GESTÃO DE RISCO COMO FERRAMENTA ESTRATÉGICA EMPRESARIAL

Davi dos Santos[1], Eduarda Vitória Cotes Pereira [1], Fernanda Garcia dos Santos[1].
Diego Lucien Domingues Martins [2], Tiago Bazolli [2]

[1] Alunos – Faculdades Integradas ASMEC – UNISEP, Ouro Fino MG.
[2] Orientadores – Faculdades Integradas Asmec UNISEP, Ouro Fino MG.

RESUMO

O presente artigo tem por objetivo analisar a gestão de risco como pratica estratégica empresarial, como as organizações modernas utilizam métodos e modelos como ferramenta prática. Em um cenário de negócios cada vez mais competitivo e dinâmico, uma empresa ter a capacidade de identificar, avaliar e responder a riscos se tornou um diferencial de mercado, e base para manter a sustentabilidade organizacional. Assim, este estudo aborda os conceitos fundamentais de risco, considerado tanto ameaça quanto oportunidade, e propõe fazer um exame dos principais tipos de riscos empresariais e descrever o processo sistemático de gestão, da identificação ao monitoramento contínuo. Ademais, são apresentadas ferramentas como Matriz de Risco, Análise SWOT, Indicadores-Chave de Risco (KRIs) e auditorias internas, bem como os modelos normativos ISO 31000:2018 e COSO ERM (2017). Os resultados evidenciam que organizações com práticas estruturadas de gestão de riscos obtêm vantagens competitivas, maior resiliência diante de crises e melhoria contínua no desempenho. Conclui-se que a gestão de riscos deve ser compreendida como processo contínuo, integrado à estratégia e à cultura organizacional, e não apenas como instrumento reativo de controle.

Palavras-chave: Gestão de risco. ISO 31000. COSO ERM. Processos organizacionais. Sustentabilidade empresarial.

1. INTRODUÇÃO

Na última década, o ambiente organizacional tem se mostrado progressivamente mais instável e complexo, este fenômeno é intensificado por eventos recentes da humanidade. Entre eles podemos destacar a pandemia da COVID-19. A pandemia expôs fragilidades estruturais em cadeias de suprimentos globais e impôs migrações abruptas para o trabalho remoto, testando a capacidade de adaptação das empresas em tempo real. Paralelamente, a aceleração da transformação digital ampliou exponencialmente as vulnerabilidades cibernéticas, enquanto oscilações macroeconômicas e mudanças regulatórias sucessivas tornaram o cenário ainda mais imprevisível. Esses acontecimentos não apenas pressionaram a resiliência organizacional, mas também redefiniram prioridades, evidenciando que o risco sistêmico pode surgir de qualquer direção e em velocidade inesperada. Diante desse contexto de incertezas permanentes,

a capacidade de antecipar, absorver e responder a choques externos deixou de ser percebida como uma função meramente defensiva ou restrita a departamentos específicos, passando a ocupar o centro da estratégia corporativa e da governança. É nesse cenário que a gestão de risco empresarial se consolida como disciplina indispensável, atuando não apenas para mitigar perdas, mas para garantir adaptabilidade, continuidade dos negócios e criação de valor mesmo em situações adversas severas.

A gestão de risco pode ser compreendida como um conjunto estruturado de práticas orientadas à identificação, análise e resposta a eventos que possam comprometer, ou potencializar, o alcance dos objetivos organizacionais. Segundo o COSO (2017), a integração da gestão de riscos à estratégia e ao desempenho das organizações representa um passo decisivo para a criação e preservação de valor. De maneira complementar, a ABNT NBR ISO 31000 (2018) reforça que gerenciar riscos de forma sistemática contribui diretamente para a melhoria do desempenho, o estímulo à inovação e a qualificação do processo decisório. A relevância do tema justifica-se não apenas pela sua aplicabilidade prática, mas também pela crescente exigência de transparência e governança nas organizações. Empresas que negligenciam a gestão de riscos ficam expostas a consequências que vão desde perdas financeiras e danos operacionais até crises reputacionais capazes de comprometer sua continuidade no mercado.

