Universidade de Brasília (UnB)
Faculdade de Economia, Administração, Contabilidade e Gestão de Políticas Públicas (FACE)
Programa de Pós-Graduação em Economia (PPGECO)

Nara Cardoso de Oliveira Neto

Compliance e Gestão de Riscos:
Benefícios, Diferenças e Aplicabilidade à Universidade de Brasília

Brasília, DF
2026

Universidade de Brasília (UnB)
Faculdade de Economia, Administração, Contabilidade e Gestão de Políticas Públicas (FACE)
Programa de Pós-Graduação em Economia (PPGECO)

Compliance e Gestão de Riscos:
Benefícios, Diferenças e Aplicabilidade à Universidade de Brasília

Nara Cardoso de Oliveira Neto

Dissertação apresentada ao Programa de Pós-Graduação em Economia (PPGECO), área de concentração: Gestão de Finanças Públicas, da Faculdade de Economia, Administração, Contabilidade e Gestão de Políticas Públicas (FACE) da Universidade de Brasília (UnB) como requisito parcial à obtenção do título de Mestre em Economia.

Orientador: Prof. Dr. Alexandre Maduro de Abreu.

Brasília, DF
2026

Universidade de Brasília (UnB)
Faculdade de Economia, Administração, Contabilidade e Gestão de Políticas Públicas (FACE)
Programa de Pós-Graduação em Economia (PPGECO)

NARA CARDOSO DE OLIVEIRA NETO

Compliance e Gestão de Riscos:

Benefícios, Diferenças e Aplicabilidade à Universidade de Brasília

A Comissão Examinadora, abaixo identificada, aprova o Trabalho de Dissertação de Mestrado do Curso de Pós-Graduação *Stricto Sensu* em Economia da Universidade de Brasília.

_____

Prof. Dr. Alexandre Maduro de Abreu
Universidade de Brasília (UnB)
Orientador e Presidente da banca

_____

Prof.ª Dr.ª Milene Takasago
Universidade de Brasília (UnB)
Examinadora e Membra interna

_____

Prof. Dr. Marcelo Felipe Moreira Persegona
SENAC/DF
Examinador e Membro externo

_____

Prof. Dr. Carlos Rosano Pena
Universidade de Brasília (UnB)
Suplente

Brasília, 30 de janeiro de 2026

AGRADECIMENTOS

Primeiramente, expresso minha profunda gratidão a Deus e ao meu pai, Luiz Augusto, que sempre me incentivou a estudar. Em seus discursos, ele repetia: “Minha filha, seu diploma ninguém te toma; priorize o seu mestrado; você tomou a decisão certa ao iniciá-lo”.

Ao professor e orientador, Alexandre Maduro, sou imensamente grata pelas orientações, conselhos encorajadores e disponibilidade constante. Sua dedicação ao ensino e à pesquisa foi uma fonte inesgotável de inspiração.

Agradeço profundamente à minha filha, Alice Melgaço, minha maior motivação diária para seguir em frente. Ao meu tio Divaldo, pelo apoio incondicional desde minha entrada na faculdade; ao Carlos Cacau, pelo incentivo inicial no processo seletivo e, especialmente, pelo cuidado com Alice durante essa jornada.

Estendo meus agradecimentos à Reitoria da Universidade de Brasília, em especial à professora Márcia Abrahão Moura (reitora de 2016 a 2024), pela criação do Programa de Mestrado Profissional em Economia para servidores e ao Decanato de Orçamento, Planejamento, Avaliação e Estatísticas Institucionais (DPO), por conceder acesso às bases de dados essenciais a este trabalho. Aos membros da banca, especialmente à coordenadora Milene Takasago; aos professores do curso, em especial ao professor Lucas Vittor de Carvalho Sousa, pela paciência e ensinamentos valiosos.

À minha chefe, Marcela Barbosa, pelo apoio constante; aos colegas de trabalho, pelo companheirismo que torna o ambiente um espaço de crescimento profissional; ao Bruno Modesto, pela parceria nos desafios; ao amigo Beto, pelos dois anos de aulas compartilhadas e incentivo à conclusão; e aos colegas de sala, pelas palavras de apoio nos momentos difíceis.

Por fim, agradeço à minha família pelo amor e suporte inabaláveis ao longo dessa jornada, e a todos que, de forma silenciosa, guiaram meus passos e inspiraram minhas escolhas. Vocês foram o alicerce dessa conquista.

RESUMO

Esta dissertação tem como fundamento contribuir com a aplicação de práticas de normas pautadas em diretrizes jurídicas, observando os princípios éticos, bem como avaliar a coordenação de riscos no âmbito da Universidade de Brasília. A pesquisa faz uma análise no tocante à aplicação do programa de Compliance e Gestão de Riscos à Universidade de Brasília. A parte mais desafiadora do trabalho envolve o cálculo dos custos e os riscos e os benefícios para a UnB.

Palavras-chaves: Universidade de Brasília; UnB; Gestão de Riscos, Compliance, Governança Pública.

ABSTRACT

This dissertation aims to contribute to the application of normative practices based on legal guidelines, observing ethical principles, as well as to evaluate risk management within the University of Brasília. The research conducts a cost-benefit analysis to implement a Compliance Management program at the University of Brasília. The most challenging part of the work involves calculating the costs, risks, and benefits for UnB.

Keywords: University of Brasilia; UnB; Risk Management; Compliance, Public Governance.

.

LISTA DE FIGURAS e GRÁFICOS

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

ABBI - Associação Brasileira de Bancos Internacionais

A.E.D. - Análise Econômica do Direito

CADE - Conselho Administrativo de Defesa Econômica (

COSO - *Committee of Sponsoring Organizations of the Treadway Commission*

DOJ - *Department of Justice*

ERM - *Enterprise Risk Management*

EUA – Estados Unidos da América

FCPA - *Foreign Corrupt Practices Act*

GR - Gestão de Riscos

IFES - Instituições Federais de Ensino Superior

ISO - *International Organization for Standardization*

OCDE - Organização para a Cooperação e Desenvolvimento Econômico

OEA - Organização dos Estados Americanos

OLAF - Organismo Europeu de Luta Antifraude

PDI - Planos de Desenvolvimento Institucional

SEC - *U.S. Securities and Exchange Commission*

SOX - *Sarbanes-Oxley Act*

TCU - Tribunal de Contas da União

UnB - Universidade de Brasília

VaR - Valor em Risco

SUMÁRIO

1. INTRODUÇÃO

1.1 *Compliance*

O termo *compliance* tem origem no verbo inglês *to comply*, que significa obedecer ou estar em conformidade. No contexto organizacional, o conceito passou a representar o conjunto de práticas adotadas pelas instituições com o objetivo de assegurar o cumprimento de normas legais e regulatórias, bem como de diretrizes internas. Segundo a Associação Brasileira de Bancos Internacionais (ABBI), compliance é o dever de cumprir e fazer cumprir os regulamentos internos e externos impostos às atividades da organização, promovendo condutas éticas e íntegras no ambiente corporativo.

No setor público, a aplicação de programas de compliance tem ganhado destaque como ferramenta estratégica para a prevenção de irregularidades, o fortalecimento da integridade institucional e a promoção de uma cultura organizacional baseada na ética e na responsabilidade. Nesse contexto, a gestão de riscos surge como prática complementar, voltada à identificação, análise e mitigação de eventos que possam comprometer o alcance dos objetivos institucionais. Conforme o Tribunal de Contas da União (TCU), um processo efetivo de gestão de riscos visa garantir razoável segurança quanto à realização das metas organizacionais, contribuindo para a melhoria da governança e da prestação de contas à sociedade.

A distinção entre compliance e gestão de riscos, embora sutil, é essencial para a efetividade das políticas públicas. Enquanto o primeiro assegura o alinhamento das ações institucionais às normas legais e éticas, o segundo busca antecipar, avaliar e tratar potenciais incertezas que possam impactar negativamente os processos administrativos. Ambas as ferramentas, quando integradas de forma estratégica, fortalecem os mecanismos de controle interno e a tomada de decisão.

No âmbito da Administração Pública federal, especialmente nas Instituições Federais de Ensino Superior (IFES), a adoção dessas práticas tem se mostrado cada vez mais necessária diante das crescentes demandas por transparência, eficiência e responsabilidade na gestão dos recursos públicos. A Universidade de Brasília (UnB), nesse cenário, tem se destacado por implementar ações voltadas à conformidade normativa, à modernização de seus processos internos e ao fortalecimento de sua cultura institucional.

Diante disso, o presente estudo tem como objetivo geral analisar a aplicabilidade e os benefícios dos programas de compliance e gestão de riscos na Universidade de Brasília, destacando suas contribuições para o aprimoramento da governança pública. Como objetivos específicos, busca-se: (i) compreender os fundamentos conceituais de compliance e gestão de riscos; (ii) identificar os principais instrumentos legais que regulamentam essas práticas no setor público; (iii) avaliar o modelo atual de governança da UnB e suas iniciativas relacionadas à conformidade e ao gerenciamento de riscos; e (iv) propor recomendações para a consolidação de um programa eficaz de compliance na instituição.

A escolha da UnB como objeto de análise se justifica não apenas por sua relevância no cenário nacional da educação superior, mas também por seu protagonismo na adoção de medidas voltadas à ética institucional, à gestão responsável e ao desenvolvimento de uma imagem organizacional íntegra e confiável. O estudo pretende, ainda, contribuir para o avanço do conhecimento sobre a temática, propondo uma perspectiva inovadora sobre a aplicação do compliance no setor público, com foco na prevenção de irregularidades e no fortalecimento da cultura de integridade nas universidades federais.

A pesquisa será desenvolvida por meio de revisão bibliográfica e documental, com base em legislações, normativos institucionais, manuais técnicos e literatura especializada sobre o tema. Ao longo do trabalho, serão abordados os conceitos centrais, os marcos legais e os desafios da implementação do compliance e da gestão de riscos na administração pública, com especial atenção à experiência da Universidade de Brasília.

1.2. *Compliance*: Breve Histórico e Definições

As práticas de Compliance (que envolvem conformidade com leis, regulamentos e padrões internos) tiveram origem, especialmente nos Estados Unidos, e elas estão relacionadas ao desenvolvimento do sistema financeiro. O conceito de Compliance, como o conhecemos hoje, tem raízes em um contexto mais amplo de regulamentação e controle das instituições financeiras, com ênfase no monitoramento de suas atividades para garantir a conformidade com as leis e regulamentos vigentes.

A origem de Compliance remonta ao surgimento de várias agências regulamentadoras nos Estados Unidos. Essas agências foram criadas para supervisionar as atividades das instituições

financeiras, buscando assegurar que essas empresas seguissem as regras estabelecidas. Esse movimento foi impulsionado principalmente pelo governo norte-americano, que queria melhorar a fiscalização do setor financeiro, especialmente após a crise financeira de 1907, que revelou vulnerabilidades no sistema bancário.

O autor Manzi (2008) confirma que a origem das práticas de Compliance se deu com a criação do Banco Central Americano (*Federal Reserve*) em 1913. O objetivo inicial era estabelecer um sistema financeiro mais estável, seguro e flexível, capaz de prevenir crises e promover a confiança no sistema bancário.

De forma resumida, as práticas de Compliance começaram nas instituições financeiras dos Estados Unidos, com o intuito de tornar o sistema financeiro mais seguro e robusto, e ao longo do tempo, essas práticas se expandiram e se sofisticaram, sendo adotadas em diversas outras áreas e países.

Vamos estudar o surgimento da preocupação das empresas com os Programas de Compliance, especialmente após escândalos corporativos de grandes dimensões que impactaram a reputação e a legislação internacional.

O caso da WorldCom, nos Estados Unidos, é um exemplo de um grande escândalo financeiro que envolveu fraude contábil em larga escala. Esse escândalo foi um dos maiores escândalos corporativos da história e levou à falência da empresa. Em resposta a esse tipo de comportamento ilícito e fraudulento nas corporações, o governo dos Estados Unidos criou a Lei Sarbanes-Oxley de 2002. Essa lei visava melhorar a governança corporativa e aumentar a transparência financeira das empresas, impondo mais responsabilidades às lideranças e criando mecanismos de auditoria mais rigorosos. Assim, a preocupação com Compliance, ou conformidade com normas éticas e legais, se intensificou, pois as empresas começaram a se preocupar mais com práticas de governança e compliance para evitar fraudes e garantir a integridade nos processos financeiros.

O Caso Siemens (Alemanha): uma das maiores empresas de engenharia do mundo, que foi envolvida em um escândalo de corrupção internacional, com práticas ilegais de suborno e violações de normas de concorrência. Esse escândalo levou a Siemens a ser condenada judicialmente em vários países. A magnitude do caso gerou uma reflexão global sobre a necessidade de regulamentações e práticas de compliance, especialmente no que diz respeito à

corrupção e ao cumprimento das leis antitruste. A condenação da Siemens também demonstrou a necessidade de sistemas de controle interno e práticas empresariais responsáveis para prevenir esses tipos de condutas.

Em sintese, a preocupação com os Programas de Compliance nas empresas surgiu a partir de grandes escândalos como o da WorldCom e o da Siemens. Esses casos evidenciaram a necessidade de legislações mais rígidas e de práticas empresariais que garantissem a conformidade com as leis, prevenindo fraudes, corrupção e outras práticas ilegais que pudessem prejudicar a integridade das organizações e do mercado. Gaban e Domingues (2016, p. 344), ainda, especificam quanto à relação entre as medidas de Governança Corporativa, as leis Anticorrupção e os Programas de Compliance que:

> Esses escândalos de corrupção e fraudes financeiras, bem como a instabilidade decorrente de crises econômicas fomentaram medidas de integração supranacional dos mercados. A adoção de programas de Compliance é, então, incorporada às regras de soft law, uma vez que passa a ser recomendada por instituições internacionais como a Organização para Cooperação e Desenvolvimento Econômico (ONU) e a Organização dos Estados Americanos (OEA) (recomenda-se que os governos incentivem suas empresas a desenvolver controles internos adequados, programas de ética e Compliance ou medidas para prevenir ou detectar infrações) [Good Practice Guidance on Internal Controls, Ethics, and Compliance Adopted 18 February 2010 This Good Practice Guidance was adopted by the OECD Council as an integral part of the Recommendation of the Council for Further Combating Bribery of Foreign Public Officials in International Business Transactions of 26 November 2009].

1.3. *Compliance* como instrumento de políticas públicas

A governança pública contemporânea enfrenta desafios crescentes relacionados à corrupção, à ineficiência administrativa e à perda de confiança social nas instituições estatais. Nesse contexto, o compliance emerge como instrumento estratégico para alinhar condutas organizacionais aos princípios éticos, legais e regulatórios, promovendo uma gestão pública mais responsável e eficaz.

Conforme destaca Di Pietro (2019, p. 456), “a governança moderna exige mecanismos de controle interno que transcendam a mera legalidade formal, incorporando a probidade como dever funcional”. O conceito de compliance, originário do direito anglo-saxão e incorporado ao ordenamento brasileiro, especialmente a partir da Lei n. 12.846/2013 (Lei Anticorrupção), refere-se à adoção de políticas e procedimentos internos para prevenir, detectar e remediar atos ilícitos.

Na esfera pública, sua aplicação ultrapassa a lógica do setor privado, integrando-se aos pilares de governança definidos pelo Tribunal de Contas da União, como transparência, accountability (responsabilidade) e controle social (TCU, 2016). Assim, busca-se demonstrar como o compliance fortalece a governança pública, com ênfase na realidade brasileira.

1.4. Evolução conceitual e normativa

O *compliance* evoluiu de prática corporativa para imperativo também na esfera pública, impulsionado por escândalos como o Mensalão e a Operação Lava Jato, que expuseram fragilidades sistêmicas na administração. Em perspectiva internacional, a OCDE (2009, p. 23) enfatiza que "programas de compliance são essenciais para restaurar a confiança nas instituições públicas, alinhando-as a padrões globais de integridade".

No Brasil, a Lei n. 12.846/2013 estabelece a responsabilidade objetiva de pessoas jurídicas por atos lesivos, incentivando a implementação de programas de integridade. O Decreto n. 8.420/2015 regulamenta esses programas, definindo elementos mínimos como código de ética, canais de denúncia e auditorias internas. Ademais, a Resolução TCU n. 259/2016 orienta órgãos públicos a adotarem práticas de integridade para aprimorar controles internos, ecoando Bandeira de Mello (2021, p. 789), que defende "o controle preventivo como antídoto à discricionariedade abusiva".

1.5. *Compliance* versus Governança: Interseções e Diferenças

A governança pública, conforme Bovaird, Loeffler e Van Ryzin (2017, p. 12), envolve redes de atores públicos, privados e sociedade civil para decisões coletivas mais eficientes. O compliance atua como ferramenta operacional dessa governança, materializando princípios constitucionais como legalidade e moralidade administrativa. Medauar (2018, p. 112) reforça que "a accountability não é mero formalismo; exige mecanismos como o compliance para tornar os agentes públicos responsáveis por seus atos". A tabela a seguir ilustra como o compliance operacionaliza a governança, transformando abstratos princípios em práticas concretas.

