Gerenciando riscos corporativos: Uma análise da taxonomia de Kaplan e Mikes

William Donizete Carvalho[1]
[1]Programa de Pós-Graduação em Governança Corporativa pela FMU|UNIFESP
wmvg.carvalho@gmail.com

Dilton Andrade Costa[1]
dilton.andrade@gmail.com

Prof. Dr. Leonardo Fabris Lugoboni[1,2]
[2]Programa de Pós-Graduação em em Contabilidade pela FECAP
leonardo.lugoboni@unifesp.br

Recebido em: 16/10/2025 | Aceito em: 30/10/2025 | Publicado em: 31/12/2025

Resumo: A gestão de riscos corporativos evoluiu de uma função isolada para um processo integrado e estratégico central à governança contemporânea. Este artigo propõe uma estrutura analítica para classificar e gerenciar riscos com base na taxonomia de Kaplan e Mikes, distinguindo riscos preveníveis, estratégicos e externos. Argumenta-se que cada categoria exige abordagens, instrumentos e sistemas de controle específicos, evitando soluções uniformes. O estudo discute o papel do Escritório de Gestão de Riscos como mecanismo de coordenação organizacional, bem como a atuação do Chief Risk Officer na integração do ERM à tomada de decisão. Também analisa distintas concepções de risco presentes na literatura e suas implicações gerenciais. Os resultados indicam que uma gestão diferenciada dos riscos melhora a alocação de recursos, fortalece a capacidade de antecipação e resposta a ameaças e contribui para maior resiliência e qualidade da governança corporativa. Esses achados dialogam com os princípios do ODS 8, ao promover a sustentabilidade e a estabilidade das empresas.

Palavras-chave: Gerenciamento de Riscos Corporativos; Taxonomia de Riscos; Governança Corporativa; Chief Risk Officer; Escritório de Gestão de Riscos

Abstract: Corporate risk management has evolved from an isolated function into an integrated and strategic process central to contemporary governance. This article proposes an analytical framework to classify and manage risks based on the taxonomy of Kaplan and Mikes, distinguishing preventable, strategic, and external risks. It argues that each category requires distinct approaches, tools, and control systems, avoiding one size fits all solutions. The study discusses the role of a Risk Management Office as a mechanism for organizational coordination, as well as the contribution of the Chief Risk Officer in integrating ERM into decision making. It also examines different conceptions of risk in literature and their managerial implications. The findings indicate that a differentiated approach to risk management improves resource allocation, strengthens the ability to anticipate and respond to threats, and contributes to greater resilience and higher quality corporate governance. These insights align with the principles of SDG 8 by promoting the sustainability and stability of companies.

Keywords: Corporate Risk Management; Risk Taxonomy; Corporate Governance; Chief Risk Officer; Office Risk Management

Resumén: La gestión de riesgos corporativos ha evolucionado de una función aislada a un proceso integrado y estratégico central para la gobernanza contemporánea. Este artículo propone un marco analítico para clasificar y gestionar riesgos basado en la taxonomía de Kaplan y Mikes, distinguiendo riesgos prevenibles, estratégicos y externos. Se argumenta que cada categoría requiere enfoques, herramientas y sistemas de control diferenciados, evitando soluciones uniformes. El estudio analiza el papel de una Oficina de Gestión de Riesgos como mecanismo de coordinación organizacional, así como la contribución del Chief Risk Officer en la integración del ERM en la toma de decisiones. También examina distintas concepciones de riesgo presentes en la literatura y sus implicaciones gerenciales. Los resultados indican que una gestión diferenciada de los riesgos mejora la asignación de recursos, fortalece la capacidad de anticipar y responder a amenazas y contribuye a una mayor resiliencia y calidad de la gobernanza corporativa. Estos hallazgos.

Palabras clave: Gestión de Riesgos Corporativos; Taxonomía de Riesgos; Gobernanza Corporativa; Chief Risk Officer; Oficina de Gestión de Riesgos

1. Introdução

A gestão de riscos corporativos (*Enterprise Risk Management* - ERM) representa uma das mais significativas evoluções no ambiente empresarial contemporâneo. Tradicionalmente concebida como uma função reativa e desconectada da estratégia organizacional, a gestão de riscos transformou-se em um processo integrado e estratégico, essencial para a governança corporativa moderna (Nocco & Stulz, 2022). Entretanto, o uso de uma abordagem única para todos os tipos de risco ainda é identificado como prática comum em muitas organizações, podendo resultar em gestão ineficaz e na alocação indevida de recursos (Kaplan & Mikes, 2011a). A relevância dessa problemática é amplificada por desastres corporativos recentes que demonstraram as consequências devastadoras de falhas na gestão de riscos, como o vazamento de petróleo da *BP Deepwater Horizon* em 2010 e a crise financeira global de 2007-2009 (Mikes & Kaplan, 2011b).