Este artigo tem como objetivo geral apresentar os fundamentos da gestão de risco empresarial, com ênfase nos processos, métodos e modelos utilizados pelas organizações. Para tanto, foram definidos os seguintes objetivos específicos: (a) conceituar risco e seus elementos constitutivos; (b) classificar os principais tipos de riscos empresariais; (c) descrever o processo de gestão de riscos; (d) apresentar as ferramentas e métodos de análise mais utilizados; e (e) discutir os principais modelos normativos e os benefícios e desafios da implementação da gestão de riscos nas organizações.

Do ponto de vista metodológico, trata-se de uma pesquisa bibliográfica de natureza qualitativa, desenvolvida a partir da revisão de literatura especializada, normas internacionais e obras de referência na área de gestão estratégica e análise de riscos.

METODOLOGIA

Para melhor compreendermos sobre o assunto, escolhemos a pesquisa bibliográfica, foi uma decisão alinhada à própria natureza do tema investigado. A gestão de riscos empresariais é um campo que se sustenta em conceitos, princípios e diretrizes consolidados em normas internacionais, como por exemplo a ISO 31000:2018 e o COSO ERM (2017), entre outras. Pesquisamos artigos nacionais e internacionais a respeito do tema e compilamos neste artigo as quais acreditamos serem as mais relevantes para compor este, que poderá ser utilizado para futuras pesquisas acadêmicas no futuro.

2. A GESTÃO DE RISCO E SUA RELEVÂNCIA ORGANIZACIONAL

O risco é geralmente definido como: ‘a possibilidade de ocorrência de um evento futuro incerto’ que, caso venha a se concretizar, poderá impactar os objetivos de uma organização de maneira negativa, que pode vir a configurar uma ameaça ou uma oportunidade. Essa dualidade conceitual é fundamental para que os gestores não interpretem o risco de forma unilateral, mas como fenômeno com dupla natureza. Diferentemente de um problema já materializado, o risco é sempre prospectivo: refere-se a algo que ainda não aconteceu, mas que carrega consigo a possibilidade de acontecer.

Para Hubbard (2009), a falha na gestão de riscos frequentemente acontece da aplicação equivocada de métodos de análise, estes subestimam ou superestimam a real probabilidade de eventos adversos, comprometendo a qualidade das decisões gerenciais. *"Alguns dos métodos de 'gestão de riscos' mais populares não são melhores do que a astrologia"* (Hubbard, 2009, p. 46).

Para o autor, sua principal crítica é que as metodologias populares, em vez de reduzirem a incerteza, criam uma falsa sensação de segurança.

O autor aponta que um dos principais problemas, são os "erros humanos completamente evitáveis em julgamentos subjetivos de risco". Hubbard (2009) aponta que os gestores, ao confiarem em sua memória e intuição, acabam por subestimar o nível dos riscos. O resultado é que as decisões são tomadas com base em "achismos" que podem não proteger a empresa, o que leva a uma avalição falsa do risco.

O conceito de risco pode ser desmembrado em três componentes analíticos: (i) a natureza do evento, que descreve o fenômeno passível de ocorrer; (ii) sua probabilidade de concretização; e (iii) a magnitude dos efeitos que sua materialização causaria à organização. A fórmula tradicional expressa essa relação como: Risco = Probabilidade × Impacto. Essa relação pode ser expressa pela equação: Risco = Probabilidade × Impacto. A tabela a seguir ilustra como a combinação entre probabilidade e impacto determina o nível de criticidade de um risco:

Impacto **Probabilidade**	**Baixa**	**Média**	**Alta**
Alto	Médio	Alto	Muito Alto
Médio	Baixo	Médio	Alto
Baixo	Baixo	Baixo	Médio

Quadro 1 – Matriz de criticidade dos riscos

Fonte: Adaptado de ABNT NBR ISO 31000 (2018).