Quadro 1. Relação entre Elementos da Governança Pública e Funções do Compliance

Elemento de Governança	Função do Compliance	Exemplo de Aplicação Pública	Referência

Transparência	Divulgação de políticas e relatórios	Portais de integridade em ministérios	OCDE (2009)
Accountability	Canais de denúncia e sanções internas	Ouvidorias com proteção ao denunciante	Medauar (2018)
Controle Interno	Auditorias e treinamentos	Monitoramento de licitações via sistemas automatizados	TCU (2016)
Participação Social	Consultas públicas em códigos éticos	Engajamento de ONGs em avaliações de risco	Bovaird et al. (2017)

Fonte: elaborado pela autora

1.6. Estrutura de um Programa de *Compliance* Público

Um programa eficaz de compliance público deve ser tailor-made, adaptado à realidade do órgão. Seus pilares fundamentais incluem: **Avaliação de riscos:** identificação de vulnerabilidades, como fraudes em contratações. Ferramentas como matrizes de risco, baseadas na ISO 37001, são consideradas essenciais. Hood (1991, p. 5), na tradição do *New Public Management*, enfatiza que "controles inteligentes previnem falhas sistêmicas"; **Código de conduta e treinamentos:** capacitações obrigatórias para servidores, incluindo simulações de dilemas éticos e situações práticas do cotidiano administrativo; **Mecanismos de monitoramento:** utilização de tecnologias (*big data, analytics*) para análise de licitações, a exemplo de plataformas como o sistema Compras.gov.br; **Cultura de integridade:** liderança comprometida (*tone at the top*), com o dirigente máximo atuando como patrocinador do programa.

Estudos da Controladoria-Geral da União indicam que órgãos com programas de integridade maduros reduzem de forma significativa os casos de irregularidades detectados em auditorias (CGU, 2022).

1.7. Casos Práticos no Brasil

A implementação de *compliance* na Petrobras no período pós-Lava Jato exemplifica o impacto dessas medidas. O programa de integridade da estatal, posteriormente reconhecido em

premiações, incluiu due diligence em fornecedores, canais de denúncia (*whistleblower channels*) e aprimoramento dos controles internos, contribuindo para a recuperação de ativos via acordos de leniência. Di Pietro (2019, p. 502) ressalta que “a integridade corporativa no setor público é o calcanhar de Aquiles da corrupção endêmica”.

No âmbito federal, o então Ministério da Economia adotou, em 2019, programa de integridade integrado ao Sistema de Correição. Dados divulgados pela CGU apontam queda relevante na quantidade de processos disciplinares após a implementação do programa (CGU, 2024).

1.8. Desafios e Perspectivas para o *Compliance* Público

Apesar dos avanços, persistem obstáculos, notadamente a resistência cultural de segmentos da burocracia tradicional, que muitas vezes veem o compliance apenas como “mais uma fiscalização” (Bandeira de Mello, 2021, p. 812). Somam-se a isso a escassez de recursos para tecnologia e a fragmentação da coordenação entre CGU, TCU e Ministério Público Federal. Pesquisas de Abrucio (2020) apontam que parcela expressiva dos programas públicos permanece em estágio incipiente em razão desses fatores.

1.9. Recomendações e Inovações

Para superar tais desafios, recomenda-se a integração obrigatória do compliance nos planos de gestão anual, o uso de inteligência artificial para detecção preditiva de fraudes, parcerias público-privadas para capacitação e a adoção de métricas de maturidade (como modelos inspirados no CMMI). Em perspectiva futura, vislumbra-se um “Compliance 4.0”, incorporando critérios ESG à governança pública, alinhado à visão de Bovaird *et al*. (2017).

O compliance consolida-se como instrumento indispensável de governança pública, promovendo integridade e eficiência em um cenário de escassez de recursos e alta demanda por legitimidade. Sua adoção estratégica não apenas mitiga riscos, mas eleva a capacidade estatal de entregar valor público, como sintetiza Medauar (2018, p. 150): "A verdadeira governança reside na prevenção ética".

2. REFERENCIAL TEÓRICO

O referencial teórico dessa pesquisa tem o objetivo de aprofundar as regras do Compliance e Gestão de Riscos, bem como as diferenças, benefícios e aplicabilidade na Universidade de Brasília. Sendo assim, o referencial teórico foi projetado da seguinte forma: Compliance e Gestão de Riscos.

2.1. Compliance

O termo *Compliance* provém do inglês "comply", que significa "cumprir, obedecer, "estar de acordo" ou "em conformidade".Compliance é um conjunto de práticas e políticas que asseguram que a empresa está em conformidade com a lei, regulamentos, normas e padrões éticos, que abrangem uma empresa, um determinado setor da economia ou uma instituição.

Para Gabardo e Castella (2015), o *Compliance* surge como uma proposta nova de minimização dos riscos da sociedade moderna e contemporânea. Para Rotsch (2012), o termo é relativamente novo e, muitas vezes, é analisado e incluído em discussões próprias do Direito Penal Econômico. Ainda de acordo com Rotsch (2012), Compliance se apresenta como um novo objeto de estudo da ciência jurídica, sendo que os esforços devem ser concentrados no sentido de discutir as questões que resultam precisamente da necessidade de antecipar riscos que podem culminar na responsabilidade penal bem como em sua atuação preventiva.

O desafio do compliance é alinhar valores e mitigar riscos relacionados às condutas antiéticas dos profissionais, tendo impactos positivos na imagem organizacional, no ambiente de trabalho, na motivação dos profissionais e na perenidade das Organizações (Santos; Hoyos; Amorim, 2013). Destaca-se a importância de prevenir uma série de crimes que podem comprometer a integridade e a ética nas atividades empresariais e financeiras. Vamos analisar cada um desses crimes abaixo:

1. Corrupção: Refere-se ao ato de oferecer, dar, receber ou solicitar algo de valor como influência em ações de uma pessoa em posição pública ou privada. A prevenção da corrupção é essencial para garantir a transparência e a justiça nas relações comerciais.

2. Lavagem de dinheiro: Este crime envolve disfarçar a origem de dinheiro obtido de forma ilícita, tornando-o aparentemente legítimo. A prevenção é crucial para manter a integridade do sistema financeiro.

3. Formação de cartel: Trata-se de um acordo entre empresas para fixar preços, limitar a produção ou dividir mercados, prejudicando a concorrência. Evitar cartéis é fundamental para garantir um mercado justo e competitivo.

4. Financiamento ao terrorismo: Refere-se ao ato de fornecer apoio financeiro a atividades terroristas. A prevenção é vital para a segurança pública e a estabilidade social.

5. Violações contábeis e tributárias: Envolvem práticas fraudulentas que distorcem a realidade financeira de uma empresa, como sonegação de impostos ou manipulação de registros contábeis. A prevenção ajuda a manter a conformidade legal e a confiança dos investidores.

6. Negociação com informações privilegiadas: Este crime ocorre quando alguém utiliza informações não públicas para obter vantagem em transações financeiras. A prevenção é importante para garantir a equidade no mercado de ações.

7. Delitos ambientais: Envolvem ações que causam danos ao meio ambiente, como poluição ou exploração irresponsável de recursos naturais. A prevenção é essencial para proteger o planeta e promover a sustentabilidade.

8. Quebra de segredos comerciais: Refere-se à divulgação não autorizada de informações confidenciais que podem prejudicar uma empresa. Proteger esses segredos é fundamental para a competitividade e a inovação.

Em resumo, a meta de evitar esses crimes é fundamental para promover um ambiente de negócios ético, seguro e sustentável, garantindo a confiança de consumidores, investidores e da sociedade em geral.

O conceito de *Compliance*, segundo Coimbra e Manzi (2010), começou a se consolidar nas instituições financeiras, mas ganhou força significativa após uma série de escândalos globais relacionados à governança corporativa. Os exemplos citados por eles, como os casos da Barings, Enron, WorldCom e Parmalat, foram eventos que expuseram falhas graves de controle e conduta dentro das empresas, o que gerou uma pressão global por práticas empresariais mais

transparentes e éticas.

Esse movimento de fortalecimento do *Compliance* também foi influenciado pela crise financeira de 2008, que revelou a fragilidade de sistemas financeiros e a necessidade de uma fiscalização mais rígida para evitar fraudes, corrupção e outros comportamentos ilícitos no mundo corporativo. Para implementar esse movimento de melhoria na governança, as instituições internacionais desempenharam um papel importante, emitindo uma série de documentos e recomendações que incentivavam as empresas a adotar políticas de Compliance mais robustas. Silveira e Saad-Diniz (2012) destacam que essas orientações ajudaram a impulsionar a ideia de que as empresas precisavam se estruturar internamente para monitorar e controlar suas operações, prevenindo riscos jurídicos e financeiros.

Além disso, vários países passaram a criar legislações que obrigavam as empresas a elaborar e implementar ferramentas de monitoramento interno. Essas ferramentas visam garantir que as práticas empresariais estejam em conformidade com a legislação vigente, prevenindo a ocorrência de atos ilícitos como corrupção, fraude e lavagem de dinheiro, além de promover uma cultura organizacional ética.

Em resumo, o conceito de Compliance evoluiu de uma necessidade das instituições financeiras para um movimento global que visa a integridade e a transparência nas empresas, sendo consolidado tanto por regulamentações internacionais quanto por legislações nacionais. Diante disso, foram elaborados Programas de Compliance em diferentes áreas de atuação de uma empresa, com o objetivo de garantir que a organização atenda às normas e legislações específicas em cada uma dessas áreas e, assim, evitar infrações. Vamos avaliar as cinco áreas específicas para as quais foram criados programas de compliance:

***Compliance* Anticorrupção:** Tem como objetivo garantir que a empresa esteja em conformidade com a Lei Anticorrupção, que busca prevenir a prática de corrupção dentro das empresas, como suborno, fraude e outros atos ilícitos.

***Compliance* Antitruste:** Foca no cumprimento da Lei de Defesa da Concorrência, que regula práticas anticoncorrenciais, como cartel, abuso de poder econômico e outras ações que possam prejudicar a livre concorrência no mercado.

***Compliance* Ambiental:** Relacionado à Política Nacional do Meio Ambiente, que visa à proteção do meio ambiente e regula atividades empresariais que possam causar danos ao meio

ambiente, como poluição, desmatamento e exploração ilegal de recursos naturais.

***Compliance* Trabalhista:** Visa assegurar que a empresa cumpra as normas da Consolidação das Leis do Trabalho (CLT), evitando práticas ilegais relacionadas ao trabalho, como exploração de mão de obra, condições de trabalho inadequadas, entre outros.

***Compliance* do Consumidor:** Refere-se à conformidade com o Código de Defesa do Consumidor (CDC), que protege os direitos dos consumidores e regulamenta práticas empresariais voltadas ao atendimento adequado e ético dos consumidores, evitando fraudes ou práticas enganosas.

O principal objetivo desses programas é prevenir infrações legais que possam ocorrer devido à não conformidade com as respectivas legislações mencionadas. Dessa forma, a empresa evita riscos jurídicos, financeiros e de reputação que poderiam surgir caso não cumprisse as leis e regulamentos aplicáveis. Em resumo, destaca-se a importância dos programas de compliance como ferramentas de prevenção a infrações legais específicas em diferentes áreas de atuação de uma empresa, visando a conformidade com as leis vigentes e a manutenção da integridade da organização.

2.2. A Lei Anticorrupção Brasileira (Lei nº 12.846/2013)

A Lei nº 12.846/13, também conhecida como Lei Anticorrupção ou Lei da Empresa Limpa, foi sancionada em 1º de agosto de 2013 e entrou em vigor em janeiro de 2014. Ela representa um marco importante no combate à corrupção no Brasil, principalmente ao estabelecer a responsabilidade civil e administrativa das pessoas jurídicas por atos de corrupção praticados contra a administração pública, tanto nacional quanto estrangeira. Para Jordace (2017), a edição da Lei 12.846/2013 objetivou gerar meios para assegurar a indenização de potenciais danos ocasionados por tais atos praticados por empresários no desempenho de suas atividades empresariais.

Cumpre destacar que, nos termos do Parágrafo Único do Art. 7º, da Lei n°. 12.846/1315, é a Administração Pública quem define a existência efetiva e os parâmetros de avaliação dos Programas de Compliance, através de regulamento do Poder Executivo Federal. (Carvalhosa, 2015, p. 331). Diante dessas influências internacionais e da pressão para melhorar as práticas

anticorrupção, o Brasil promulgou sua própria legislação em 2013, com o objetivo de responsabilizar as empresas por atos de corrupção, independentemente de a ação ter sido cometida por seus funcionários ou representantes. Principais pontos da Lei nº 12.846/2013:

Responsabilidade das Pessoas Jurídicas: A lei estabelece que as empresas podem ser responsabilizadas administrativamente e civilmente por atos de corrupção, como o pagamento de subornos a funcionários públicos, tanto no Brasil quanto no exterior.

Sanções: As empresas podem sofrer pesadas sanções, como multas, perda de bens, suspensão de atividades e até a proibição de firmar contratos com o poder público.

Programas de *Compliance*: A lei também estimula as empresas a implementarem programas de compliance eficientes como forma de mitigar os riscos de corrupção e, se comprovado que a empresa possui um programa eficaz, isso pode ser considerado para atenuar a pena.

Em síntese, a criação da Lei nº 12.846/2013 foi uma resposta às tendências globais de reforço das legislações anticorrupção e à necessidade de o Brasil atender a compromissos internacionais. A lei reflete as influências do FCPA, do Bribery Act e das convenções da ONU e OEA, e é um passo importante para aumentar a transparência e combater a corrupção no setor público e privado no Brasil. Entre os principais aspectos da lei anticorrpução, têm-se:

Responsabilização das Pessoas Jurídicas: A lei introduz, no sistema jurídico brasileiro, a possibilidade de responsabilização direta das empresas por corrupção, uma mudança significativa em relação à legislação anterior, que focava principalmente na responsabilização de indivíduos. Ou seja, as empresas podem ser punidas por atos de corrupção cometidos por seus empregados, representantes, ou quaisquer pessoas que agem em nome da empresa, mesmo que esses atos não tenham sido praticados com o consentimento da alta administração da empresa.

Atos de Corrupção: São considerados atos de corrupção aqueles que envolvem o pagamento de subornos ou outras vantagens indevidas a funcionários públicos, tanto nacionais quanto estrangeiros. Isso significa que a empresa pode ser responsabilizada por atos de corrupção que ocorram no Brasil ou em outros países.

Fomento a Práticas Éticas no Mercado: A principal meta da lei é promover uma mudança de cultura dentro das empresas, incentivando um padrão de mercado mais ético e

transparente. Para isso, a lei cria incentivos para que as empresas adotem boas práticas empresariais e políticas de compliance, ou seja, sistemas internos de controle que busquem prevenir e detectar atos ilícitos, como a corrupção.

A legislação visa também melhorar a imagem do Brasil no cenário internacional, ao alinhar o país a práticas globais de combate à corrupção, como as já adotadas por outras legislações de destaque, como o *Foreign Corrupt Practices Act* (FCPA) dos EUA e o *Bribery Act* do Reino Unido.

2.3. Incentivos para adoção de programas de *compliance*

A lei prevê que as empresas que adotarem programas eficazes de prevenção à corrupção podem ser beneficiadas com redução de multa caso venham a ser processadas por corrupção. Esses programas de compliance incluem a implementação de políticas internas, treinamentos, auditorias e mecanismos de denúncia.

O incentivo é uma forma de estimular que as empresas não apenas evitem práticas corruptas, mas que também ajudem a criar uma cultura de compliance dentro de suas operações, promovendo uma governança mais responsável.

2.4. Acordos de Leniência

Outro ponto importante da Lei Anticorrupção é a previsão da cooperação com as autoridades para o esclarecimento de infrações e a punição dos responsáveis. As empresas que se mostram dispostas a colaborar com as investigações podem firmar acordos de leniência com as autoridades.

Por meio desses acordos, a empresa pode reduzir a pena ou até evitar punições mais severas, desde que cooperem ativamente nas investigações, fornecendo informações úteis para a descoberta de outros envolvidos ou a comprovação dos ilícitos. O acordo de leniência tem o objetivo de incentivar a autodenúncia e a colaboração, ajudando na descoberta e prevenção de outros atos de corrupção.

2.5. Sanções para as Empresas

Quando uma empresa é responsabilizada por atos de corrupção, ela pode sofrer uma série de sanções, incluindo multas de até 20% do faturamento bruto anual da empresa no exercício anterior à infração. Além disso, as empresas podem ser suspensas de contratar com o poder público, ter bens e valores sequestrados, e até ser proibidas de receber incentivos fiscais.

A lei também permite que, ao ser punida, a empresa tenha a oportunidade de mitigar suas penas, especialmente se demonstrar que adotou medidas para prevenir a corrupção e colaborou com as investigações. Objetivos da Lei Anticorrupção:

Prevenção e Combate à Corrupção: A principal intenção da lei é evitar a ocorrência de atos de corrupção no Brasil, responsabilizando as empresas e incentivando-as a adotar comportamentos éticos.

Melhoria da Governança Corporativa: A lei visa promover uma cultura empresarial mais transparente e responsável, contribuindo para um mercado mais ético.

Alinhamento Internacional: O Brasil, ao adotar uma legislação robusta de combate à corrupção, alinha-se com os compromissos internacionais, mostrando seu comprometimento com as práticas de governança e o combate à corrupção globalmente.

Podemos concluir, que a Lei nº 12.846/13 (Lei Anticorrupção) é uma das ferramentas mais poderosas que o Brasil tem para combater a corrupção no setor privado. Ela responsabiliza as empresas, oferece incentivos para boas práticas e cria mecanismos de colaboração com as autoridades para detectar e prevenir atos ilícitos. Através da introdução de programas de compliance e da possibilidade de acordos de leniência, a lei busca criar um novo padrão ético no mercado, beneficiando tanto o ambiente corporativo quanto a sociedade em geral.

