos de proyectos, enfatizan la importancia de un enfoque iterativo. Esto implica que, en lugar de ser una actividad puntual, la gestión de riesgos debe ser incorporada como un componente integral de la operación cotidiana de una

organización. La identificación y la evaluación de riesgos son pasos críticos en todas las metodologías. Cada una de ellas proporciona métodos y procesos específicos para identificar los riesgos potenciales y evaluar su probabilidad e impacto. Algunas metodologías se centran en riesgos estratégicos, mientras que otras se enfocan en riesgos operativos o en riesgos de seguridad de la información. Sin embargo, todas comparten la premisa de que la identificación y la evaluación de riesgos son fundamentales para la toma de decisiones informadas.

La planificación de respuestas es otro componente clave en la gestión de riesgos. Cada metodología presenta un conjunto de pasos que incluyen la definición de respuestas a los riesgos identificados. Estas respuestas pueden incluir medidas de mitigación, aceptación del riesgo, transferencia o eliminación. Esta fase de planificación asegura que las organizaciones estén preparadas para abordar los riesgos de manera proactiva y efectiva.

La comunicación y consulta son aspectos críticos que se destacan en varias de las metodologías, especialmente en el contexto de la seguridad de la información y la gestión de proyectos. La interacción con partes interesadas internas y externas es esencial para asegurar que los riesgos se comprendan y gestionen adecuadamente. Esta comunicación facilita la colaboración y la toma de decisiones informadas.

Aunque cada metodología aborda riesgos en contextos específicos, existen elementos comunes que subyacen a todas ellas. La gestión de riesgos es un proceso continuo que requiere identificación, evaluación, planificación de respuestas y comunicación. La aplicación de estas metodologías ayuda a las organizaciones a minimizar la incertidumbre, tomar decisiones fundamentadas y garantizar la continuidad de sus operaciones, independientemente de su ámbito de actividad.

Referencias

Arévalo, F. M., Cedillo, I. P., & Moscoso, S. A. (2017). Metodología Ágil para la Gestión de Riesgos Informáticos Agile Methodology for Computer Risk Management. Revista Killkana Técnica, 1(2). https://www.researchgate.net/publication/321176840

Barboza, M. (2015). Generalidades de la NTC-ISO 31000: 2009 para la atención de los riesgos corporativos en las empresas.

Bodero, E., De Giusti, M. R., & Morales, C. (2022a). Preservación digital a largo plazo: estándares, auditoría, madurez y planificación estratégica. Revista Interamericana de Bibliotecología, 45(2). https://doi.org/10.17533/udea.rib.v45n2e344178

Bodero, E. M., De Giusti, M. R., & Morales, C. H. (2022b). Modelo de madurez para preservación digital basado en conceptos de planificación estratégica. Investigación Bibliotecológica: Archivonomía, bibliotecología E información, 37(94), 51–73. https://doi.org/10.22201/iibi.24488321xe.2023.94.58654

Brito, D. (2018). El riesgo empresarial. Revista Universidad y Sociedad, 10(1), 269-277. http://scielo.sld.cu/scielo.php?pid=S2218-36202018000100269&script=sci_arttext

Castañeda, J. (2018). Gestión, administración de riesgos y modelos de control interno. https://digitk.areandina.edu.co/handle/areandina/3542

Contreras, A. B. (2020). Papel estratégico de la gestión de "nuevos" riesgos. En Y. Rico, D. López Cortés, & A. Cerón R. (comps.), Enfoques y gestión en Seguridad Integral (pp. 129-160). Escuela de Postgrados de la Fuerza Aérea Colombiana.

Cruz, M., & Morejón, M. (2019). Metodología para la gestión integral de riesgos y seguros con enfoque de gestión social cooperativa. Cooperativismo y Desarrollo, 7(1), 74-96. http://scielo.sld.cu/scielo.php?pid=S2310-340X2019000100074&script=sci_arttext&tlng=en

Díaz, D. A. (2017). Gestión de riesgos en entornos empresariales alineados a la Norma ISO 31000. Universidad Piloto de Colombia. http://repository.unipiloto.edu.co/handle/20.500.12277/4930

Espinoza, L., Barriga, B., Izurieta, J., & Morales, C. (2022). Seguridad informática aplicando la Autentificación por Doble factor para la plataforma HomeOfi. Dominio de las Ciencias, 8(3), 503-523. https://dialnet.unirioja.es/descarga/articulo/8637935.pdf

Espinoza, L., Congacha, A. & Díaz, J. (2023). Calidad de datos con Python: un enfoque práctico. Esprint Investigación, 2(2). 26-34. https://doi.org/10.61347/ei.v2i2.55

Fiscalía General del Estado. (2016). Guía para la Administración del Riesgo Institucional. https://www.fiscalia.gob.ec/transparencia/resoluciones/resolucion019FGE2016.pdf