2. Objetivo

Este Relato Técnico tem como objetivo principal detalhar um *framework* abrangente e prático para a gestão de riscos, fundamentado na categorização proposta por Kaplan e Mikes e enriquecido por outras abordagens teóricas e empíricas da literatura acadêmica especializada. Os objetivos específicos incluem examinar a evolução epistemológica do conceito de risco e suas implicações para a prática de liderança; detalhar as três categorias de risco propostas por Kaplan e Mikes; explorar o papel e a estrutura do Escritório de Gestão de Riscos; e examinar as funções e responsabilidades do *Chief Risk Officer* em diferentes contextos organizacionais, contribuindo para o desenvolvimento sustentável das organizações (ODS 8).

3. Metodologia

Fundamentada em pesquisa bibliográfica abrangente dos artigos seminais de Kaplan e Mikes (2011a; 2011b), que propõem taxonomia categorizando riscos em três dimensões distintas: preveníveis, estratégicos e externos. A metodologia incorpora análise da evolução epistemológica do conceito de risco, examinando perspectivas ontológicas e epistemológicas que fundamentam diferentes abordagens de gestão

CC BY

(Boholm et al., 2012). O estudo analisa *frameworks* consolidados como COSO *Enterprise Risk Management*, explorando sua evolução e contribuições para integração entre controles internos e estratégia organizacional (Prewett & Terry, 2018; Udeh, 2019; Jean-Jules & Vicente, 2020). A pesquisa examina o papel do *Chief Risk Officer* e sua evolução como integrador organizacional (Liebenberg & Hoyt, 2003; Karanja & Rosso, 2017), bem como taxonomias de riscos em diferentes contextos (Carr, 1993; Bautista et al., 2016; Rabitti et al., 2024). A análise integra perspectivas sobre o Escritório de Gestão de Riscos como mecanismo coordenador (Mikes & Kaplan, 2011b).

4. Resultados

A análise revelou que a taxonomia de Kaplan e Mikes (2011a) fundamenta-se na distinção de Frank Knight entre risco mensurável e incerteza. A Categoria I (Riscos Preveníveis) compreende riscos internos controláveis que surgem dentro da organização, devendo ser eliminados. As empresas implementam procedimentos operacionais padronizados para reduzir a probabilidade desses riscos, sendo a auditoria interna crucial. A Categoria II (Riscos Estratégicos) representa riscos assumidos voluntariamente para gerar retornos superiores. A Categoria III (Riscos Externos) abrange eventos além do controle organizacional, incluindo desastres naturais, pandemias e crises econômicas. A gestão requer visão de risco baseando-se em experiência para criar modelos mentais, conforme demonstra a Figura 1.

Figura 1

RISCOS	MENSURABILIDADE	COMPREENSÃO	ABORDAGENS DE AVALIAÇÃO DE RISCO	OBJETIVO DE MITIGAÇÃO DE RISCO	ABORDAGENS DE CONTROLE
Categoria I: Má conduta e mau comportamento de funcionários	Alta: pode mensurar probabilidade e impacto	"Conhecidos conhecidos"	Autoavaliações de controle; controles diagnósticos; coleta de dados de quase-acidentes; bancos de dados de perdas operacionais	Reduzir a incidência de ocorrência a zero	Controle interno; sistemas de limites; declarações de missão e valores; auditoria interna
Categoria II: Execução de estratégia	Média: pode estimar probabilidade e impacto	"Conhecidos desconhecidos"	Mapas de risco com escalas nominais; modelos estatísticos de estimação de risco (VaR, capital ajustado ao risco, medidas de desempenho baseadas em risco)	Reduzir probabilidade e impacto de forma custo-eficiente	Scorecards de indicadores-chave de risco; iniciativas de mitigação de risco; revisões de risco em reuniões de revisão estratégica
Categoria III: Externos, incontroláveis	Baixa: não pode mensurar ou estimar probabilidade; pode apenas prever	"Desconhecidos desconhecidos"	Visualização de risco: cenários; jogos de guerra; avaliações de "tail-risk"; modelos mentais	Reduzir impacto caso o risco ocorra	Planejamento de contingência; programas de seguro e hedge (limitados)