A Lei Anticorrupção (Lei nº 12.846/2013), também conhecida como "Lei da Empresa Limpa", tem como objetivo principal a responsabilização de pessoas jurídicas pela prática de atos de corrupção, tanto em relação ao setor público quanto ao privado. Ela busca estabelecer mecanismos de prevenção e punição de práticas corruptas, criando um sistema de responsabilização objetiva das empresas, com implicações tanto administrativas quanto judiciais.

Silvio de Salvo Venosa (2014), renomado jurista brasileiro, comenta que a Lei Anticorrupção "constitui um marco na história do direito penal empresarial no Brasil, ao impor uma nova perspectiva de responsabilização das pessoas jurídicas". Segundo ele, a implementação de políticas internas de compliance nas empresas é essencial para evitar que atos de corrupção aconteçam, visto que a responsabilidade das empresas é objetiva.

Para Tércio Sampaio Ferraz Júnior (2015), jurista e professor, a lei reflete a necessidade de adaptação do Brasil a um contexto internacional de combate à corrupção. Ele destaca a importância de um controle mais rigoroso sobre as ações das empresas, com a responsabilização das mesmas quando envolvidas em práticas de corrupção.

Por fim, a Lei Anticorrupção não se limita a punir práticas ilícitas, mas busca, principalmente, criar uma cultura de prevenção, transparência e compliance, ampliando a fiscalização e responsabilização das empresas para que atuem de maneira ética e legal.

2.6. *Compliance* sob a perspectiva da Análise econômica do direito

A teoria da Análise Econômica do Direito (A.E.D.) de Richard Posner é uma abordagem que busca integrar o Direito com a economia, aplicando conceitos e métodos econômicos para entender as regras e instituições jurídicas. Posner e outros teóricos dessa corrente defendem que as normas jurídicas não devem ser analisadas isoladamente, mas sim em um contexto que leve em consideração os incentivos, custos e benefícios que geram para os indivíduos e a sociedade.

O ponto central da A.E.D. é que o Direito deve ser compreendido como um meio para promover a eficiência econômica, ou seja, uma busca por soluções que maximizem o bem-estar social. Para Posner, a lógica econômica pode ser aplicada em diversas áreas do Direito, como contratos, responsabilidade civil, propriedade intelectual e direito penal, oferecendo uma perspectiva pragmática que visa entender as consequências econômicas das decisões jurídicas.

A crítica à ideia de completude e autonomia do Direito que você menciona está relacionada à visão tradicional que considera o Direito como uma ciência fechada, com suas próprias normas e princípios, separados de outras áreas do conhecimento. A A.E.D. refuta essa visão, argumentando que o Direito é, na verdade, uma disciplina interdependente que deve ser analisada também sob a ótica de outras ciências sociais, como a economia, a sociologia e a

psicologia.

A constante mudança das sociedades é outro ponto importante dentro da A.E.D., pois as normas jurídicas devem ser dinâmicas e adaptáveis aos novos desafios econômicos, sociais e tecnológicos. Isso significa que uma análise do Direito deve levar em conta essas transformações e os incentivos que elas geram, o que é mais fácil de fazer com uma abordagem interdisciplinar.

Dessa forma, a teoria de Posner e seus seguidores rejeita a ideia de que o Direito possa ser uma ciência exata, como as ciências naturais, pois ele está sempre sujeito a variáveis sociais, econômicas e políticas. A interdisciplinariedade proposta pela A.E.D. visa enriquecer a análise jurídica e melhorar a eficácia das normas, levando em consideração não apenas os princípios jurídicos tradicionais, mas também os aspectos econômicos das decisões e suas repercussões na sociedade.

Battesini (2011, pp. 25-26) divide a história da interação entre Direito e Economia em três estágios: precursores (período anterior à década de 1830), primeira "onda" (período de 1830 a 1930) e segunda "onda" (período posterior à década de 1930). No âmbito empresarial, todas as definições de *compliance* estão intrinsecamente relacionadas ao respeito às leis, às normas regulatórias e à adoção de uma conduta ética que reflita os valores da cultura organizacional. Tradicionalmente, esse conceito esteve fortemente vinculado à perspectiva jurídica, sendo compreendido, sobretudo, como o dever de observar e cumprir o ordenamento legal aplicável à atividade empresarial.

Contudo, essa concepção evoluiu de forma significativa nos últimos anos. A partir da consolidação de práticas mais robustas de governança corporativa e da crescente complexidade do ambiente regulatório e institucional, o *compliance* ultrapassou os limites do campo estritamente jurídico. Atualmente, sua aplicação se estende a diversas esferas da gestão empresarial, como as áreas contábil, econômica, ambiental, social e tecnológica.

Essa expansão reflete uma nova compreensão: o *compliance* não é apenas um instrumento de prevenção a riscos legais, mas também um componente estratégico da gestão organizacional, contribuindo para a sustentabilidade, a integridade e a reputação da empresa. Consequentemente, os programas de *compliance* passaram a ser desenhados de maneira mais abrangente e integrada, com o objetivo de assegurar a conformidade e a ética em todas as frentes de atuação da organização.

Segundo Vasconcelos e Soares (2022), “a maior adesão e engajamento organizacional aos comandos da liderança tornam os controles internos mais eficazes, reduzindo o número de comportamentos desviantes ou mesmo ilegais”, evidenciando que a eficácia dos programas de compliance depende de forte comprometimento gerencial. Cabe ressaltar que o objetivo inicial dos programas de compliance adotados se manteve no sentido de prevenir o cometimento às infrações em diferentes legislações, segundo Ferreira e Queiroz (2018):

> Compliance Anticorrupção pautado pela Lei Anticorrupção;
> Compliance Antitruste ou Concorrencial em consonância com a Lei de Defesa da Concorrência;
> Compliance Ambiental relacionado com a Política Nacional do Meio-Ambiente;
> Compliance Trabalhista de acordo com a Consolidação Nacional das Leis Trabalhistas e
> Compliance do Consumidor conforme o Código de Defesa do Consumidor.

Diante desse cenário, observa-se que o conceito de *compliance* passou por um processo de ampliação em sua aplicação dentro do ambiente empresarial. Ainda que sua essência — voltada à mitigação de riscos, especialmente os de natureza legal, ética e reputacional — permaneça inalterada, sua atuação tem se expandido para além do mero cumprimento de normas jurídicas. Essa evolução é reflexo da crescente complexidade organizacional e das demandas por maior transparência e responsabilidade corporativa:

> Compliance não existe apenas para assegurar que a instituição cumpra com suas obrigações regulatórias, mas também para assistir à alta administração na sua responsabilidade de observar o arcabouço regulatório e as melhores práticas na execução das estratégias e dos processos decisórios. (Candeloro; Rizzo; Pinho *apud* Silva; Covac, 2019, p. 19)

Nesse contexto, é possível afirmar que o *compliance* deixou de ser uma prática restrita a departamentos jurídicos ou regulatórios, passando a integrar outras áreas estratégicas das organizações, como finanças, sustentabilidade, recursos humanos, tecnologia da informação, entre outras. Tal movimento reforça a ideia de que a conformidade deve estar incorporada à cultura organizacional, permeando todas as instâncias da empresa.

> Não se pode confundir o compliance com o mero cumprimento de regras formais e informais, sendo o seu alcance bem mais amplo… manter-se em conformidade com as leis e padrões éticos, agindo de maneira preventiva, tentando antecipar condutas reprováveis e criando mecanismos para evitar ações que possam deixar a empresa em desconformidade. (Ribeiro; Diniz, 2015, p. 88).

Conforme exposto acima, é razoável afirmar que a tendência é de que o *compliance*

continue expandindo seu alcance, acompanhando as transformações do ambiente institucional e respondendo às novas exigências impostas por stakeholders, órgãos reguladores e pela sociedade em geral.

2.7. O *Compliance* e a Corrupção

Para compreender a crescente relevância das políticas de *compliance* nas organizações, é necessário contextualizar o cenário contemporâneo, marcado por uma maior conscientização e intolerância em relação a práticas como a corrupção, a violação de normas legais e o desrespeito aos princípios éticos. Essas questões, que outrora podiam ser tratadas com certa permissividade ou invisibilidade, passaram a ser alvo de atenção prioritária tanto por parte da sociedade quanto dos órgãos reguladores nacionais e internacionais. No ambiente empresarial, em especial, essas condutas passaram a representar riscos significativos, não apenas de ordem legal, mas também reputacional e econômica.

Nesse contexto, as políticas de *compliance* emergem como instrumentos essenciais para prevenir, identificar e mitigar essas práticas, promovendo uma cultura organizacional baseada na integridade, na transparência e na responsabilidade. Sua implementação e fortalecimento foram impulsionados, sobretudo, por marcos legais e regulatórios que surgiram com o propósito inicial de combater a corrupção entre agentes econômicos — como é o caso da Lei Anticorrupção Empresarial no Brasil (Lei nº 12.846/2013), inspirada em legislações internacionais, a exemplo do *Foreign Corrupt Practices Act* (FCPA) dos Estados Unidos e do *UK Bribery Act* do Reino Unido.

Dessa forma, as políticas de *compliance* deixaram de ser uma simples formalidade para se tornarem uma exigência estratégica e legal, incorporando-se ao núcleo da governança corporativa e contribuindo diretamente para a perenidade e a legitimidade das organizações perante seus diversos públicos de interesse. Diante do supracitado, podemos definir corrupção como:

> A relação social (de caráter pessoal, extramercado e ilegal) que se estabelece entre dois agentes (corruptos e corruptores), cujo objetivo é a transferência de renda dentro da sociedade ou do fundo público para realização de fins estritamente privados. Tal relação envolve a troca de favores entre os grupos de agentes e geralmente a remuneração dos corruptos ocorre com o uso de propina ou de 13 qualquer tipo de pay-off, prêmio ou recompensa (CGU, 2009 *apud* Amorim; Guevara; Santos, 2013, p.56).

A partir dessa perspectiva, pode-se afirmar que o conceito de *compliance*, conforme previamente discutido, mantém uma relação direta com o enfrentamento da corrupção no âmbito empresarial e governamental. Por esse motivo o *compliance* não se limita apenas ao cumprimento de normas legais e regulatórias, mas assume uma postura proativa na identificação e prevenção de práticas ilícitas, entre elas, a corrupção. Trata-se de um instrumento que visa não apenas conter irregularidades, mas também compreender suas causas estruturais dentro das organizações. Nesse diapasão, Ciekalski (2019, p. 37) afirma que "Compliance como instrumento de melhoria de gestão e prevenção à prática da corrupção na administração pública, mecanismos de controle interno que atuam na identificação e correção de falhas que favorecem atos de corrupção."

Nesse sentido, os programas de *compliance* se configuram como mecanismos fundamentais na promoção de uma cultura organizacional ética e íntegra. Por meio da implementação de políticas, códigos de conduta, canais de denúncia, treinamentos periódicos e auditorias internas, busca-se criar um ambiente corporativo menos suscetível a comportamentos desviantes e mais comprometido com a transparência e a legalidade. Assim, o *compliance* contribui ativamente para a prevenção e o combate à corrupção, ao fortalecer mecanismos de controle e ao incentivar a responsabilização de indivíduos e instituições: "A compliance se mostra um mecanismo capaz de mitigar consideravelmente os efeitos danosos da corrupção, bem como de aprimorar a gestão pública, desde que aplicada nas organizações de maneira efetiva" (Gercwolf *apud* Mesquita, 2019).

Segundo Amorim, Guevara e Santos (2013, p.54), "discutir compliance exige compreender a natureza e a dinâmica da corrupção nas organizações". Ou seja, não se trata apenas de criar regras, mas de entender os fatores que favorecem a ocorrência de práticas corruptas e propor estratégias para mitigá-los. Nesse sentido, os programas de *compliance* assumem um papel estratégico ao fornecer instrumentos como códigos de conduta, treinamentos, auditorias e canais de denúncia, voltados à promoção de ambientes éticos e transparentes.

Nessa mesma linha, Costa e Mendes (2017, p. 112) ressaltam que "o *compliance* é um instrumento de combate preventivo à corrupção, pois atua diretamente na construção de barreiras institucionais contra práticas antiéticas". Isso demonstra que o *compliance* vai além da legalidade formal: ele atua no fortalecimento da governança corporativa e na redução da assimetria de informações dentro das empresas, criando mecanismos que dificultam a prática de atos ilícitos.

Além disso, de acordo com Dias e Ribeiro (2019, p. 89), “a efetividade dos programas de *compliance* está intimamente ligada à capacidade da organização de internalizar valores éticos em todos os níveis hierárquicos, o que contribui para a consolidação de uma cultura organizacional intolerante à corrupção”. Essa internalização se dá por meio de ações contínuas de educação corporativa, monitoramento e responsabilização.

Dessa forma, o *compliance* não apenas atua como ferramenta jurídica ou regulatória, mas se constitui como um verdadeiro sistema de integridade organizacional, fundamental para a prevenção da corrupção e para a consolidação de um ambiente corporativo ético, responsável e sustentável.

2.8. O combate à corrupção

Para compreender a constituição e a evolução das políticas de *compliance* até seu formato atual, faz- se necessário examinar o panorama histórico que envolve os marcos legais, os contextos sociopolíticos e as iniciativas institucionais que impulsionaram sua consolidação. Inicialmente, o *compliance* surgiu como resposta a práticas generalizadas de corrupção no setor público e privado, sendo concebido como um instrumento de controle e responsabilização, especialmente em ambientes econômicos que exigiam maior transparência nas relações comerciais.

No plano internacional, a Convenção da OCDE de 1997 serviu como base para a responsabilização empresarial e inspirou legislações nacionais (OCDE, 2021). Já *frameworks* contemporâneos como o ESG consolidam a visão de que o compliance é parte integrante da sustentabilidade organizacional (Silva; Campos, 2022). No setor público, recomendações de combate à corrupção reforçam a necessidade de programas de integridade institucional (Transparência Internacional, 2020).

Nesse sentido, será apresentado a seguir um percurso histórico que contempla os países, legislações e eventos-chave que atuaram como catalisadores na construção das políticas de *compliance*. Destaca-se que, em um primeiro momento, tais políticas estiveram fortemente associadas ao combate direto à corrupção, especialmente em decorrência de escândalos corporativos e pressões internacionais por boas práticas de governança. Com o tempo, no entanto,

o escopo do *compliance* foi ampliado, passando a abranger uma gama mais diversa de exigências legais e regulatórias, além de incorporar valores éticos e culturais voltados à integridade e à sustentabilidade organizacional.

Essa análise histórica é fundamental para compreender como o conceito de *compliance* foi sendo gradualmente institucionalizado nas organizações, tornando-se hoje um elemento central das estruturas de governança e um dos pilares da prevenção a riscos corporativos.

A primeira regulamentação de alcance global voltada ao cumprimento de normas legais, padrões éticos e procedimentos empresariais foi a lei federal norte-americana *Foreign Corrupt Practices Act* (FCPA), promulgada em 1977 e ainda em vigor. Essa legislação foi estabelecida conjuntamente pelo *Department of Justice* (DOJ) e pela *U.S. Securities and Exchange Commission* (SEC), em resposta a uma série de escândalos envolvendo o pagamento de propinas por corporações norte-americanas a autoridades estrangeiras, com o objetivo de obter vantagens comerciais indevidas.

O principal objetivo do FCPA é coibir a prática do suborno internacional, proibindo que empresas norte-americanas, bem como suas subsidiárias e parceiros estrangeiros que atuam nos Estados Unidos ou negociam com empresas americanas, realizem pagamentos ilícitos, ofereçam recompensas ou quaisquer benefícios de caráter pessoal a agentes públicos estrangeiros, com a finalidade de influenciar decisões governamentais ou obter favorecimentos em contratos e processos regulatórios. Por essa razão, a legislação ficou conhecida, segundo Torrey (2012), como a “lei antissuborno norte-americana”.

Segundo Martins (2019), “o Foreign Corrupt Practices Act mira a fonte financeira da corrupção: propinas pagas por grandes corporações para auferir vantagens negociais”. Torrey (2012) *apud* Catlett (2013), enfatiza o seu escopo ao observar que a lei “visa coibir o pagamento, oferta ou promessa de pagamento, ou qualquer bem de valor para agentes do governo com o objetivo de obter uma vantagem indevida”. Importante destacar que, à época de sua promulgação, o FCPA ainda não tratava de forma ampla e estruturada das políticas de *compliance* enquanto sistemas organizacionais internos. Sua ênfase recaía, fundamentalmente, sobre a repressão à corrupção e sobre a exigência de que as empresas mantivessem registros contábeis transparentes e mecanismos básicos de controle interno.

O conceito de *compliance*, como prática institucionalizada e disseminada em diversos

setores das organizações, ainda estava em construção. No entanto, o FCPA representou um marco regulatório que inaugurou as bases para o desenvolvimento futuro dos programas de *compliance*, ao colocar em pauta, de maneira inédita, a responsabilidade das empresas na prevenção de práticas ilícitas transnacionais. Com o tempo, a aplicação do FCPA se tornou mais rigorosa e ganhou alcance extraterritorial, incentivando empresas de todo o mundo a adotarem sistemas de integridade e controle mais robustos. Sua influência contribuiu significativamente para a formulação de legislações similares em outros países e para o fortalecimento da governança corporativa em nível global.