Hasper, J., Correa, J. C., Benjumea, M., & Valencia, A. (2017). Tendencias en la investigación sobre gestión del riesgo empresarial: un análisis bibliométrico. Revista Venezolana de Gerencia, 22(79), 506-524. https://www.redalyc.org/articulo.oa?id=29055964010

Marchesano, M., & Scavone, G. M. (2020). La información financiera de calidad como facilitadora de gestión de riesgos y toma de decisiones. Journal of Management & Business Studies, 2(1). https://doi.org/10.32457/jmabs.v2i1.527

Marcelino-Sádaba, S., Pérez-Ezcurdia, A., Lazcano, A. M. E., & Villanueva, P. (2014). Project risk management methodology for small firms. International journal of project management, 32(2), 327-340. https://doi.org/10.1016/j.ijproman.2013.05.009

Martínez, R., & Blanco, M. (2017). Gestión de riesgos: reflexiones desde un enfoque de gestión empresarial emergente. Revista Venezolana de Gerencia, 22(80), 693-711. https://www.redalyc.org/articulo.oa?id=29055967009

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2016). Guía para la gestión de riesgos de seguridad de la información. https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2020/04/GU%C3%8DA-PARA-LA-GESTI%C3%93N-DE-RIESGOS-DE-SEGURIDAD-DE-LA-INFORMACI%C3%93N-ABRIL-2020.pdf

Muñoz, D., & Cuadros, A. C. (2017). Comparación de metodologías para la gestión de riesgos en los proyectos de las Pymes. Revista Ciencias Estratégicas, 25(38), 319-338. http://www.redalyc.org/articulo.oa?id=151354939004

International Organization for Standardization. (2018). Gestión del riesgo — Directrices ISO 31000. https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:es

International Organization for Standardization. (2018). Sistemas de gestión de seguridad de la información ISO 27001. https://www.normas-iso.com/implantando-iso-27001/

Lizarzaburu, E. R., Barriga, G., Noriega, L. E., López, L., & Mejía, P. Y. (2017). Gestión de riesgos empresariales: marco de revisión ISO 31000. Revista Espacios, 38(59). https://www.revistaespacios.com/a17v38n59/a17v38n59p08.pdf

Palacio-Fierro, A. A., Arévalo-Chávez, P. B., & Mantilla-Garcés, D. M. (2016). Un Estudio Exploratorio a la Gestión de Riesgos Empresariales en las PYMES de la Ciudad de Quito. CienciAmérica, 5(1), 51-62. http://201.159.222.118/openjournal/index.php/uti/article/view/44

Palma, C. P. (2011). ¿Cómo construir una matriz de riesgo operativo? Revista de Ciencias económicas, 29(1). https://doi.org/10.15517/rce.v29i1.7061

Pérez, M.., & Vega, L. (2021). Gestión de riesgos en encadenamientos productivos sostenibles. Revista Venezolana de Gerencia: RVG, 26(96), 1396-1412. https://dialnet.unirioja.es/servlet/articulo?codigo=8890567

Rodríguez, M. R., Piñeiro, C., & De Llano, P. (2013). Mapa de riesgos: Identificación y gestión de riesgos. Atlantic Review of Economics: Revista Atlántica de Economía, 2(1), 2-29. https://www.econstor.eu/handle/10419/146556

Rudas, L. (2017). Modelo de gestión de riesgos para proyectos de desarrollo tecnológico. [Tesis de Maestría, Santiago de Queretaro: CIATEQ.] https://ciateq.repositorioinstitucional.mx/jspui/handle/1020/86

Rojas, L., González, A., Rivero, J., Yglesia, A., & Montes de Oca, N. (2018). Procedimiento para la gestión de riesgos de los procesos de un sistema de gestión. Revista Cubana de Administración Pública y Empresarial, 2(3), 222-240.

Soler, R. H., Pirela, A. E., & Navarro, N. (2020). La gestión de riesgos en los procesos logísticos de la empresa logistics Unlimited SA Logunsa. Revista Universidad y Sociedad, 12(3), 195-202. https://rus.ucf.edu.cu/index.php/rus/article/view/1575

Valencia, B., & Narváez, I. (2021). La gestión de riesgos financieros y su incidencia en la toma de decisiones. CIENCIAMATRIA, 7(2), 691-722. https://doi.org/10.35381/cm.v7i2.526

Vera, R., & Pilco, E. (2008). Metodología para el tratamiento de riesgos empresariales. Ciencia & Desarrollo, (12), 107-110. https://doi.org/10.33326/26176033.2008.12.268

Zevallos, M. (2019). Modelo de gestión de riesgos de seguridad de la información: Una revisión del estado del arte. Revista peruana de computación y sistemas, 2(2), 43-60. http://dx.doi.org/10.15381/rpcs.v2i2.17103