Categorias e Características de Risco - Kaplan & Mikes (2011a)

CC BY

O Escritório de Gestão de Riscos (ORM) emerge como inovação fundamental, podendo ser entidade centralizada (Arena et al., 2011). O ORM complementa auditoria interna, atuando como advogado do diabo com eficácia e depende da integração aos processos existentes (Mikes & Kaplan, 2011b). O *Chief Risk Officer* (CRO) evoluiu como integrador organizacional e a nomeação está relacionada às características organizacionais (Karanja & Rosso, 2017). Os modelos incluem guardião, facilitador e consultor estratégico. A Figura 2 demonstra os eventos do Escritório de Gestão de Riscos em relação às categorias de Riscos.

Figura 2

RISCOS	OBJETIVO DE MITIGAÇÃO DE RISCO	ABORDAGENS DE CONTROLE	ABORDAGENS DE AVALIAÇÃO DE RISCO	ESCRITÓRIO DE GESTÃO DE RISCOS: CONTRIBUIÇÃO	ESCRITÓRIO DE GESTÃO DE RISCOS: RELACIONAMENTO
Categoria I: Má conduta e mau comportamento de funcionários ("conhecidos conhecidos")	Reduzir a incidência de ocorrência a zero	Controle interno; sistemas de limites; declarações de missão e valores; auditoria interna	Autoavaliações de controle; controles diagnósticos; coleta de dados de quase-acidentes; bancos de dados de perdas operacionais	Coordenar ou supervisionar controles comuns com função de auditoria interna	Supervisores independentes
Categoria II: Execução de estratégia ("conhecidos desconhecidos")	Reduzir probabilidade e impacto de forma custo-eficiente	Scorecards de indicadores-chave de risco; iniciativas de mitigação de risco; revisões de risco em reuniões de revisão estratégica	Mapas de risco com escalas nominais; modelos estatísticos de estimação de risco (VaR, capital ajustado ao risco, medidas de desempenho baseadas em risco)	Realizar workshops de risco e reuniões de revisão de riscos; ajudar a desenvolver portfólio de iniciativas de risco; atuar como advogados do diabo e integradores (pensamento sistêmico)	Supervisores independentes e/ou gestores de risco integrados
Categoria III: Externos, incontroláveis ("desconhecidos desconhecidos")	Reduzir impacto caso o risco ocorra	Planejamento de contingência; programas de seguro e hedge (limitados)	Visualização de risco: cenários; jogos de guerra; avaliações de "tail-risk"; modelos mentais	Realizar exercícios de planejamento de cenários e jogos de guerra com equipe de gestão; atuar como advogados do diabo e integradores (pensamento sistêmico)	Gestores de risco integrados

O Escritório de Gestão de Riscos - Qual é o valor agregado? - Mikes & Kaplan (2011b)

5. Discussões

A percepção sobre o COSO, durante o estudo para a construção deste trabalho, indica que sua principal contribuição está intimamente relacionada com a integração entre controles internos e estratégia organizacional (Prewett & Terry, 2018). A versão mais atual, datada de 2017, apresenta visão mais ampla dos aspectos no entorno da gestão de risco. A adoção da cadeia de processos do COSO apresenta benefícios tangíveis e intangíveis, desde o fortalecimento dos controles internos, engajamento dos funcionários, maior compreensão da importância da gestão de riscos para perpetuar os negócios até a detecção de fraudes. Os artigos de Mikes e Kaplan ampliaram significativamente a compreensão sobre a gestão de riscos corporativos, propondo

CC BY

taxonomia robusta, classificando-os em três diferentes categorias (Kaplan & Mikes, 2011a).

Assumir riscos torna-se, então, uma tarefa facilitada, suportando a estratégia de crescimento da organização. Sobre taxonomias na gestão de risco, ficou evidenciado que a classificação sistemática facilita a identificação e o desenvolvimento de controles específicos para cada categoria, apoiando a decisão pelo apetite da organização de tomar riscos (Carr, 1993). As taxonomias disponíveis refletem diferentes perspectivas organizacionais e setoriais sobre natureza e impacto dos riscos. A relação entre governança corporativa e gestão de riscos constitui sinergia fundamental na qual se complementam (Arena et al., 2011). A simbiose dessa relação manifesta-se através de mecanismos independentes de supervisão e prestação de contas. Estruturas de governança corporativa eficazes proporcionam ambiente ideal para a adoção de práticas robustas de gestão de riscos, proporcionando a longevidade dos negócios.