2.1 Importância da gestão de riscos nas organizações

A gestão de riscos ocupa um lugar estratégico no conjunto de práticas de gestão organizacional, pois viabiliza uma atuação mais segura, previsível e eficiente por parte das empresas. Em um ambiente de negócios cada vez mais competitivo, a ausência de mecanismos de gestão de riscos pode comprometer significativamente os resultados e até a sobrevivência da empresa. Entre os principais aspectos que justificam a relevância da gestão de riscos, destacam-se: a prevenção de perdas financeiras, operacionais e estratégicas; o aprimoramento do processo decisório com base em informações estruturadas; a garantia de continuidade do negócio em situações adversas; a proteção da imagem e da reputação institucional; o cumprimento das obrigações legais e regulatórias; a identificação de oportunidades de crescimento e inovação; e a obtenção de vantagem competitiva sustentável.

Conforme Freeman (1984), a gestão organizacional eficaz pressupõe a consideração das demandas e expectativas de todas as partes interessadas (stakeholders), o que torna a gestão de riscos um instrumento de alinhamento entre a estratégia corporativa e os interesses dos diferentes grupos que compõem o ecossistema organizacional. O autor define Stakeholder como:

"Qualquer grupo ou indivíduo que pode afetar ou ser afetado pela realização dos objetivos da organização, o que torna a gestão de riscos um instrumento de alinhamento entre a estratégia corporativa e os interesses dos diferentes grupos que compõem o ecossistema organizacional". (Freeman 1984, p. 46)

2.2 Tipologias dos riscos empresariais

As organizações estão sujeitas a uma pluralidade de riscos que variam conforme o setor de atuação, o porte da empresa e o contexto ambiental em que estão inseridas. A classificação dos riscos empresariais permite uma abordagem mais sistematizada e facilita a definição de estratégias específicas de mitigação e resposta. Apresentam-se, a seguir, as principais categorias.

Riscos estratégicos - Os riscos estratégicos decorrem de decisões de alto nível relacionadas ao posicionamento competitivo, ao planejamento de longo prazo e à formulação dos objetivos organizacionais. A má interpretação de tendências de mercado, escolhas mal embasadas ou a incapacidade de adaptação a mudanças no ambiente externo podem comprometer seriamente o desempenho da organização. Mintzberg, Ahlstrand e Lampel (2010) ressaltam que a formulação estratégica eficaz requer visão sistêmica e capacidade de leitura do ambiente, características que são diretamente impactadas quando os riscos estratégicos não são devidamente gerenciados.

Riscos financeiros - Os riscos financeiros dizem respeito à gestão dos recursos monetários da organização e incluem exposições a variações nas taxas de juros, câmbio, inadimplência de clientes, falta de liquidez e desequilíbrios no fluxo de caixa. Tais riscos podem afetar diretamente a rentabilidade e a capacidade de sustentação das operações, exigindo controles financeiros rigorosos e planejamento adequado.

Riscos operacionais - Os riscos operacionais estão relacionados a falhas nos processos internos, erros humanos, problemas em sistemas tecnológicos ou inadequações em procedimentos operacionais. Quando não gerenciados, podem resultar em interrupções das atividades, redução da produtividade, aumento de custos e comprometimento da qualidade dos produtos ou serviços.

Riscos legais e regulatórios - Os riscos legais e regulatórios referem-se ao descumprimento de legislações, normas e regulamentações que disciplinam a atividade empresarial. Suas consequências podem incluir multas, sanções administrativas, processos judiciais e danos à reputação. A constante atualização normativa e a adoção de práticas de compliance são medidas fundamentais para a mitigação desse tipo de risco.

Riscos de mercado - Os riscos de mercado estão associados a oscilações nas condições externas ao negócio, como variações na oferta e demanda, comportamento do consumidor, movimentos da concorrência e instabilidades econômicas. Tais fatores podem afetar preços, receitas e a posição competitiva da organização, demandando monitoramento contínuo do ambiente externo.

Riscos tecnológicos - Com a digitalização crescente dos processos empresariais, os riscos relacionados à tecnologia ganharam destaque. Falhas em sistemas de informação, ataques cibernéticos, perda de dados e obsolescência tecnológica figuram entre as principais ameaças desse tipo, exigindo investimento contínuo em segurança da informação e atualização tecnológica.

Riscos ambientais e sociais - Os riscos ambientais e sociais envolvem impactos relacionados ao meio ambiente e à responsabilidade social corporativa. Desastres ambientais, uso inadequado de recursos naturais e impactos negativos sobre comunidades são exemplos de eventos que podem afetar não apenas o desempenho financeiro da empresa, mas também sua imagem institucional e legitimidade social.