A institucionalização das políticas de *compliance* nas organizações é resultado de um processo histórico marcado por escândalos corporativos, pressões internacionais por integridade nas relações econômicas e a necessidade de fortalecer os mecanismos de governança. Esse processo teve início, de forma mais sistematizada, nos Estados Unidos, com a promulgação do *Foreign Corrupt Practices Act* (FCPA), em 1977. Essa legislação foi uma resposta direta a uma série de casos de suborno envolvendo grandes corporações norte-americanas e governos estrangeiros. O FCPA passou a proibir o pagamento de propinas a agentes públicos internacionais, além de exigir controles internos e registros contábeis precisos nas empresas, representando o primeiro grande marco legal voltado ao combate à corrupção transnacional: "A FCPA foi o primeiro diploma legal a ter aplicabilidade em territórios estrangeiros […] aplica-se a qualquer pessoa jurídica que quotiza no mercado de valores norte‑americano, … caso haja supervisão pela SEC." (Blok, 2020, p. 31)

Na década de 1990, o tema ganhou projeção internacional com a assinatura da Convenção Anticorrupção da Organização para a Cooperação e Desenvolvimento Econômico (OCDE), em 1997. Essa convenção, da qual o Brasil é signatário, ampliou o escopo das obrigações anticorrupção, incentivando a criação de legislações nacionais que penalizassem empresas envolvidas em atos ilícitos, sobretudo em transações internacionais. A partir de então, diversas nações passaram a desenvolver marcos legais que incentivavam ou exigiam a adoção de programas de *compliance* como forma de prevenção e de responsabilização das organizações.

Outro marco importante foi o *Sarbanes-Oxley Act* (SOX), sancionado nos Estados Unidos em 2002, após os escândalos financeiros envolvendo empresas como Enron e WorldCom. Essa lei reforçou as exigências de controle interno e transparência contábil, impulsionando o

fortalecimento dos programas de *compliance* no setor corporativo, especialmente nas empresas de capital aberto.

No contexto europeu, destaca-se o UK Bribery Act, promulgado no Reino Unido em 2010, que estabeleceu uma das legislações anticorrupção mais rigorosas do mundo, responsabilizando não apenas indivíduos, mas também empresas que não adotassem medidas preventivas adequadas contra o suborno, inclusive em operações internacionais. A legislação britânica consolidou a ideia de que o *compliance* deveria ser parte integrante da gestão de riscos corporativos.

No Brasil, o avanço mais significativo nesse campo ocorreu com a promulgação da Lei nº 12.846/2013, conhecida como Lei Anticorrupção Empresarial. Inspirada nos modelos norte-americano e europeu, essa legislação inovou ao prever a responsabilização objetiva de pessoas jurídicas por atos de corrupção praticados contra a administração pública, nacional ou estrangeira. Além disso, a lei atribuiu importância estratégica aos programas de integridade, prevendo que a existência de mecanismos efetivos de *compliance* pode atenuar penalidades em eventuais processos sancionatórios. Conforme Machado de Souza e Pontes Vianna (2020, p 186): "a Lei 12.846/2013 prevê um significativo benefício, por meio da redução de multa, para as pessoas jurídicas que adotam programas efetivos de integridade". Essa ideia é reforçada por Frazão (2015), ao destacar que "a existência de mecanismos e procedimentos internos de integridade, auditoria e incentivo à denúncia […] será fator relevante para a consideração da penalização".

Esse conjunto de legislações e convenções internacionais não apenas impulsionou a disseminação dos programas de *compliance*, como também consolidou uma nova perspectiva de governança organizacional, voltada à prevenção de riscos, à promoção da ética corporativa e à conformidade com normas legais e regulatórias. A partir desse percurso histórico, observa-se que o *compliance* deixou de ser um mecanismo reativo para se tornar uma ferramenta estratégica de gestão, com aplicações que transcendem o campo jurídico, alcançando áreas como finanças, meio ambiente, tecnologia, segurança da informação e responsabilidade social.

Duas décadas após a promulgação do FCPA nos Estados Unidos, o combate à corrupção ganhou força na América do Sul, especialmente no Brasil. Um marco importante foi a Convenção Interamericana contra a Corrupção, aprovada pela Organização dos Estados Americanos (OEA)

em 1996 e promulgada no Brasil pelo Decreto nº 4.410/2002. A convenção estabeleceu diretrizes para a adoção de medidas preventivas e repressivas à corrupção, promovendo cooperação internacional entre os países signatários.

Paralelamente, na Europa, a criação do Organismo Europeu de Luta Antifraude (OLAF) em 1999 representou um avanço importante no combate a fraudes e na fiscalização do uso de recursos públicos no âmbito da União Europeia. O OLAF, ativo até hoje, investiga casos de corrupção e atua no desenvolvimento de políticas antifraude, tendo ampliado sua abrangência em 2013 para incluir relações com países não membros da UE.

> Até o início da década de 1990, a corrupção era vista como mero 'lubrificante' burocrático, mas a partir daí passou a ser reconhecida como grave prejuízo social, econômico e político. O OLAF foi criado em 1999 para coordenar ações interorganizacionais e fortalecer o combate à corrupção e fraude na UE. (Rocha; Fernandes, 2020, p. 2)

Nos anos 2000, novos escândalos corporativos nos Estados Unidos, como o caso da Enron e da Arthur Andersen, expuseram práticas contábeis fraudulentas e manipulação de mercado. Como resposta, foi sancionada em 2002 a Lei Sarbanes-Oxley (SOX), que fortaleceu os mecanismos de controle interno e auditoria das empresas. A SOX marcou uma nova fase no combate à corrupção corporativa, sendo considerada um complemento ao FCPA e um divisor de águas na institucionalização de políticas de *compliance*.

Esse movimento influenciou a atuação de organizações internacionais como a OCDE e a própria OEA, que passaram a promover a adoção de práticas de *compliance* como ferramenta essencial de integridade empresarial. Na Europa, o caso da Siemens, em 2006, revelou um esquema global de subornos, inclusive no Brasil, reforçando a necessidade de medidas mais rigorosas. Em resposta, o Reino Unido aprovou, em 2010, o UK Bribery Act, uma das legislações mais rígidas do mundo contra a corrupção, que estabeleceu sanções para corrupção ativa e passiva e impôs às empresas o dever de prevenir práticas corruptas. A existência de programas de *compliance* passou a ser considerada um atenuante em eventuais processos judiciais:

A Convenção Antissuborno da OCDE constituiu um marco no combate à corrupção em âmbito internacional, ao impulsionar a revisão dos códigos de ética empresariais e estabelecer parâmetros normativos para a atuação de empresas privadas nas relações com agentes públicos estrangeiros (Guimarães, 2018 *apud* LEC, 2018). Ademais, a literatura aponta que grandes

escândalos corporativos historicamente atuaram como fatores catalisadores para o fortalecimento da governança corporativa e de seus mecanismos de fiscalização e controle, incluindo a consolidação da função de compliance nas organizações (Blanchet, 2023).

Assim, ao longo das últimas décadas, o combate à corrupção evoluiu de ações isoladas para a construção de um sistema normativo internacional que valoriza a integridade corporativa, estimula a cooperação entre Estados e exige das empresas maior comprometimento ético por meio da adoção de programas de *compliance*.

2.9. O Brasil sob a perspectiva do *compliance* e combate à corrupção

No contexto brasileiro, a adesão a tratados e convenções internacionais voltados ao combate à corrupção tem desempenhado papel central na consolidação de políticas públicas de integridade e na promoção de práticas mais transparentes no setor público e privado. Após a assinatura da Convenção Interamericana contra a Corrupção, em 1996, no âmbito da Organização dos Estados Americanos (OEA), e sua promulgação no Brasil por meio do Decreto Presidencial nº 4.410, de 7 de outubro de 2002, o país reafirmou seu compromisso com o enfrentamento da corrupção ao participar de uma nova iniciativa internacional sobre a mesma temática: a Convenção das Nações Unidas contra a Corrupção, realizada em 2003, na cidade de Mérida, no México: A aderência do Brasil às convenções internacionais anticorrupção é monitorada periodicamente, sendo os relatórios resultantes importantes fontes de informação sobre as medidas adotadas internamente para o cumprimento das obrigações assumidas no plano internacional (Saadi; Machado *apud* JusBrasil, 2024).

Essa convenção — considerada um dos instrumentos multilaterais mais abrangentes sobre o tema — foi internalizada no ordenamento jurídico brasileiro por meio do Decreto Presidencial nº 5.687, de 31 de janeiro de 2006. A Convenção de Mérida, como ficou conhecida, ampliou significativamente a abordagem sobre a corrupção, tratando não apenas da repressão a atos ilícitos, mas também da prevenção, da recuperação de ativos desviados, da cooperação internacional e da assistência técnica entre os países signatários.

A participação do Brasil nesse tratado representou um avanço importante no alinhamento do país com as diretrizes internacionais de integridade, incentivando a criação de marcos legais

internos voltados ao controle da corrupção e à promoção da ética na administração pública e no ambiente empresarial. A partir dessas convenções, observa-se o fortalecimento de uma agenda institucional voltada à construção de um sistema nacional de integridade, que mais tarde daria origem a legislações como a Lei de Acesso à Informação (Lei nº 12.527/2011) e a Lei Anticorrupção Empresarial (Lei nº 12.846/2013). A finalidade dessa convenção foi: "Art. 5º A Convenção da ONU contra a Corrupção, promulgada pelo Decreto nº 5.687/2006, prioriza medidas preventivas e de combate à corrupção, cooperação internacional para recuperação de ativos e promoção de integridade na gestão pública" (Brasil, 2006).

Diante desse cenário, foi sancionada a Lei nº 12.846/2013, conhecida como Lei Anticorrupção ou Lei da Empresa Limpa, que passou a permitir a responsabilização civil e administrativa de pessoas jurídicas por atos de corrupção cometidos contra a administração pública. A legislação prevê sanções severas, como multas que variam de 0,1% a 20% do faturamento bruto da empresa no exercício anterior à instauração do processo.

Além do caráter punitivo, a lei também introduziu mecanismos de incentivo à integridade corporativa, ao estabelecer benefícios para empresas que adotam programas de *compliance*, como a redução de multas e a celebração de acordos de leniência mediante cooperação com as investigações. Com isso, a norma passou a estimular uma cultura empresarial voltada à ética, à prevenção de riscos e à transparência nas relações institucionais.

Apesar da participação do Brasil em convenções internacionais voltadas ao combate à corrupção, até o início da década de 2010 o país ainda carecia de instrumentos legais eficazes para responsabilizar e sancionar pessoas jurídicas envolvidas em práticas ilícitas. A exemplo do que ocorreu em outros países, os escândalos de corrupção revelados em território nacional — especialmente com a Operação Lava Jato, iniciada em 2009 — evidenciaram a necessidade de medidas mais rigorosas. Entre 2014 e 2017, segundo dados da Polícia Federal, os prejuízos causados pela corrupção no Brasil chegaram a R$ 123 bilhões (Estadão, 2017): Segundo Carvalho e Mendes (2017), a Operação Lava Jato representou o maior combate à corrupção empresarial da história brasileira, punindo pessoas jurídicas e físicas envolvidas em esquemas de propina.

Diante do exposto, pode-se afirmar que o combate à corrupção está diretamente relacionado à implementação de programas de *compliance* no setor corporativo. No entanto, é

importante destacar que esses programas não devem ser vistos como a única estratégia de enfrentamento da corrupção, mas sim como uma ferramenta complementar dentro de um conjunto mais amplo de mecanismos institucionais e regulatórios voltados à integridade, à prevenção de riscos e à responsabilização de condutas ilícitas. “Os programas de compliance constituem os mecanismos e procedimentos internos de prevenção, detecção e remediação de condutas ilícitas no âmbito das empresas.” (Ayres, 2023). Além disso, Rainho (2023) ressalta que programas de compliance “têm caráter preventivo, complementando o arcabouço institucional”, evidenciando que eles são ferramentas fundamentais dentro de um conjunto mais amplo de mecanismos voltados à integridade e responsabilização.

Programas de *compliance* representam uma abordagem preventiva essencial, pois contribuem para o fortalecimento da cultura ética nas organizações, para a transparência das operações e para a construção de um ambiente empresarial menos propenso a práticas fraudulentas. No entanto, sua eficácia depende da integração com outras ações estruturais, como o fortalecimento dos órgãos de controle, a transparência pública, a educação para a ética e a atuação independente do sistema judiciário.

No ordenamento jurídico brasileiro, a Lei nº 12.846/2013 (Lei Anticorrupção) constitui um marco legal importante ao estabelecer a responsabilização objetiva de pessoas jurídicas por atos lesivos à administração pública. Especificamente, o artigo 7º, inciso VIII da referida norma dispõe que, no momento da aplicação das sanções administrativas, será considerada “a existência de mecanismos e procedimentos internos de integridade, auditoria e incentivo à denúncia de irregularidades, bem como a aplicação efetiva de códigos de ética e de conduta no âmbito da pessoa jurídica”.

Esse dispositivo legal revela a clara intenção do legislador de incentivar a adoção voluntária de programas de integridade (*compliance*) por parte das empresas, associando sua existência e efetividade à possibilidade de atenuação das sanções aplicáveis em casos de infrações. Assim, mais do que apenas um instrumento de combate à corrupção, o *compliance* passa a ser valorizado como um critério de avaliação da conduta organizacional, estimulando empresas a adotar práticas preventivas como parte de sua estratégia institucional.

A análise do artigo 7º, inciso VIII, portanto, mostra que o Estado brasileiro reconhece a importância de políticas internas de integridade como elementos que, embora não eliminem a

corrupção por completo, contribuem de forma relevante para sua mitigação, promovendo um ambiente empresarial mais ético, responsável e transparente.

A existência de mecanismos e procedimento de integridade, auditoria e incentivo à denúncia de irregularidades e a aplicação efetiva de códigos de ética e de conduta no âmbito da pessoa jurídica como atenuante na aplicação das sanções administrativas. Tem-se, portanto, que a norma propõe verdadeira mudança conceitual a partir do seu aspecto prospectivo, visto que incentiva a precaução ex ante por parte do agente econômico em detrimento da atuação dos agentes estatais (Ferreira; Queiroz, 2018, p. 246).

A adoção efetiva de políticas de *compliance* é considerada um fator atenuante na aplicação de sanções a empresas envolvidas em atos ilícitos, conforme previsto na legislação brasileira. Além do papel sancionador, destaca-se o caráter preventivo desses programas, que buscam evitar irregularidades antes que ocorram, reduzindo a necessidade de atuação estatal.

Contudo, o combate à corrupção não é o único motivo que justifica a adoção de *compliance*. Práticas inadequadas de gestão podem decorrer não apenas de má-fé, mas também de desconhecimento ou inaptidão para cumprir normas. Nesse sentido, conforme apontam Neron e Portella (2018, p. 220), embora o *compliance* não elimine totalmente os riscos de conduta indevida, ajuda a preveni-los.

Em 2015, o Decreto nº 8.420/2015 regulamentou a Lei Anticorrupção, definindo legalmente o conceito de programa de *compliance* e estabelecendo os critérios para sua avaliação. Paralelamente, outros órgãos também atuam na promoção da integridade empresarial, como o Conselho Administrativo de Defesa Econômica (CADE), que publicou o Guia de Programas de Compliance (2016). Esse documento orienta a implementação desses programas e destaca sua relevância para a livre concorrência e para o cumprimento da Lei de Defesa da Concorrência (Lei nº 12.529/2011).

Para que o programa de compliance seja implementado e obtenha êxito faz-se necessário seguir alguns critérios, tais como: Estruturação de programas robustos com comprometimento e envolvimento da alta direção; Autonomia e independência da equipe responsável pelas diretrizes e manutenção do programa; Treinamento e comunicação interna voltado para os colaboradores; Monitoramento do programa por métricas e pesquisas e Documentação e punições àqueles que venham a descumprir as regras estabelecidas pelo programa de compliance.

Diante do que foi exposto até aqui, é possível afirmar que tanto a Lei nº 12.846/2013 (Lei Anticorrupção) quanto o Decreto nº 8.420/2015, que a regulamenta, representam importantes marcos normativos para a consolidação do conceito de *compliance* no ordenamento jurídico brasileiro. Ambas as normas incorporam, de forma explícita, elementos centrais dos programas de integridade, tais como o cumprimento de normas legais e regulamentares, a observância de padrões éticos, a implementação de controles internos e a prevenção de práticas ilícitas no âmbito empresarial.

Essas legislações evidenciam que os programas de *compliance* deixaram de ser meras práticas voluntárias e passaram a ocupar um papel estratégico na gestão de riscos corporativos, sendo reconhecidos como instrumentos relevantes para garantir conformidade legal, integridade organizacional e governança ética. A partir desse novo cenário, observa-se um movimento crescente de valorização institucional do compliance, refletido tanto nas políticas públicas quanto na atuação das empresas diante das exigências legais e da pressão por maior transparência.

Assim, podemos afirmar que esses programas: Segundo Assi (2018), programas de compliance planejam a prevenção de riscos éticos e legais, incorporam métodos de detecção e controle, e demandam postura proativa dos gestores no tratamento de riscos empresariais.

Além disso, a previsão normativa da possibilidade de atenuação de sanções administrativas mediante a existência de programas de *compliance* efetivos, conforme disposto na legislação, demonstra a intenção do legislador de fomentar sua adoção por parte do setor privado. Isso indica uma tendência regulatória recente no Brasil, voltada não apenas à repressão de condutas ilícitas, mas à estruturação preventiva de sistemas de integridade capazes de evitar a ocorrência de irregularidades.

Nesse contexto, torna-se evidente a necessidade de que as políticas de *compliance* adotadas pelas organizações sejam não apenas formais, mas também estruturadas de modo a atingir os objetivos definidos por cada empresa — como o fortalecimento da cultura ética, a mitigação de riscos legais e reputacionais, e o alinhamento com os padrões regulatórios nacionais e internacionais.