6. Considerações finais

Este relato técnico demonstrou que a gestão de riscos corporativos transcendeu sua fase inicial como função departamentalizada. A análise de *frameworks* consolidados como COSO ERM, além da taxonomia de Kaplan e Mikes, solidifica percepção de mudança paradigmática fundamental: gestão de riscos como pilar estratégico e de geração de valor. A eficácia reside na sua natureza diferenciada e integrada, constituindo espinha dorsal que força abandono da ilusão de solução única. A implementação de Escritório de Gestão de Riscos atuando em sinergia com o papel estratégico do *Chief Risk Officer* emerge como mecanismo coordenador essencial. A relação simbiótica entre governança corporativa e gestão de riscos garante sustentabilidade organizacional (Arena et al., 2011). Conclui-se que a gestão de riscos, quando abordada de forma estratégica e culturalmente enraizada, transforma-se em vantagem competitiva, motor para inovação e escudo para resiliência organizacional.

CC BY

7. Referências

Arena, M., Arnaboldi, M., & Azzone, G. (2011). Is enterprise risk management real? Journal of Risk Research, 14(7), 779-797. https://doi.org/10.1080/13669877.2011.571775

Bautista, J. R., Juan, A. A., & Reyes, A. A. (2016). A risk taxonomy for the management of information technology projects. In 2016 IEEE Region 10 Conference (TENCON) (pp. 2774-2779). IEEE. https://doi.org/10.1109/TENCON.2016.7848546

Boholm, Å., Corvellec, H., & Karlsson, M. (2012). The practice of risk governance: lessons from the field. Journal of Risk Research, 15(1), 1-20. https://doi.org/10.1080/13669877.2011.587886

Carr, M. J. (1993). Taxonomy-Based Risk Identification (Technical Report CMU/SEI-93-TR-006). Carnegie Mellon University Software Engineering Institute.

Jean-Jules, J., & Vicente, R. (2020). Rethinking the implementation of enterprise risk management (ERM) as a socio-technical challenge. Journal of Risk Research, 24(9), 1114-1134. https://doi.org/10.1080/13669877.2020.1815595

Kaplan, R. S., & Mikes, A. (2011a). Gerenciando as múltiplas dimensões do risco: Parte I de uma série de duas partes. Balanced Scorecard Report, 13(4), 48-60.

Karanja, E., & Rosso, M. A. (2017). The Chief Risk Officer: a study of roles and responsibilities. Risk Management, 19(2), 103-130. https://doi.org/10.1057/s41283-017-0014-z

Liebenberg, A. P., & Hoyt, R. E. (2003). The determinants of enterprise risk management: Evidence from the appointment of chief risk officers. Risk Management and Insurance Review, 6(1), 37-52. https://doi.org/10.1111/1098-1616.00019

Mikes, A., & Kaplan, R. S. (2011b). Gerenciando as múltiplas dimensões do risco - Parte II: O Escritório de Gestão de Riscos. Balanced Scorecard Report, 13(5), 42-50.

Nocco, B. W., & Stulz, R. M. (2022). Enterprise risk management: Theory and practice. Journal of Applied Corporate Finance, 34(4), 8-21. https://doi.org/10.1111/jacf.12521

Prewett, K., & Terry, A. (2018). COSO's Updated Enterprise Risk Management Framework-A Quest For Depth And Clarity. Journal of Corporate Accounting & Finance, 29(3), 59-68. https://doi.org/10.1002/jcaf.22341

Rabitti, G., Khorrami Chokami, A., Coyle, P., & Cohen, R. D. (2024). A taxonomy of cyber risk taxonomies. Risk Analysis, 44(8), 1751-1761. https://doi.org/10.1111/risa.14254

Udeh, I. (2019). Observed effectiveness of the COSO 2013 framework. Journal of Accounting & Organizational Change, 16(2), 217-244. https://doi.org/10.1108/JAOC-09-2018-0091

Recebido em: *16/10/2025*
Aceito em: *30/12/2025*

CC BY