2.3 Processo de gestão de riscos

A gestão de riscos organizacionais é estruturada em um processo contínuo, sistemático e integrado à estratégia da empresa. Esse processo permite identificar, analisar e tratar incertezas que possam impactar os objetivos organizacionais, conferindo maior previsibilidade e segurança à tomada de decisão. As principais etapas desse processo são descritas a seguir.

Primeira fase, a identificação dos riscos: A identificação dos riscos consiste em mapear todos os eventos potenciais, sejam eles internos e ou externos, desde que possam afetar, de forma positiva ou negativa, os objetivos da organização. Essa etapa é crítica: riscos não identificados simplesmente não podem ser gerenciados. Para tanto, recorre-se a técnicas como brainstorming com equipes multidisciplinares, entrevistas com gestores, checklists estruturados de riscos e análise do histórico de ocorrências da própria organização ou do setor. Uma identificação eficaz demanda a participação de diferentes níveis hierárquicos, já que cada área possui uma percepção particular dos riscos aos quais está exposta.

Segunda fase, análise e avaliação dos riscos: logo que um risco for identificado, é necessário classifica-lo de acordo com a sua natureza, causas e potenciais consequências. Nessa fase, avaliam-se a probabilidade de ocorrência, o impacto potencial sobre os objetivos, a velocidade com que o risco pode se manifestar e a capacidade da organização de detectá-lo a tempo. A análise pode ser conduzida de forma qualitativa — baseada em julgamento e experiência — ou quantitativa — com suporte em dados estatísticos e modelos matemáticos. Organizações que utilizam dados históricos têm maior precisão nessa avaliação e, por consequência, tomam decisões mais assertivas.

Terceira fase, a classificação e priorização: Após a análise, os riscos são classificados em níveis de criticidade, se ele é alto, médio ou baixo, e assim, cria-se uma matriz entre combinação, probabilidade e impacto. Essa etapa é fundamental para a alocação eficiente de recursos, concentrando esforços nos riscos mais críticos e evitando desperdício com riscos de relevância marginal. A priorização deve estar alinhada ao apetite ao risco da organização, ou seja, ao nível de risco que ela deliberadamente aceita assumir em busca de seus objetivos estratégicos.

Quarta fase, o tratamento e resposta aos riscos: O tratamento dos riscos acontece com a definição de quais estratégias serão adotadas para lidar com cada risco identificado. As principais são: (i) evitar, eliminar a atividade que origina o risco; (ii) reduzir (mitigar), criar controles que diminuam a ocorrência ou que possam vir a diminuir o impacto na empresa; (iii) transferir, ou repassar o risco a empresas terceiras que prestam serviço, por meio de contratos de terceirização; e (iv) aceitar, quando o risco está dentro do da capacidade organizacional e seu custo de miti gação supera o impacto esperado. Cada ação de resposta deve ser acompanhada de responsável definido, prazo e indicadores de acompanhamento.

E por fim, é necessário manter o, monitoramento e controle contínuo: A gestão de riscos não se encerra com o tratamento dos riscos identificados. O ambiente organizacional é dinâmico e novos riscos emergem constantemente, enquanto riscos já mapeados podem mudar de natureza ou intensidade. Por isso, o monitoramento contínuo é indispensável. Ele envolve a revisão periódica dos riscos, o acompanhamento de indicadores de desempenho e a atualização das estratégias em função de mudanças

internas ou externas. Ferramentas como dashboards de risco, relatórios gerenciais e auditorias periódicas são instrumentos habituais nessa fase.

2.4 Ferramentas e métodos de análise de risco

A eficácia da gestão de riscos está diretamente relacionada à qualidade dos instrumentos utilizados para identificar, analisar e monitorar os riscos organizacionais. A seguir, são apresentadas as principais ferramentas empregadas nesse processo.

Matriz de risco – provavelmente é a ferramentas mais conhecida na gestão organizacional. Por meio de um formato tabular ou gráfico, permite visualizar os riscos em função de dois eixos: probabilidade de ocorrência e impacto potencial. Sua simplicidade visual facilita a comunicação dos resultados entre diferentes níveis da organização e agiliza o processo de priorização. Deve ser atualizada regularmente para refletir a realidade dinâmica da empresa.