3. GESTÃO DE RISCOS

3.1. Introdução

Risco refere-se a probabilidade de ocorrência de um evento que comprometa parcial ou totalmente, o cumprimento dos objetivos determinados por uma organização. O risco é realizado, tendo como embasamento legal a possibilidade e impacto, que ambos podem provocar.

Galante (2015) cita risco como sendo o potencial de ocorrência de consequência indesejáveis decorrentes da realização de uma atividade e perigo como sendo a propriedade ou condição inerente a uma substância ou atividade capaz de causar dano às pessoas, as propriedades ou ao meio ambiente.

Para Kerzner (2011), considerando o que já foi dito por Galante, riscos se tratam de uma medida da probabilidade e consequência e a maioria das pessoas concordam que envolve a noção de incerteza por constituírem uma ausência de conhecimento de eventos futuros. Quando o risco

passa a ser considerado, ou seja, tem probabilidades significantes de ocorrer, deve-se considerar as consequências e dados associados ao evento.

Os riscos do ambiente externo são os riscos difíceis de serem identificados e controlados. Eles se referem às mudanças sociais, políticas, econômicas, ambientais, além dos riscos ligados a terceiros como fornecedores, clientes e concorrentes. Segundo Coso (2007), toda organização está exposta a incertezas que podem afetar o objetivo para o qual esta foi criada. O desafio é estabelecer o nível de incerteza que se está disposto a aceitar. Essas incertezas ou eventos são conceituados de diferentes formas.

Baraldi (2005) define os riscos como todos os eventos e expectativas de eventos incertos que agem constantemente sobre os meios estratégicos (pessoas, processos, informação e comunicação) que impedem a empresa e as pessoas de ganharem dinheiro, agindo sobre os meios estratégicos e o ambiente constantemente, provocam problemas financeiros, mas se bem gerenciados, forçam a criatividade e fazem nascer as oportunidades.

Baraldi (2005) diz que se os riscos bem gerenciados causam a oportunidade de ganho ou redução de perda, a identificação de oportunidades causa riscos a serem gerenciados. Então, quaisquer que sejam as decisões, riscos serão aumentados e devem ser gerenciados para que os objetivos sejam atingidos. Neste sentido, Costa (2009) faz menção a dificuldade de perceber as oportunidades, pois não se vê aquilo que não se espera ver. As oportunidades não esperam pelas percepções. Assim, Cicco (2017) afirma que gerenciar riscos significa identificar oportunidades e utilizá-las para melhorar o desempenho.

Antes do tema gerenciamento de risco ser abordado, é necessário citar a diferença conceitual de risco e perigo, visto que essa diferença entre ambos é sutil. Galante (2015) cita risco como sendo o potencial de ocorrência de consequência indesejáveis decorrentes da realização de uma atividade e perigo como sendo a propriedade ou condição inerente a uma substância ou atividade capaz de causar dano às pessoas, às propriedades ou ao meio ambiente.

Gestão de Riscos pode ser definida como o conjunto de atividades coordenadas e estruturadas que definem de maneira clara os princípios, objetivos, estruturas, competências e processos essenciais para gerenciar e controlar os riscos em uma organização de forma eficaz. Gerenciamento de Riscos consiste em uma prática sistemática dentro das organizações que identifica, avalia, administra e controla potenciais eventos ou situações, com impactos negativos

ou positivos, como oportunidades, que visam oferecer uma segurança razoável quanto ao cumprimento dos objetivos.

Podemos afirmar que o Gerenciamento de Riscos não elimina totalmente as incertezas, mas ajuda a organização a estar melhor preparada para enfrentá-las de forma estrategicamente. Segundo Carvalho Neto e Silva (2009), o gerenciamento de risco é um processo necessário, lógico e sistemático para organizações identificarem e avaliarem riscos e oportunidades, visando melhorar a tomada de decisões e a avaliação de desempenhos.

Segundo Ávila (2014), o sucesso na implementação do gerenciamento de risco deverá resultar em melhorias na qualidade dos serviços públicos e na eficácia das políticas públicas. Deverá igualmente apoiar um diálogo entre cidadãos e o serviço público sobre a natureza do risco e como se pode melhor operar em um ambiente de incerteza e de recursos limitados.

Diante disso, destaca-se que implementar bem o gerenciamento de riscos - ou seja, identificar, analisar e lidar com ameaças que podem prejudicar o funcionamento das instituições públicas - traz benefícios diretos para a gestão pública.

Entre esses benefícios estão: Melhoria na qualidade dos serviços públicos: Quando os riscos são bem administrados, os serviços oferecidos à população (como saúde, educação, segurança etc.) tendem a ser mais estáveis, confiáveis e eficientes; Maior eficácia das políticas públicas: As ações planejadas pelo governo (políticas públicas) se tornam mais eficazes, pois há menos surpresas negativas, desperdícios ou falhas durante sua execução. Com os riscos sob controle, é mais fácil alcançar os resultados esperados.

Além dos benefícios citados, deve-se reforçar a ocorrência de fortalecimento do diálogo entre Estado e sociedade: O gerenciamento de riscos também cria um ambiente mais transparente. Isso facilita a comunicação entre o governo e os cidadãos, permitindo que as pessoas compreendam quais são os principais riscos enfrentados pela gestão pública, quais estratégias estão sendo adotadas para lidar com esses riscos e porque certas decisões são tomadas, especialmente em contextos de incerteza e limitação de recursos (como orçamentos apertados, crises sanitárias, desastres naturais, etc.). Em síntese, boa gestão de riscos não só torna o governo mais eficiente, mas também aproxima o cidadão das decisões públicas, promovendo mais confiança e compreensão mútua sobre os desafios enfrentados na administração pública.

Segundo Silva (2015), enquanto o gerenciamento de riscos corporativos amplia o alcance

dos controles internos de uma organização, de modo a adotar um processo completo de gerenciamento de riscos, a ISO 31000 estabelece um número de princípios que precisam ser atendidos para tornar a gestão de riscos mais eficaz. Já o Orange Book é um modelo de gerenciamento de riscos com viés governamental e apresenta metodologia específica para a classificação dos riscos.

O Processo de Gestão de Riscos pode ser entendido como um conjunto estruturado e contínuo de atividades que visa identificar, avaliar, compreender, e responder a eventos incertos que possam influenciar negativamente (ou positivamente) os objetivos de uma organização, projeto ou sistema. Trata-se de uma abordagem sistemática, de políticas, procedimentos e práticas de gestão, com metodologias coerentes e organizadas, que embasam a tomada de decisão e a alocação de recursos de forma eficiente. Podemos afirmar que essas políticas e práticas não atuam de forma isolada, mas integram um ciclo composto por etapas fundamentais, conforme detalhes abaixo:

Identificação dos riscos: baseia-se em identificar, descrever e registrar os eventos, condições ou circunstâncias que podem significar ameaças ou oportunidades. Essa fase permite que os gestores tomem consciência dos riscos antes que eles se concretizem. Um risco não identificado, por definição, não poderá ser analisado, tratado ou monitorado.

Segundo Moraes (2010), a escolha do método de identificação dos riscos depende de diversos aspectos, como os objetivos do estudo e nível de complexidade do sistema em estudo. Segundo Heldman (2006) *Brainstorming* é provavelmente a técnica mais usada para identificação de riscos. Nela reúnem-se os membros que podem contribuir para o processo e pedir para que comecem a pensar em possíveis eventos de risco. O segredo é que uma ideia pode inspirar outra, de modo que, até o final da reunião você tenha identificado todos os riscos possíveis.

A identificação de riscos deve envolver uma ampla gama de fontes, contemplando tanto fatores internos quanto externos à organização. Entre os riscos internos, podemos destacar, por exemplo, falhas operacionais, deficiências na gestão, conflitos organizacionais e restrições de recursos humanos, financeiros ou tecnológicos. Agora os riscos externos podem incluir alterações no marco regulatório, instabilidades econômicas, eventos ambientais extremos e mudanças no comportamento de consumidores ou demais partes interessadas no processo.

Além disso, é de suma importância que esse processo reconheça não apenas os eventos

que possam resultar em impactos adversos (ou seja, ameaças), mas também aqueles que tenham o potencial de gerar efeitos positivos (oportunidades). Essa abordagem ampliada contribui para uma visão mais estratégica da gestão de riscos, permitindo que a organização não apenas se proteja de perdas, mas também explore condições favoráveis ao seu desenvolvimento, o que é visto como um grande objetivo de qualquer organização.

Para ser eficaz, essa etapa demanda uma metodologia organizada e participativa, contando com a participação de diversos níveis hierárquicos e áreas da organização, além de eventualmente considerar a visão de stakeholders externos. Várias técnicas podem ser utilizadas nesse processo, como brainstorming, análise de cenários, entrevistas com especialistas chaves, análise de histórico de eventos passados, diagramas de causa e efeito (como o diagrama de Ishikawa), entre outras.

O principal objetivo dessa fase é a criação de um registro de riscos (ou inventário de riscos), no qual são documentadas as características de cada risco identificado — incluindo sua descrição, possíveis causas e consequências, categorias envolvidas e áreas afetadas. Esse documento serve para embasar as etapas subsequentes, além de promover maior transparência e sistematização no processo decisório, o que significa um grande avanço para a organização.

Ao ter conhecimento e colocar os riscos visíveis desde o início, a organização se destaca em posição de vantagem, pois passa a atuar de forma proativa e não apenas reativa. A antecipação é, portanto, um dos principais benefícios proporcionados por uma identificação bem conduzida, contribuindo significativamente para a resiliência e para a eficácia do planejamento estratégico. Sendo assim, é indispensável a prevenção dos problemas, para buscar soluções assertivas.

Análise dos riscos: é a avaliação da probabilidade de ocorrência e do impacto de cada risco identificado. Tem como intuito compreender sua natureza, causas e relevância de seus possíveis resultados. Pode ser realizada por meio de métodos qualitativos, quantitativos ou mistos, com o objetivo de entender a natureza e a relevância dos riscos, conforme detalhes abaixo:

De acordo com Kerzner (2011) o objetivo da análise de riscos é reunir informações suficientes sobre os riscos para estimar a probabilidade de ocorrência e a consequência da ocorrência caso ele ocorra. Depois dos riscos serem identificados, é importante que a análise seja

profunda a ponto de se compreender as suas causas e as possíveis consequências.

Xavier *et al.* (2009), diz que essa análise dos riscos deve apontar dois aspectos: sua probabilidade de ocorrência e o impacto que ele pode causa, caso ocorra. O resultado serão as prioridades de resposta em função do grau de exposição que o risco gera. Essa análise ajuda a decidir se a análise quantitativa deve ser realizada ou se é possível passar diretamente para os planos de resposta. O processo também leva em consideração os níveis de tolerância aos riscos (Heldman, 2006).

Métodos qualitativos: baseiam-se em metodologias focadas em técnicas subjetivas, descrições narrativas e classificações em escalas descritivas (como baixa, média e alta probabilidade/impacto). Quando há escassez de dados quantitativos ou quando se busca rapidez e simplicidade na avaliação, eles são de suma importância. Nocêra (2009) diz que para realizar análise qualitativa deve-se considerar também (além de impacto e probabilidade de ocorrência) fatores como prazo e tolerância a risco, restrições de custo, cronograma e qualidade do projeto. Nesse processo é de suma importância a escolha de ferramentas e técnicas para priorizar os riscos.

Já o PMI (2012) afirma que realizar a análise qualitativa dos riscos é o processo de priorização de riscos para análise de sua probabilidade de ocorrência, além do seu impacto. Essa análise avalia a prioridade dos riscos que foram identificados usando sua probabilidade e plausibilidade de ocorrência, o impacto correspondente nos objetivos estabelecidos, o intervalo de tempo para resposta e o grau de tolerância aos riscos.

Métodos quantitativos: utilizam ferramentas com base em dados numéricos, modelos estatísticos e simulações matemáticas para obter a probabilidade e o impacto dos riscos. Podemos citar como exemplos: análise de valor em risco (VaR), modelagem estocástica, análise de sensibilidade e simulações de Monte Carlo. Esse método demanda dados confiáveis e maior complexidade técnica, portanto oferece maior precisão.

Métodos mistos: técnica que utiliza elementos das abordagens qualitativa e quantitativa, buscando equilibrar profundidade analítica com viabilidade prática. Essa é uma estratégia normalmente praticada em contextos onde parte das informações pode ser quantificada, enquanto outras dependem de interpretações subjetivas, julgamento especializado ou experiência profissional.

Na prática, sempre que dados confiáveis estiverem disponíveis, os métodos mistos permitem que os riscos sejam primeiramente avaliados de forma qualitativa - por meio de escalas descritivas de probabilidade e impacto, por exemplo - e, posteriormente, sofisticados por meio de análises quantitativas mais exatas. Da mesma forma, pode-se iniciar com uma abordagem quantitativa, complementando-a com percepções qualitativas que agregam variáveis não mensuráveis, como reputação, clima organizacional ou posicionamento estratégico.

Em 1970, Denzin (1970) afirmou que a combinação de diferentes teorias, métodos e fontes de dados pode ajudar a superar o viés natural que atinge estudos com abordagens singulares (*single- method, single-observer, single-theory studies*) (Denzin, 1970). Depois de mais de 30 anos desse alerta, a combinação de métodos permanece uma prática analiticamente desejável, mas raramente utilizada (Niglas, 2004; Bryman; Bell, 2006; Wooley, 2008). Como explicar esse paradoxo? Acreditamos que o principal obstáculo à abordagem multimétodo está mais relacionado à falta de treinamento específico, do que a uma opção ontológica e/ou epistemológica da comunidade científica.

Tratamento dos riscos: trata-se da definição, seleção e implementação de medidas para mitigar os riscos negativos ou potencializar os riscos positivos. Isso pode incluir a eliminação do risco, sua redução, transferência ou aceitação, de acordo com o exposto a seguir:

Eliminação: quando é possível evitar completamente a exposição ao risco, por meio da modificação de processos, produtos ou decisões;

Redução: envolve ações para diminuir a probabilidade de ocorrência ou o impacto do risco, como o fortalecimento de controles internos, capacitação de equipes ou investimentos em tecnologia;

Transferência: refere-se à realocação do risco, total ou parcialmente, para terceiros, por meio de contratos, seguros ou parcerias estratégicas;

Aceitação: ocorre quando a organização opta por não adotar medidas específicas, assumindo conscientemente os efeitos do risco, geralmente quando os custos de mitigação superam os potenciais prejuízos. No caso de riscos positivos (oportunidades), o tratamento pode envolver estratégias para aumentar a probabilidade de ocorrência ou maximizar os benefícios associados. Independentemente da abordagem adotada, é fundamental que o tratamento esteja alinhado aos objetivos estratégicos da organização e seja acompanhado de um plano de ação

claro, com responsabilidades, prazos e critérios de monitoramento bem definidos.

Monitoramento e revisão: compreende o acompanhamento contínuo dos riscos, das ações de tratamento implementadas e do ambiente externo e interno, com vistas à atualização das estratégias de gestão de riscos, à medida que novos riscos surgem ou os existentes se modificam.

> O monitoramento e a revisão são componentes fundamentais da gestão de riscos, assegurando que os controles estejam funcionando conforme o planejado e que os riscos estejam sendo identificados e tratados de maneira eficaz. (ABNT NBR ISO 31000:2018, p. 11).

Ainda,

> O contexto interno e externo de uma organização está em constante mudança; assim, a supervisão sistemática dos riscos deve ser contínua para garantir a eficácia das respostas e estratégias. (ISO 31000:2018).

Como ferramenta, Kerzner (2011) diz que o necessário para a eficácia do processo de monitoramento e controle é importante estabelecer um sistema de indicadores de gestão de custos, desempenho e cronograma. Esse sistema irá fornecer uma alerta de potenciais problemas, permitindo assim que ações sejam feitas a tempo.

Comunicação dos riscos: assegura o fluxo de informações relevantes entre os responsáveis pela gestão de riscos e os demais públicos envolvidos. A comunicação eficaz é essencial para garantir que todos compreendam os riscos e participem de forma informada na sua gestão.

3.2. Gestão de riscos e compliance na Universidade de Brasília

Benefícios identificados:

a) Fortalecimento da Transparência e Prestação de Contas: Adoção de políticas que ampliam o acesso público às informações institucionais, promovendo visibilidade e confiança da sociedade na gestão pública universitária.

b) Melhoria na Qualidade dos Serviços Públicos: A gestão eficaz dos riscos contribui para serviços mais estáveis, confiáveis e eficientes, impactando positivamente na educação, pesquisa e extensão.

c) Maior Eficácia das Políticas Públicas: A análise e o tratamento antecipado dos riscos evitam surpresas e falhas, aumentando a chance de alcançar metas institucionais.

d) Promoção da Cultura de Integridade e Ética: Programas de compliance estabelecem mecanismos preventivos contra desvios de conduta, corrupção e fraudes, fortalecendo a ética e os valores organizacionais.

e) Engajamento e Sensibilização da Comunidade: Comunicação eficaz, campanhas de sensibilização e treinamentos fortalecem o envolvimento de todos os níveis hierárquicos e unidades acadêmicas e administrativas.

f) Redução de Riscos Financeiros e Legais: Mitigação das causas de passivos e desperdícios, especialmente em áreas de maior sensibilidade orçamentária como investimentos e litígios.

g) Apoio à Governança e Tomada de Decisão: A gestão estruturada de riscos e compliance fornece informações relevantes e confiáveis para a alta administração, orientando decisões estratégicas.