Para Baraldi (2005), a matriz de risco, embora amplamente utilizada por sua simplicidade visual, deve ser empregada com cautela, pois sua eficácia depende da qualidade dos dados que a alimentam e da frequência com que é atualizada.

Análise SWOT - Strengths, Weaknesses, Opportunities, Threats, também conhecida no Brasil como FOFA (Forças, Oportunidades, Fraquezas e Ameaças) é uma ferramenta de diagnóstico estratégico que examina os dois ambientes de uma empresa, o interno e o externo.

Segundo Chiavenato (2014), destaca que a análise SWOT, embora simples em sua estrutura, exige um olhar crítico para que as forças e fraquezas internas não sejam confundidas com meras impressões gerenciais.

No contexto da gestão de riscos, as ameaças identificadas na análise correspondem a riscos externos, enquanto as fraquezas mapeadas revelam vulnerabilidades internas. A SWOT não substitui ferramentas específicas de análise de risco, mas complementa o diagnóstico estratégico, favorecendo uma visão integrada dos fatores que podem impactar a organização.

Análise de cenários – consiste na elaboração de projeções sobre possíveis configurações futuras do ambiente organizacional, contemplando situações otimistas, realistas e pessimistas. Por meio dessa abordagem, os gestores antecipam possíveis impactos de eventos como quedas nas vendas, aumento de custos ou mudanças regulatórias. Essa ferramenta é amplamente utilizada em planejamento financeiro e estratégico, pois fortalece a capacidade de resposta da organização diante de incertezas.

Indicadores chave de risco (KRIs) – são métricas concebidas para sinalizar, com antecedência, a possível materialização de um risco. Exemplos incluem o índice de inadimplência, a taxa de falhas

operacionais e o índice de rotatividade de colaboradores. Para serem eficazes, os KRIs devem ser mensuráveis, relevantes para os riscos identificados e atualizados com frequência compatível com a dinâmica do negócio.

Para Hubbard (2009) o autor alerta que indicadores só são úteis se forem calibrados com base em dados históricos confiáveis e se houver clareza sobre o que cada métrica realmente sinaliza, do contrário, podem gerar falsa sensação de segurança.

Auditorias internas – são mecanismos de avaliação sistemática dos processos e controles organizacionais, com o objetivo de identificar falhas, garantir a conformidade com normas e regulamentos e propor melhorias. Diferentemente de uma ação punitiva, as auditorias devem ser entendidas como instrumento de aprendizagem organizacional e aprimoramento contínuo. Podem ser classificadas em operacionais, financeiras ou de conformidade, cada uma com foco específico.

2.5 Modelos e normas de gestão de risco

A adoção de modelos e normas reconhecidos internacionalmente confere rigor, padronização e credibilidade à gestão de riscos. Dois referenciais se destacam no cenário global: a ISO 31000 e o COSO ERM.

ISO 31000:2018 - A ABNT NBR ISO 31000 (2018) é uma norma internacional que estabelece princípios e diretrizes para a gestão de riscos em organizações de qualquer porte, setor ou natureza jurídica. Sua estrutura contempla três dimensões inter-relacionadas: princípios, estrutura e processo. Os princípios orientam os valores que devem nortear a gestão de riscos; a estrutura descreve como organizar e sustentar a gestão de riscos no contexto da governança organizacional; e o processo detalha as etapas de implementação, da comunicação e consulta ao monitoramento contínuo. A norma, portanto, não se limita a oferecer um conjunto de recomendações abstratas; ela propõe uma abordagem concreta e aplicável.

Conforme observa Santos (2021) em:

> A International Organization for Standardization (ISO) publicou a norma ISO 31000:2009 devido à necessidade de harmonização dos padrões, regulamentações e estruturas de recomendações feitas por normas anteriores, entretanto por ser um modelo generalista que visa propor diretrizes para a gestão de todos os tipos de riscos, alguns estudiosos criticaram severamente seus conceitos e recomendações. Em 2018, a ISO lançou uma versão mais atualizada da norma (ISO 31000:2018), com o intuito de solucionar algumas inconsistências existentes na anterior. Na literatura consultada, identificou-se diversas aplicações da ISO 31000 em modelos de gerenciamento de riscos de variados segmentos empresariais, e mesmo contendo alguns pontos a ser melhorados, conclui-se que as recomendações realizadas por esta norma são de grande relevância para ter-se como base na construção do processo de um modelo de gestão de riscos. (Santos, 2021, p. 1)

Embora não seja uma norma certificável, a ISO 31000 serve como referência de boas práticas, sendo amplamente adotada por organizações que buscam aprimorar a qualidade de seu processo decisório e aumentar a confiança de seus stakeholders.

O modelo COSO ERM (2017) – Enterprise Risk Management: Integrating with Strategy and Performance, publicado em 2017 pelo Committee of Sponsoring Organizations of the Treadway Commission —, representa uma das referências mais consolidadas para a gestão de riscos corporativos. Originalmente publicado em 2004, o framework foi revisado em 2017 para incorporar a integração mais explícita entre a gestão de riscos, a estratégia e o desempenho organizacional.

O COSO ERM (2017) é organizado em cinco componentes interrelacionados: Governança e Cultura; Estratégia e Definição de Objetivos; Identificação e Avaliação de Riscos; Resposta ao Risco; e Monitoramento, Revisão e Comunicação. Seu diferencial reside na visão holística dos riscos, no alinhamento com o planejamento estratégico e no foco na criação de valor para as organizações e seus stakeholders.

2.6 Benefícios da gestão de risco empresarial

A implementação estruturada da gestão de riscos proporciona um conjunto expressivo de benefícios às organizações. Conforme o COSO (2017), a gestão de riscos contribui diretamente para a criação, preservação e geração de valor, enquanto a ABNT NBR ISO 31000 (2018) destaca que esse processo melhora o desempenho organizacional, estimula a inovação e qualifica a tomada de decisão.

Entre os principais benefícios identificados na literatura, destacam-se: (a) a antecipação e mitigação de riscos, com desenvolvimento de estratégias preventivas que fortalecem a resiliência organizacional; (b) a melhoria na tomada de decisão, com base em informações estruturadas e análises de cenários; (c) a redução de perdas financeiras por meio da identificação e controle de riscos operacionais, estratégicos e financeiros; (d) o fortalecimento dos controles internos, resultando em processos mais seguros e eficientes; (e) o aumento da competitividade, pela maior capacidade de adaptação às mudanças do ambiente; (f) a melhoria da governança corporativa, com promoção de transparência e responsabilidade; (g) a proteção da imagem e reputação institucional; (h) o suporte à continuidade do negócio em cenários adversos; (i) a identificação de oportunidades estratégicas de crescimento; e (j) a melhoria do desempenho organizacional global, com maior alinhamento entre estratégia, processos e resultados.

Para Kahneman (2012), a respeito da melhoria na tomada de decisão, afirma que decisões baseadas em intuição são frequentemente influenciadas por vieses cognitivos. A gestão de riscos deve não seguir

obviamente esta linha, mas estruturar informações e cenários. A gestão de riscos, ao estruturar informações e cenários, oferece um contraponto racional a essas distorções, qualificando o processo decisório.

2.7 Desafios da implementação da gestão de riscos empresarial

A respeito dos inúmeros benefícios, a implementação da gestão de risco empresarial enfrenta obstáculos relevantes, de natureza cultural, estrutural e humana.

Segundo o COSO (2017) e a ABNT NBR ISO 31000 (2018), esses desafios devem ser reconhecidos e tratados de forma proativa para que a gestão de riscos seja efetiva.

Entre os principais desafios, identificam-se: (a) a resistência à mudança, comum entre os colaboradores, que pode dificultar a adoção de novos processos; (b) a ausência de uma cultura organizacional orientada à prevenção, que leva à percepção equivocada da gestão de riscos como burocracia; (c) a carência de profissionais capacitados para aplicar corretamente as metodologias; (d) a dificuldade na identificação e mensuração dos riscos, em razão de limitações de dados e ferramentas; (e) a falta de comprometimento da alta gestão, sem o qual a gestão de riscos tende a ser ineficaz; (f) os custos de implementação, as vezes mudanças na estrutura, maquinários, entre outros exigem investimentos altos para pequenas de pequeno porte; (g) a integração insuficiente com os processos organizacionais, tornando a gestão de riscos um processo isolado; (h) a dificuldade de manutenção do monitoramento contínuo; (i) o excesso de burocracia quando a implementação é mal conduzida; e (j) falhas de comunicação que comprometem a efetividade do processo.