Desafios identificados:

a) Desenvolvimento Insuficiente de Análise e Tratamento de Riscos: Predominância das ações de comunicação em detrimento de análises técnicas detalhadas e implementação efetiva de respostas mitigadoras, indicando maturidade ainda em desenvolvimento no sistema de gestão de riscos.

b) Baixa Ênfase em Medidas de Resposta: Pouca atenção sistemática às ações corretivas e sancionatórias, o que pode comprometer a efetividade dos mecanismos de integridade.

c) Complexidade na Integração de Diferentes Áreas e Disciplinas: A ampliação do alcance do compliance para além do jurídico exige alinhamento entre setores variados como finanças, sustentabilidade, recursos humanos e tecnologia, o que pode ser desafiador.

d) Dependência de Recursos e Capacitação: Implementar programas robustos requer investimentos em formação, tecnologia e monitoramento, que nem sempre estão plenamente disponíveis.

e) Limitações de Dados e Informação: A análise e avaliação integrada dos resultados enfrentam dificuldades pela ausência ou insuficiência de dados desagregados, dificultando a mensuração do impacto e refinamento das políticas.

f) Cultura Organizacional e Resistência Interna: Promover a internalização de valores éticos em todos os níveis requer tempo, liderança comprometida e superação de resistências ou desconhecimento.

g) Necessidade de Aperfeiçoamento Metodológico: Falta de metodologias sistemáticas para avaliação de riscos, definição clara de critérios de priorização e acompanhamento contínuo das ações.

h) Desenvolvimento Insuficiente de Análise e Tratamento de Riscos: Predominância das ações de comunicação em detrimento de análises técnicas detalhadas e implementação efetiva de respostas mitigadoras, indicando maturidade ainda em desenvolvimento no sistema de gestão de riscos.

3.3. Observações gerais

A UnB apresenta uma concentração significativa de ações relacionadas à comunicação, sensibilização e prestação de contas, o que é essencial, mas insuficiente sem o balanceamento com análise, tratamento e monitoramento técnicos mais profundos. A classificação das despesas orçamentárias da universidade em relação à sensibilidade para compliance revela que, embora grande parte dos recursos esteja em rubricas de baixa sensibilidade (com menor espaço para gestão), as áreas de média e alta sensibilidade demandam maior atenção para evitar riscos financeiros e legais relevantes.

A maturidade institucional no tema ainda apresenta lacunas, apontando para possibilidades de avanço na consolidação de programas mais integrados e efetivos de compliance e gestão de riscos. Esses benefícios e desafios demonstram que, na UnB, a gestão de compliance e riscos é vista como estratégica para garantir integridade, eficiência e transparência, embora exija esforços contínuos para superar limitações operacionais, culturais e técnicas e alcançar um sistema robusto e consolidado.

3.4. Normas de Gestão de Riscos: ISO e COSO

A ISO 31000 é uma a norma internacional de referência para gestão de riscos, publicada

pela International Organization for Standardization (ISO). Ela oferece diretrizes para identificar, analisar e tratar riscos, promovendo abordagem sistemática voltada à criação e proteção de valor. No Brasil, foi internalizada como ABNT NBR ISO 31000:2018, sucedendo a versão de 2009 e consolidando-se como framework relevante também para o setor público.

A norma estrutura-se em princípios como integração, estruturação, personalização, inclusão, dinamismo, base em informações, consideração de fatores humanos e melhoria contínua. Santos (2021) enfatiza que tais princípios permitem aplicação ampla da norma, independentemente do setor, enquanto Damodaran (2019) destaca sua relevância em ambientes voláteis para a tomada de decisões estratégicas.

Os oito princípios da ISO 31000 — integrada, estruturada e abrangente, personalizada, inclusiva, dinâmica, baseada em informações, atenta a fatores humanos e culturais, e de melhoria contínua — garantem uma gestão de riscos eficaz e adaptável. Santos (2021) enfatiza que esses princípios facilitam a aplicação universal, independentemente do risco ou setor, fortalecendo a cultura organizacional. Damodaran (2019) complementa, destacando sua integração à tomada de decisões estratégicas em ambientes voláteis.

O processo de gestão de riscos proposto pela ISO 31000 é iterativo e composto pelas etapas de comunicação e consulta, estabelecimento de escopo e contexto, avaliação de riscos (identificação, análise e avaliação), tratamento de riscos e monitoramento contínuo. Almeida Ferreira (2013) valida essa estrutura pela praticidade em cenários reais. No contexto desta pesquisa, a ISO 31000 subsidia a análise de riscos em políticas públicas, conectando a teoria de compliance aos desafios concretos dos setores público e privado.

A adoção da norma reflete maturidade crescente no campo, no qual a gestão de riscos evolui de prática reativa para abordagem estratégica, gerando benefícios como redução de perdas, maior previsibilidade e otimização de recursos. Para dissertações em Economia, como a do usuário na UnB, a ISO 31000 subsidia análises de risco em políticas de desenvolvimento econômico e eventos corporativos. Ela alinha compliance e inovação, com autores como Junqueira (2021) ilustrando ganhos em processos de gestão. Essa abordagem eleva a relevância prática da pesquisa, conectando teoria a desafios reais do setor público e privado.

A gestão de riscos ganhou destaque positivo e valor agregado, tornando-se essencial na administração diária, especialmente para tomadores de decisões que a incorporam rotineiramente

nas organizações. Seu impacto reflete-se no reconhecimento de sua alta relevância, evidenciado pela publicação da norma ISO 31000:2009 – Gestão de Risco. Essa norma já foi traduzida e adaptada para o português como NP ISO 31000:2012 – Gestão de Risco, facilitando sua implementação em contextos lusófonos. Ambas serão referidas daqui em diante simplesmente como ISO 31000 e NP ISO 31000.

O "balanço favorável e de mais-valia" indica que a gestão de riscos evoluiu de uma prática reativa para uma estratégica, gerando benefícios como redução de perdas, otimização de recursos e aumento da resiliência organizacional. Essa mudança reflete uma maturidade no campo, impulsionada por crises globais e demandas regulatórias, posicionando-a como ferramenta indispensável para decisões cotidianas.

A publicação da ISO 31000:2009 em 2009 marcou um marco normativo internacional, fornecendo princípios, framework e processo para gerenciar riscos de forma integrada e proporcional. Seu reconhecimento como "grande imprescindibilidade" decorre da adoção ampla em setores públicos e privados, promovendo uma cultura de risco proativa. A versão portuguesa NP ISO 31000:2012, equivalente à tradução oficial, remove barreiras linguísticas, acelerando sua difusão em países como Portugal e Brasil (ABNT NBR ISO 31000).

A norma NP ISO 31000 estabelece um conjunto de princípios essenciais para tornar a gestão de riscos eficaz e eficiente, enfatizando que apenas organizações que os integrem transversalmente em todas as áreas reduzirão incertezas e alcançarão seus objetivos. Esses princípios promovem uma abordagem sistemática, garantindo que a gestão de riscos seja incorporada à estratégia, cultura e operações diárias. A norma destaca a necessidade de estruturas organizacionais que suportem essa integração contínua.

A norma recomenda que as organizações desenvolvam, implementem e aprimorem continuamente uma estrutura dedicada a integrar a gestão de riscos à gestão estratégica, planejamento, relatórios, políticas, valores e cultura organizacional. Essa integração global proporciona o melhor suporte, tornando a gestão de riscos parte inerente de toda a organização. Ela fornece princípios e diretrizes para lidar com qualquer tipo de risco de forma sistemática, transparente e confiável, independentemente do contexto ou setor.

Cada organização ou setor possui necessidades, percepções e critérios específicos para a Gestão de Riscos (GR), o que justifica o "estabelecimento do contexto" como primeira atividade

do processo genérico. Essa etapa inicial assegura que a GR seja personalizada, considerando fatores internos e externos únicos. Assim, a norma promove mais-valias como maior resiliência, otimização de recursos e resposta eficaz às expectativas de diversas partes interessadas.

Relações entre Elementos e Benefícios

A NP ISO 31000 estabelece claras relações entre os princípios da gestão de riscos, o quadro organizacional (estrutura de suporte) e o processo (etapas operacionais), formando um framework coeso. Os benefícios incluem redução de incertezas, melhoria na tomada de decisões e valor agregado sustentável. Essa abordagem holística responde às demandas de stakeholders variados, reforçando a relevância da norma em contextos acadêmicos e empresariais, como dissertações sobre economia e eventos corporativos.

COSO, ou *Committee of Sponsoring Organizations of the Treadway Commission*, é um framework americano desenvolvido por entidades como AICPA e IIA para aprimorar controles internos e gestão de riscos corporativos (ERM), com sua versão principal de 2017 integrando riscos à estratégia e performance organizacional. Diferente de normas internacionais como ISO 31000, o COSO enfatiza governança e apetite a risco em contextos corporativos, sendo amplamente referenciado por autores como Robert S. Kaplan e Steven R. Covey em análises de risco estratégico.

Criado em 1985 após escândalos como Enron, o COSO evoluiu do framework de controle interno (1992, atualizado em 2013 por COSO e Kaplan) para ERM em 2004 e 2017, definindo gestão de riscos como processo contínuo para valor sustentável. Kaplan e Cooper (1996), em "Cost & Effect", influenciaram sua ênfase em atividades geradoras de valor, enquanto a versão 2017 organiza 20 princípios em 5 componentes: governança/cultura, estratégia, performance, revisão e informação. Essa estrutura prescritiva contrasta com abordagens mais genéricas, promovendo alinhamento entre risco e objetivos.

O COSO ERM estrutura-se em cinco domínios interligados, com princípios detalhados para implementação: Governança e Cultura: Liderança define apetite e tolerância a riscos; Estratégia e Objetivos: Integra riscos à formulação estratégica; Performance: Identifica, avalia e responde a riscos (evitar, mitigar, transferir); Revisão e Revisão: Monitora e adapta continuamente; Informação e Comunicação: Assegura transparência. Moeller (2011), em "COSO Enterprise Risk Management", elogia sua aplicação prática em auditorias internas, enquanto

Power (2007) critica em "Organized Uncertainty" a ênfase excessiva em compliance sobre inovação. COSO ERM (2017) e ISO 31000 (2018) convergem na integração estratégica de riscos, mas divergem em escopo e rigidez, como analisado por autores como Hillson e Murray-Webster (2012) em "Managing Risk Appetite".

Quadro 2. Comparativo entre Frameworks de Gestão de Riscos: COSO ERM e ISO 31000

Dimensão	COSO ERM (2017)	ISO 31000 (2018)
Origem	Comitê americano, foco corporativo	ISO internacional, universal
Abordagem	Prescritiva, 5 componentes/20 princípios	Princípios flexíveis (8), processo genérico
Foco Principal	Apetite a risco, performance estratégica	Criação/proteção de valor, contexto inicial
Flexibilidade	Moderada, para grandes organizações	Alta, adaptável a qualquer escala
Aplicação	Governança e controles internos (EUA/Brasil)	Compliance global e operacional

Fonte: elaborado pela autora

O Tribunal de Contas da União (TCU) integra ativamente a ISO 31000 e o COSO ERM em sua governança e auditorias públicas, promovendo gestão de riscos estratégica no setor brasileiro para mitigar incertezas e alinhar objetivos institucionais. A Resolução TCU nº 287/2017 estabelece sua política de riscos, incorporando princípios da ABNT NBR ISO 31000 e referenciando COSO, como destacado por Beasley *et al*. (2017) no framework COSO ERM, que enfatiza integração com performance. Oliveira e Santos (2020), em análises de tribunais de contas, reforçam que essa abordagem eleva a maturidade em controles internos.

O TCU adota os oito princípios da ISO 31000 (integrada, personalizada, dinâmica etc.), estruturando seu processo em etapas como estabelecimento de contexto e tratamento de riscos, conforme o Manual de Gestão de Riscos do TCU (2ª ed., 2018). Moeller (2011), em "COSO

Enterprise Risk Management", elogia essa flexibilidade operacional para auditorias de conformidade, enquanto Hillson (2019), autor de "Capturing Upside Risk", valida sua aplicação em contextos públicos para redução de volatilidade. Desde 2012, o TCU recomenda planos de risco em administrações indiretas, ligando-os à alta administração.

A Resolução 287/2017 referencia COSO para governança, apetite a risco e "três linhas de defesa", alinhando supervisão do Conselho a componentes como cultura e estratégia. Fraser e Simkins (2010), editores de "Enterprise Risk Management", destacam sua eficácia em emergentes como o Brasil, complementando ISO em avaliações de performance. Kaplan e Mikes (2012), em "Managing Risks: A New Framework" (Harvard Business Review), analisam como COSO fortalece auditorias fiscais do TCU contra fraudes orçamentárias.

Quadro 3. Comparação de Frameworks no Contexto TCU

Framework	**Ênfase no TCU**	**Autores de Referência**
ISO 31000	Processo flexível e operacional	Hillson (2019); Moeller (2011)
COSO ERM	Governança estratégica e apetite	Beasley et al. (2017); Fraser (2010)

Fonte: elaborado pela autora

4. METODOLOGIA

A elaboração da tabela de ações sobre Políticas de Compliance e Gestão de Riscos seguiu um processo sistemático de leitura, conforme detalhes abaixo:

4.1. Processo Sistemático Adotado

Leitura completa: Todos os documentos foram lidos integralmente para captar o contexto e evitar interpretações isoladas.

Extração de informações: Identificados os trechos relevantes que mencionavam ações, políticas ou práticas ligadas a Compliance (como prevenção de fraudes e conformidade ética) e Gestão de Riscos (como identificação e mitigação de ameaças operacionais).

Classificação: Cada informação extraída foi categorizada por tipo de ação (ex.: preventiva, corretiva), eixo temático (Compliance ou Riscos) e nível de implementação (ex.: estratégica, operacional).

Consolidação: as informações foram unificadas em uma única entrada padronizada, criando um banco de dados único e sem redundâncias.

O foco principal foi gerar uma tabela unificada que permita:

Identificar ações: Visualizar o que existe em cada documento de forma rápida.

Comparar iniciativas: Avaliar diferenças ou semelhanças entre políticas de Compliance e Riscos.

Avaliar de modo padronizado: Usar critérios uniformes (como status de implementação ou responsáveis) para análises imparciais. Isso assegura rastreabilidade (é possível voltar à fonte original de cada dado) e transparência (todas as etapas são documentadas, facilitando auditorias ou atualizações futuras). No fim, a tabela vira uma ferramenta prática para planejamento estratégico em governança corporativa.

A primeira etapa do processo foi a identificação precisa das ações relevantes em cada documento listado na coluna "Fonte". Isso garantiu que só entrassem na tabela itens diretamente ligados a Políticas de Compliance ou Gestão de Riscos, evitando dispersão.

4.2. Como funcionou essa identificação

Leitura integral: Cada documento foi analisado do início ao fim, captando o contexto completo para não perder conexões sutis;

Critérios semânticos: Buscamos termos chave, explícitos ou implícitos, como: Gestão de riscos, mapa de riscos, apetite a risco, planos de tratamento; Controles internos, integridade, ética, anticorrupção, conformidade regulatória; Monitoramento, auditoria interna, comitês, políticas, normativos, procedimentos, due diligence, gestão de continuidade; Extração e associação: Quando uma ação se conectava claramente a pelo menos um eixo (Compliance ou

Riscos), ela era resumida e ligada à meta ou objetivo original do documento (se mencionado).

Filtros rigorosos: excluídas ações puramente administrativas ou operacionais sem vínculo com controles, conformidade ou risco; Casos limítrofes incluídos com uma nota para revisão futura, priorizando completude sem comprometer a qualidade. Essa abordagem criou uma base limpa e focada, pronta para as próximas etapas de classificação e consolidação. Ela reflete um equilíbrio entre precisão e abrangência, ideal para análises de governança.

Em seguida, cada ação identificada foi classificada segundo seu estágio de execução. As políticas foram divididas entre planejadas e executadas com base nas evidências encontradas no documento original. Foram consideradas planejadas aquelas descritas como previsões, metas futuras, ações propostas ou iniciativas dependentes de deliberação. Já as executadas correspondiam a ações implementadas, normativos publicados, processos já operacionais ou resultados entregues.

Para ações com execução parcial, o critério adotado variou conforme o nível de evidência: em casos com artefato institucional claro, mesmo incompleto, elas foram registradas como executadas, com a observação “parcial”; quando predominava a fase de concepção ou piloto, elas permaneceram como planejadas, acompanhadas de uma nota descritiva sobre o estágio de desenvolvimento.

A terceira etapa foi a classificação dessas ações de acordo com quatro referenciais complementares: a norma ISO 31000, o *framework* COSO-ERM, os referenciais do Tribunal de Contas da União (TCU) e uma taxonomia acadêmica. Na perspectiva da ISO 31000, as ações foram enquadradas em princípios e governança de risco, processo de gestão de riscos (comunicação e consulta; contexto; identificação; análise; avaliação; tratamento; monitoramento e revisão; registro e reporte) ou integração com processos organizacionais.

No COSO-ERM, as classificações seguiram os cinco componentes principais: governança e cultura; estratégia e definição de objetivos (incluindo apetite a risco); desempenho (identificação e avaliação de riscos, respostas e desenvolvimento de portfólio); revisão e melhoria; e informação, comunicação e reporte. Já nos referenciais do TCU, foram utilizadas categorias como liderança e estratégia; controles internos e gestão de riscos; integridade, ética e conformidade; e transparência e prestação de contas. Por fim, na classificação acadêmica, buscou-se sintetizar as ações em macrotemas que dialogam com a literatura, como governança e

accountability, conformidade e integridade, gestão de riscos e controles, monitoramento e avaliação, e cultura organizacional e capacidades institucionais. Cada um desses *frameworks* serão melhor explicados abaixo.