Conforme observam os autores: Mintzberg, Ahlstrand e Lampel (2010), a resistência à mudança por parte dos colaboradores é a mais frequente. A implementação de novas estratégias frequentemente esbarra em resistências culturais enraizadas na rotina dos colaboradores, pois, as próprias organizações tendem a preservar rotinas estabelecidas mesmo diante de evidências de que elas não são mais adequadas.

O enfrentamento desses desafios requer comprometimento da liderança, investimento em capacitação, desenvolvimento de uma cultura de riscos e integração da gestão de riscos à rotina organizacional em todos os seus níveis.

3. CONCLUSÃO

A gestão de risco empresarial constitui uma estratégia competitiva para o sucesso das organizações em contextos marcados por constantes transformações e incertezas. Ao longo deste artigo, foram

apresentados os principais fundamentos teóricos, processos, ferramentas e modelos associados a essa área, evidenciando sua centralidade na gestão estratégica contemporânea. Os resultados da análise bibliográfica indicam que a identificação, avaliação e tratamento adequados dos riscos não apenas contribuem para a mitigação de impactos negativos, mas também favorecem a geração de valor e o fortalecimento da posição competitiva das organizações. A adoção de modelos reconhecidos internacionalmente, como a ABNT NBR ISO 31000 (2018) e o COSO ERM (2017), representa um caminho consistente para a padronização e qualificação das práticas de gestão de riscos. É importante reconhecer que a implementação da gestão de riscos não é isenta de desafios. Resistências culturais, limitações técnicas e restrições de recursos podem comprometer sua efetividade. Contudo, quando conduzida com apoio da alta gestão, alinhamento estratégico e visão sistêmica, a gestão de riscos confere às organizações maior segurança, eficiência e capacidade adaptativa.

Concluímos que a gestão de riscos pode ser melhor definida como um processo contínuo, integrado à cultura e à estratégia organizacional, e não como uma iniciativa pontual ou reativa. Nesse sentido, o desenvolvimento de futuras pesquisas empíricas sobre a aplicação desses modelos em organizações de diferentes portes e setores poderá ampliar o conhecimento sobre os fatores de risco mais críticos ou de oportunidades de sucesso para o empresarial brasileiro.

REFERÊNCIAS BIBLIOGRÁFICAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO 31000: gestão de riscos – diretrizes**. 2. ed. Rio de Janeiro: ABNT, 2018.

BARALDI, Paulo. **Gerenciamento de riscos empresariais**. Rio de Janeiro: Elsevier, 2005.

COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION (COSO). **Enterprise risk management: integrating with strategy and performance**. New York: COSO, 2017.

CHIAVENATO, Idalberto. **Planejamento estratégico**. 3. ed. Barueri: Manole, 2014.

FREEMAN, R. Edward. **Strategic management: a stakeholder approach**. Boston: Pitman, 1984.

HUBBARD, Douglas W. **The Failure of Risk Management: Why It's Broken and How to Fix It**. Hoboken, New Jersey: John Wiley & Sons, 2009. 1ª Edição.

KAHNEMAN, **Daniel. Rápido e devagar: duas formas de pensar**. Tradução de Cássio de Arantes Leite. Rio de Janeiro: Objetiva, 2012.

MINTZBERG, Henry; AHLSTRAND, Bruce; LAMPEL, Joseph. **Safári de estratégia: um roteiro pela selva do planejamento estratégico**. 2. ed. Porto Alegre: Bookman, 2010.

SANTOS, T. J. **Gestão de riscos e a norma ISO 31000: uma abordagem literária**. Management Journal, v. 3, n. 1, p. 1-14, 2021. Online disponível em DOI: http://doi.org/10.6008/CBPC2674-6417.2021.001.0001. Acessado em 12 de junho de 2026.