Essa classificação múltipla permitiu leituras cruzadas e identificou a sobreposição de *frameworks*, situação em que se optou por registrar apenas a categoria mais aderente, com anotações adicionais quando necessário. Em todos os casos, manteve-se a chave de rastreabilidade Fonte para preservar a vinculação entre a ação registrada e o documento de origem. Além disso, as colunas Categoria, Tipo, Ação, Meta/Objetivo associado, Data, Responsável (indicado ou provável) e as quatro classificações serviram como campos substantivos e analíticos da tabela. Para harmonizar a informação, houve uma etapa de normalização dos dados, incluindo a padronização dos nomes de responsáveis, a unificação de registros duplicados e a inserção de observações para casos com lacunas de evidência.

A preparação final da tabela foi realizada em R, utilizando o pacote tidyverse para manipulação de dados e o pacote openxlsx para exportação do resultado em formato Excel. Esse código percorre a pasta definida, identifica todos os arquivos no formato CSV, consolida- os em um único data frame e realiza a unificação da coluna “Responsável (indicado ou provável)” com a coluna “Responsável” original, garantindo que não haja perda de informação nos casos de campos nulos. Após essa harmonização, a coluna redundante é excluída e o arquivo final é exportado para o formato .xlsx.

Ao final, o produto resultante é uma base única que preserva a rastreabilidade, a clareza metodológica e a comparabilidade das informações. Essa base permite identificar padrões de maturidade em governança, avaliar a distribuição de ações entre planejadas e executadas, mapear lacunas de implementação e observar a aderência das iniciativas aos diferentes referenciais normativos e acadêmicos. Embora robusto, o trabalho reconhece limitações, como a dependência da precisão dos textos originais e a granularidade variável das ações descritas, apontando para a necessidade de revisões periódicas e de possíveis decomposições de ações amplas em etapas mais detalhadas. A integração de indicadores de desempenho e impacto também é recomendada para futuras versões, ampliando o potencial de análise e gestão estratégica das políticas de Compliance e de Gestão de Riscos.

4.3. ISO 31000

A ISO 31000:2018 – Risk Management – Guidelines, conforme já mencionado aqui, é uma norma internacional desenvolvida pela International Organization for Standardization (ISO), que oferece princípios e diretrizes abrangentes para o gerenciamento de riscos em qualquer tipo de organização. Essa norma visa sistematizar o processo de tomada de decisão em contextos de incerteza, promovendo uma cultura organizacional orientada à antecipação, tratamento e monitoramento de riscos. Sua aplicação é especialmente relevante no setor público, onde a governança eficiente depende de instrumentos que assegurem a integridade, a legalidade e a eficácia dos processos decisórios (ISO 31000:2018).

No contexto da Universidade de Brasília (UnB), a classificação das ações institucionais segundo os princípios da ISO 31000 permitiu identificar a aderência das iniciativas à lógica da gestão de riscos. A análise tomou como base a descrição das ações realizadas no âmbito da ouvidoria e da governança, organizando-as segundo as cinco etapas do processo de gestão de riscos delineadas pela norma, além do princípio transversal de comunicação e consulta.

A primeira categoria utilizada foi a de Identificação de Riscos, que consiste na detecção sistemática de eventos que possam impactar a consecução dos objetivos institucionais. Essa etapa envolve o mapeamento de fontes de risco, áreas vulneráveis, e a compreensão das causas e consequências potenciais. No caso da UnB, foram enquadradas nessa categoria as ações voltadas à criação de canais de escuta e denúncia, bem como iniciativas de diagnóstico preliminar de ameaças institucionais.

A segunda categoria, Análise de Riscos, refere-se à compreensão da natureza dos riscos identificados, sua probabilidade de ocorrência e os impactos potenciais. Embora menos presente de forma explícita nos documentos analisados, essa etapa está implícita em ações voltadas à elaboração de relatórios, pareceres e estudos voltados ao aprimoramento da gestão institucional. Tais atividades, quando estruturadas com metodologia analítica, podem ser interpretadas como instrumentos de análise de risco, conforme preconizado pela norma.

Em seguida, a Avaliação de Riscos constitui o processo de comparação entre os resultados da análise e critérios previamente estabelecidos para subsidiar decisões sobre a necessidade de intervenção. Apesar de essa etapa exigir uma maturidade organizacional elevada e um aparato

normativo bem definido, algumas iniciativas institucionais de priorização de temas sensíveis, revisão de fluxos de trabalho e reformulação de instâncias deliberativas podem ser relacionadas a esse esforço avaliativo.

A quarta categoria, Tratamento de Riscos, compreende o desenvolvimento e a implementação de medidas para lidar com os riscos avaliados. Essas medidas podem incluir mitigação, transferência, aceitação ou eliminação dos riscos. Na UnB, foram incluídas nessa categoria ações como a normatização de condutas, criação de novos canais de controle, revisão de protocolos institucionais e institucionalização de práticas de gestão. Já a etapa de Monitoramento e Revisão envolve a supervisão contínua dos riscos e da eficácia das medidas adotadas, promovendo ajustes e correções de rota sempre que necessário. São ações típicas desse eixo os relatórios periódicos, auditorias internas, acompanhamento de denúncias e processos de retroalimentação institucional. O fortalecimento da ouvidoria como unidade estratégica também se alinha a esse princípio.

Por fim, a Comunicação e Consulta é reconhecida pela ISO 31000 como um princípio transversal essencial em todas as fases do processo de gestão de riscos. Ela envolve o compartilhamento de informações relevantes com as partes interessadas, bem como o engajamento de públicos internos e externos na construção de um ambiente de confiança e participação. Foram categorizadas como ações de comunicação aquelas voltadas à criação de campanhas de sensibilização, elaboração de cartilhas informativas, transparência ativa e manutenção de portais e canais de atendimento.

A utilização da ISO 31000 como critério de classificação das ações da UnB permitiu uma análise mais estruturada da maturidade institucional em relação à gestão de riscos. Observou-se, nesse sentido, uma forte presença de ações de comunicação e tratamento de riscos, com menor incidência de iniciativas voltadas à análise e avaliação sistemática. Isso sugere uma oportunidade de aprimoramento, especialmente no desenvolvimento de metodologias para mensuração de riscos e definição explícita de critérios de priorização e resposta. O alinhamento aos princípios da ISO 31000 pode, assim, fortalecer a governança universitária, conferindo maior previsibilidade, controle e legitimidade às decisões institucionais.

4.4. COSO – Entreprise Risk Management (ERM)

A aplicação do COSO – Enterprise Risk Management (ERM) Framework, desenvolvido pelo Committee of Sponsoring Organizations of the Treadway Commission, representa uma das abordagens mais amplamente aceitas para a gestão de riscos corporativos, tanto no setor privado quanto no público. A estrutura do COSO tem como objetivo integrar a gestão de riscos à estratégia organizacional, à governança e ao desempenho, fortalecendo os mecanismos de controle e a responsabilização institucional (COSO, 2017).

O modelo COSO-ERM está estruturado em componentes inter-relacionados que abrangem desde o ambiente institucional até o monitoramento dos controles implementados. A classificação das ações da Universidade de Brasília (UnB) com base neste referencial permitiu organizar as iniciativas em cinco grandes grupos: Ambiente de Controle, Avaliação de Riscos, Atividades de Controle, Informação e Comunicação, e Monitoramento.

A primeira dimensão, o Ambiente de Controle, constitui o alicerce do sistema de controle interno. Refere-se à integridade, aos valores éticos e à competência das pessoas na organização, bem como ao estilo de liderança e à estrutura de governança adotada. Na UnB, foram enquadradas nessa categoria ações como a formulação de políticas institucionais, a definição de valores de integridade, e a atuação em conselhos superiores com foco em ética e transparência. Essas ações criam as bases culturais e normativas sobre as quais os demais controles se apoiam.

A segunda categoria, Avaliação de Riscos, compreende a identificação e a análise de riscos que possam afetar o alcance dos objetivos institucionais. O COSO propõe que essa avaliação leve em conta não apenas os eventos negativos, mas também oportunidades, e que seja feita de forma contínua. No caso analisado, incluíram- se aqui ações como a criação de canais de denúncia, o mapeamento de vulnerabilidades institucionais e a participação em diagnósticos setoriais — elementos que viabilizam a compreensão dos riscos e permitem antecipar cenários.

O terceiro componente, Atividades de Controle, refere-se às políticas e procedimentos que garantem que as ações estejam em conformidade com as diretrizes institucionais. Essas atividades funcionam como barreiras e mecanismos de correção de desvios. Entre as ações da UnB, foram classificadas como pertencentes a essa categoria aquelas que envolvem a normatização de processos, a implementação de instrumentos de controle interno, a criação de protocolos e a institucionalização de boas práticas administrativas.

A categoria de Informação e Comunicação abrange os processos de coleta, processamento e disseminação de informações relevantes para a tomada de decisão e o cumprimento das responsabilidades organizacionais. Incluem-se aqui iniciativas voltadas à transparência, manutenção de portais e canais institucionais, divulgação de relatórios de gestão, bem como ações de escuta e diálogo com a comunidade. Tais mecanismos são essenciais para assegurar a fluidez das informações, interna e externamente, e promovem a prestação de contas como valor institucional.

Por fim, o Monitoramento consiste na supervisão contínua ou periódica das atividades de controle para garantir sua eficácia e atualização. Esse componente envolve tanto a autoavaliação dos processos quanto auditorias independentes e mecanismos de retroalimentação. Na análise das ações da UnB, enquadrou-se nesta categoria a participação em encontros de ouvidorias, revisões de práticas institucionais e iniciativas que visam o aprimoramento contínuo da governança.

A utilização da estrutura do COSO-ERM como base classificatória revelou a centralidade de ações voltadas à informação e à comunicação na prática da UnB, bem como um esforço significativo no fortalecimento do ambiente de controle e na institucionalização de mecanismos normativos. Ao mesmo tempo, apontou para oportunidades de aprofundamento na formalização de metodologias de avaliação de riscos e na criação de rotinas sistemáticas de monitoramento. O referencial COSO fornece, assim, um modelo robusto para fortalecer a governança pública, promover maior coerência entre risco, controle e desempenho institucional, e garantir que a gestão universitária seja orientada a resultados com integridade, responsabilidade e transparência.

4.5. TCU

A governança pública no Brasil tem sido amplamente influenciada pelas diretrizes estabelecidas pelo Tribunal de Contas da União (TCU), que desenvolveu o Referencial Básico de Governança Aplicável a Órgãos e Entidades da Administração Pública (TCU, 2020). Este referencial define governança como o conjunto de mecanismos de liderança, estratégia e controle, postos em prática para avaliar, direcionar e monitorar a atuação das organizações públicas, visando a prestação de serviços de interesse da sociedade com efetividade, eficiência e

accountability.

Para a classificação das ações da Universidade de Brasília (UnB), o referencial do TCU foi adotado com base em três grandes eixos: Liderança, Estratégia e Controle, além dos princípios fundamentais de Integridade, Transparência e Prestação de Contas. Essa abordagem permite analisar as iniciativas institucionais segundo a lógica de maturidade da governança, destacando em quais dimensões há maior ênfase e onde existem oportunidades de aprimoramento.

O eixo da Liderança abrange a atuação das instâncias superiores, a definição de valores organizacionais e a promoção de um ambiente ético e colaborativo. As ações classificadas nesta categoria incluem a participação da Ouvidoria e da Administração Superior em conselhos deliberativos, bem como a elaboração de normas e estatutos que reforçam a governança da UnB. Essas iniciativas refletem o papel estratégico da liderança na definição de prioridades e na condução das políticas institucionais.

A Estratégia, por sua vez, está associada ao planejamento e ao alinhamento das ações aos objetivos de longo prazo da instituição. Iniciativas como campanhas de engajamento, criação de instrumentos de governança e participação em encontros institucionais foram enquadradas nesse eixo, por promoverem alinhamento com diretrizes estratégicas e fortalecimento das redes de governança.

De acordo com o TCU, essa dimensão deve garantir que os recursos e esforços institucionais estejam voltados para a geração de valor público. O Controle envolve o monitoramento das atividades, a avaliação de resultados e a implementação de mecanismos de correção e prevenção de irregularidades. Foram incluídas aqui ações como a normatização de processos, a implementação de instrumentos de controle interno e a criação de canais de denúncia. O objetivo dessa dimensão, segundo o TCU, é fornecer à alta gestão informações confiáveis para a tomada de decisões e assegurar o cumprimento das normas.

Além desses eixos estruturantes, os princípios de Integridade, Transparência e Prestação de Contas foram utilizados para classificar ações com ênfase na divulgação de informações, fortalecimento do controle social e promoção de práticas éticas. Exemplos incluem a publicação da Carta de Serviços ao Cidadão, a atualização do site da Ouvidoria e a participação em fóruns e redes de ouvidorias.

A aplicação do modelo do TCU permitiu identificar que a UnB possui um conjunto expressivo de ações voltadas à transparência e ao controle institucional, reforçando seu compromisso com a integridade e com a participação cidadã. Por outro lado, a análise sugere a possibilidade de avançar na dimensão estratégica, com maior integração entre os processos de governança e o planejamento de longo prazo. O referencial do TCU é amplamente aceito no setor público brasileiro e orienta não apenas o desenvolvimento da governança, mas também o aprimoramento das políticas de compliance e de gestão de riscos. Ao associar as ações institucionais aos mecanismos e princípios delineados por esse modelo, a UnB fortalece sua capacidade de gerar valor público e consolidar a confiança da sociedade na gestão universitária.

4.6. Melhor literatura

A literatura acadêmica sobre compliance e gestão de riscos nas organizações públicas e privadas tem se consolidado ao redor de três funções fundamentais dos sistemas de integridade institucional: prevenção, detecção e resposta. Esse modelo, frequentemente adotado tanto em estudos teóricos quanto em práticas organizacionais, busca estruturar os mecanismos de integridade de forma coerente com o ciclo de vida dos riscos e com a lógica de controle contínuo. A adoção dessa estrutura para classificar as ações da Universidade de Brasília (UnB) permite avaliar o grau de abrangência e coerência das iniciativas em relação aos fundamentos consagrados na literatura internacional (Treviño; Weaver; Brown, 2008).

A categoria de prevenção diz respeito às medidas adotadas para evitar a ocorrência de condutas inadequadas ou situações de risco antes que elas se materializem. A ênfase recai sobre a construção de uma cultura organizacional orientada à ética, ao cumprimento de normas e à sensibilização dos agentes públicos. Na UnB, foram classificadas como ações preventivas aquelas voltadas à produção e disseminação de conhecimento sobre os direitos e deveres institucionais, como campanhas de sensibilização, produção de cartilhas, promoção de cursos e eventos de formação e elaboração da Carta de Serviços ao Cidadão. Essas medidas visam promover o engajamento da comunidade acadêmica e fortalecer os valores institucionais.

A detecção, por sua vez, envolve o conjunto de mecanismos voltados à identificação precoce de desvios de conduta, riscos emergentes e falhas sistêmicas. Trata-se da capacidade institucional de perceber, monitorar e interpretar sinais de alerta com agilidade e precisão. Ações

como a implementação de canais de denúncia (e-OUV, ouvidoria presencial e online), o tratamento sistemático de manifestações recebidas e o acompanhamento de indicadores de riscos foram classificadas nessa dimensão. A literatura reconhece que a detecção eficaz depende não apenas da existência dos canais, mas também da credibilidade e da confiabilidade das instâncias responsáveis por seu funcionamento (Miceli; Neale; Neale, 2009).

A terceira função, resposta, compreende as ações tomadas após a identificação de um problema, com o objetivo de corrigir desvios, aplicar sanções, restaurar a confiança institucional e impedir a recorrência de práticas indevidas. A resposta eficaz exige clareza de procedimentos, responsabilização e transparência no desfecho dos casos. Na análise das ações da UnB, foram enquadradas como ações responsivas aquelas associadas ao tratamento de denúncias, elaboração de pareceres corretivos, revisão de normas e protocolos institucionais, e participação em instâncias deliberativas que avaliam e deliberam sobre situações concretas de risco ou desvio de conduta.

Esse tripé conceitual — prevenção, detecção e resposta — é amplamente utilizado em modelos de programas de compliance corporativo, como os sugeridos pela *U.S. Sentencing Commission* (1991), pelo *Department of Justice* dos EUA (2019), e por estudos acadêmicos clássicos sobre integridade organizacional (Tyler, 2006). Ele permite estruturar a atuação institucional com base na temporalidade do risco e na complexidade das medidas necessárias em cada etapa. A análise das ações da UnB com base nesse referencial revela uma forte presença de medidas preventivas e de detecção, indicando uma cultura institucional atenta à sensibilização e à escuta.

Por outro lado, a literatura sugere que a eficácia do sistema de integridade depende de um equilíbrio entre as três dimensões — sendo, portanto, recomendável o fortalecimento da dimensão responsiva por meio da normatização clara de sanções e do uso sistemático dos dados de integridade para retroalimentar os processos de decisão. Dessa forma, a classificação acadêmica fornece não apenas uma taxonomia útil para análise das ações institucionais, mas também uma orientação estratégica para a construção de programas de integridade robustos, coerentes e legitimados junto à comunidade universitária e à sociedade.

4.7. Núcleo comum de classificação

A presente seção tem por objetivo apresentar de forma sistemática o processo de identificação e análise da intersecção entre as políticas de Compliance e de Gestão de Riscos da Universidade de Brasília (UnB), quando classificadas segundo quatro referenciais metodológicos distintos: a ISO 31000, o COSO-ERM, o Referencial de Governança do TCU e a literatura acadêmica sobre o tema.

A partir da consolidação de ações previamente levantadas em documentos institucionais da UnB, essa análise responde à demanda de destacar quais políticas apresentam um núcleo comum de classificação, ou seja, quais dimensões aparecem de forma simultânea nos quatro referenciais, independentemente de suas diferenças conceituais ou estruturais. O resultado é um mapa de intersecção que evidencia os eixos de consenso e fornece subsídios para a compreensão da maturidade institucional da UnB na temática de governança e riscos.

Após as classificações em cada uma das metodologias apresentadas nessa secção, foram realizadas leituras cruzadas com o intuito de identificar os pontos de convergência entre os quatro referenciais. Nesse processo, o objetivo não foi buscar correspondências literais, mas sim interpretar a função desempenhada pelas ações em cada modelo.

Esse exercício de comparação semântica permitiu mapear como conceitos semelhantes são nomeados de formas distintas por diferentes frameworks, mas apontam para a mesma lógica de atuação institucional. Um exemplo é a forma como se apresenta o eixo da comunicação e da transparência. Na ISO, esse aspecto aparece como “Comunicação e Consulta”; no COSO-ERM, surge como “Informação e Comunicação”; no TCU, assume a forma de “Transparência”; e na literatura acadêmica, conecta-se ao papel preventivo das políticas de integridade. Embora a nomenclatura varie, todos esses termos expressam a mesma ideia central: a necessidade de promover abertura, engajamento e difusão de informações para sustentar a gestão de riscos e o fortalecimento da governança.

A análise das classificações mostrou que, apesar das diferenças conceituais entre os referenciais utilizados, existe um núcleo de consenso que se repete em todos os modelos: três grandes eixos que sustentam a governança de riscos e a política de compliance. Esses eixos foram denominados Comunicação, Transparência e Prevenção; Normatização, Controles Internos e Ética; e Monitoramento, Auditoria e Detecção. Juntos, eles configuram uma espécie de “mínimo

denominador comum" entre metodologias internacionais, nacionais e acadêmicas.

O primeiro eixo, de Comunicação, Transparência e Prevenção, destaca a centralidade da abertura institucional. Não há gestão de riscos eficaz sem que a comunidade envolvida compreenda as regras, participe do processo e disponha de canais confiáveis de escuta e de denúncia. Embora cada referencial trate desse tema de forma distinta — a ISO fala em "Comunicação e consulta", o COSO em "Informação e Comunicação", o TCU em "Transparência" e a literatura o conecta à "Prevenção"- todos convergem para a ideia de que a circulação de informações é a base da confiança institucional.

Na UnB, essa dimensão aparece concretamente em iniciativas como campanhas educativas, relatórios públicos, o fortalecimento da ouvidoria e a manutenção de portais de transparência.

O segundo eixo, de Normatização, Controles Internos e Ética, evidencia a necessidade de consolidar marcos formais para orientar a conduta organizacional. Regras claras, protocolos bem definidos e códigos de integridade reduzem a discricionariedade, previnem práticas indevidas e fortalecem a previsibilidade das decisões. Novamente, os referenciais apresentam nomenclaturas distintas: a ISO insere esse aspecto no "Tratamento de riscos", o COSO fala em "Atividades de Controle" e "Ambiente de Controle", o TCU o vincula a "Integridade e Controle", e a literatura o associa à prevenção por meio da cultura ética. Em todos os casos, o consenso é claro: sem normas e controles, não há solidez institucional. No contexto da UnB, destacam-se regimentos internos, manuais de integridade, protocolos administrativos e a atuação de comissões de ética e integridade.

O terceiro eixo identificado foi o de Monitoramento, Auditoria e Detecção, que se refere à supervisão contínua das práticas e ao aprendizado institucional por meio de correções e retroalimentações. A ISO nomeia esse processo como "Monitoramento e revisão", o COSO trata diretamente como "Monitoramento", o TCU insere no eixo de "Controle" e a literatura acadêmica chama de "Detecção".

Essa convergência mostra que o ciclo de gestão de riscos só se completa quando há mecanismos de acompanhamento e auditoria capazes de identificar falhas, corrigir rotas e aprimorar continuamente o sistema. Na UnB, esse eixo se materializa em auditorias internas, revisões periódicas de práticas e relatórios de acompanhamento, que servem como instrumentos

de aprendizado coletivo.

Ao observar os três eixos em conjunto, nota-se que eles não são apenas complementares, mas também interdependentes. A comunicação só é eficaz se houver normas e controles que deem suporte ao que está sendo divulgado. Do mesmo modo, controles só produzem efeito real se forem constantemente monitorados e auditados, permitindo a detecção de falhas. Por fim, auditorias e monitoramentos precisam ser comunicados à sociedade e à comunidade universitária para que a transparência legitime o processo. Assim, os três eixos formam um círculo virtuoso de governança, no qual cada elemento reforça os demais.

A identificação dessa intersecção é particularmente relevante porque demonstra que, apesar da diversidade de frameworks disponíveis, há um núcleo duro de práticas consensuais que devem ser priorizadas em uma organização que pretenda avançar em compliance e gestão de riscos. Para a UnB, esse diagnóstico aponta tanto para os avanços já consolidados, especialmente em comunicação e transparência, quanto para as lacunas ainda existentes, sobretudo na detecção e resposta a falhas.

Por fim, o reconhecimento dessa convergência metodológica fornece um critério seguro para orientar futuras políticas institucionais. Ao alinhar suas ações de forma equilibrada entre comunicação, normatização e monitoramento, a UnB não apenas cumpre boas práticas de governança, mas também fortalece sua legitimidade perante a sociedade. Além disso, esse núcleo de intersecção pode servir de referência comparativa em análises futuras, permitindo avaliar o grau de maturidade institucional ao longo do tempo e a evolução da universidade no campo do compliance e da gestão de riscos.

Para sintetizar os resultados, elaborou-se um diagrama de Venn, que demonstra graficamente a sobreposição entre os três eixos de intersecção. Cada círculo representa um eixo (Comunicação, Normas, Monitoramento), e o centro destaca o núcleo comum das quatro metodologias, que corresponde exatamente à tríade identificada: Comunicação/Transparência/Prevenção;Normatização/Controles/Ética e Monitoramento/Auditoria/Detecção.

Figura 1. Intersecção das 4 Metodologias de Risco e Compliance (UnB)

O

cruzamento metodológico mostrou que, mesmo diante da diversidade de frameworks, existe um núcleo comum de práticas indispensáveis para sustentar sistemas de compliance e gestão de riscos. Esse núcleo se estrutura em três pilares: Comunicação e Transparência, fundamentais para engajamento e construção de confiança; Normatização e Controles, que oferecem sustentação ética e institucional; e Monitoramento e Detecção, responsáveis por garantir a retroalimentação contínua e a correção de falhas.

No caso da UnB, observou-se que as ações institucionais documentadas estão mais fortemente concentradas no eixo da comunicação e transparência, evidenciando a ênfase em campanhas, portais e relatórios voltados ao diálogo com a comunidade. Há, contudo, também avanços relevantes em normatização e monitoramento, ainda que em proporções menores, o que indica que esses campos vêm sendo fortalecidos de forma gradual. Esse diagnóstico permite não apenas reconhecer os progressos realizados, mas também identificar lacunas e orientar futuras iniciativas. Assim, o mapeamento oferece uma visão integrada da governança universitária, permitindo compreender onde a instituição já apresenta maturidade e onde pode avançar. Ele também cria uma base sólida para análises futuras de impacto, ao indicar quais dimensões precisam de maior equilíbrio para consolidar um sistema de integridade robusto, legítimo e capaz de responder aos desafios de gestão de riscos no setor público.

5. RESULTADOS

5.1. Ações de políticas de *compliance* e gestão de riscos

A tabela seleciona as dez primeiras linhas da base ações gestão risco_compliance_classificados, que pode ser analisada, em sua integralidade, no anexo dessa dissertação. A fonte dessa tabela é de Elaboração própria, baseada em diversos documentos institucionais.

Quadro 4: Ações de Políticas de *Compliance* e Gestão de Riscos

Categoria	Tipo	Ação	Meta	Responsável (indicado ou provável)	Responsável Principal	Fonte	Classificação ISO 31000	Classificação COSO ERM	Classificação TCU	Classificação Academia
Compliance	Executada	Alinhamento dos procedimentos administrativos às normas da CGU/TCU	Atender às exigências dos órgãos de controle	Administração / Auditoria / Procuradoria	Administração Superior	PDI 2014–2017	Comunicação e consulta	Informação e Comunicação	Transparência	Prevenção
Compliance	Executada	Adoção de sistema de controle eletrônico de contratos e convênios	Garantir conformidade legal e efetividade dos recursos	Administração / CPD	Administração Superior	PDI 2014–2017	Comunicação e consulta	Atividades de Controle	Transparência	Prevenção
Compliance	Executada	Aprimoramento dos mecanismos de controle interno e conformidade	Fortalecer a transparência e responsabilidade administrativa	Administração / Auditoria / CPAD	Administração Superior	PDI 2018–2022	Comunicação e consulta	Atividades de Controle	Transparência	Prevenção
Gestão de Risco	Planejada	Criação de comissão de análise de riscos operacionais	Segurança patrimonial e organizacional	Administração / Segurança Institucional	Administração Superior	PDI 2002-2006	Análise de riscos	Avaliação de Riscos	Transparência	Prevenção
Gestão de Risco	Planejada	Aperfeiçoamento de mecanismos de controle da infraestrutura física e de segurança	Garantir a integridade de bens e pessoas	Administração / Segurança Institucional	Administração Superior	PDI 2008	Comunicação e consulta	Atividades de Controle	Transparência	Prevenção

Fonte: Elaboração própria.

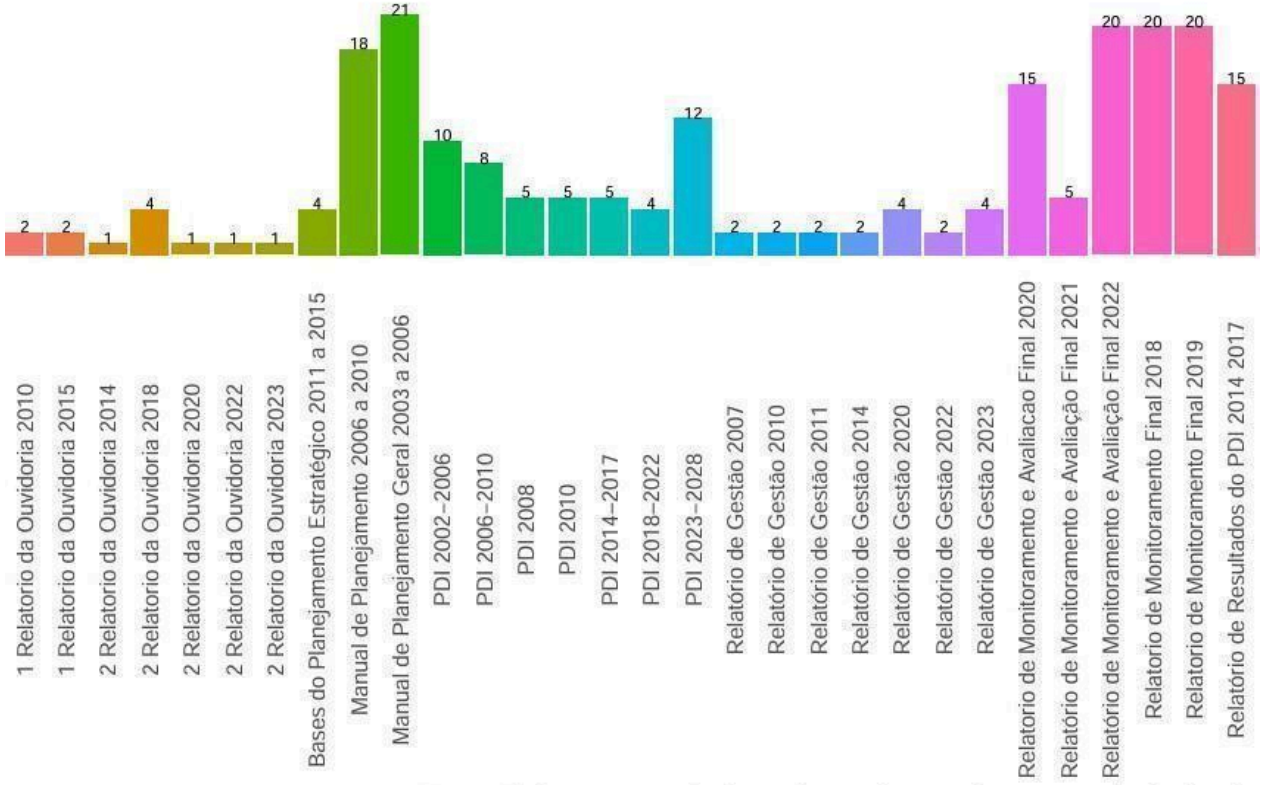
Fonte: elaborado pela autora

Ela reúne as dez primeiras ações registradas na base de dados de ações de gestão de risco e compliance. Ela apresenta, para cada ação de políticas de Compliance ou Gestão de Riscos, a categoria a que pertence, o tipo (se já executada ou apenas Planejada), a descrição da ação, a meta ou objetivo associado, o responsável indicado ou provável pela execução, e a fonte documental que embasou sua identificação. Além disso, as ações são classificadas conforme quatro referenciais: ISO 31000, COSO ERM, TCU e classificação acadêmica, seguidas do ano de

referência.

Os dados indicam que essas ações foram extraídas de documentos institucionais, especialmente dos Planos de Desenvolvimento Institucional (PDI), dos Relatórios de Gestão e dos Relatórios de Ouvidoria da Universidade de Brasília. Sua categorização permite compreender de forma estruturada como cada medida se alinha às práticas de controle, transparência, prevenção e gestão de riscos adotadas pela instituição.

Gráfico 1. Distribuição das ações por fonte



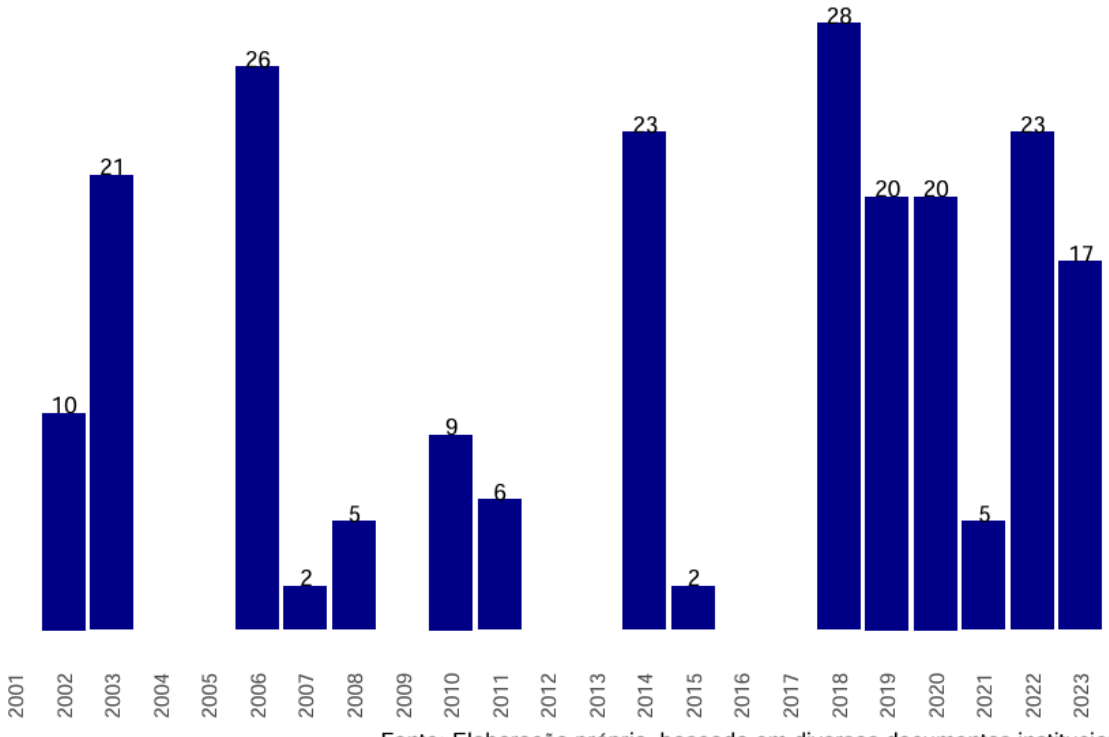
Fonte: Elaboração própria, baseada em diversos documentos institucionais.

O gráfico apresenta a distribuição das ações de políticas de Compliance e Gestão de Riscos segundo suas fontes documentais. Cada barra representa um documento institucional – como Relatórios da Ouvidoria, Planos de Desenvolvimento Institucional (PDI), manuais de planejamento, relatórios de gestão e relatórios de monitoramento – e a altura da barra indica a quantidade de ações identificadas nesse documento. A numeração acima de cada barra mostra o valor exato de ocorrências, facilitando a leitura precisa dos dados.

Observa-se que algumas fontes concentram maior número de ações, como o PDI 2006-2010 (21 ações), o PDI 2002-2006 (18 ações), e os Relatórios de Monitoramento e Avaliação Final de 2022 e 2019 (20 ações cada). Outros documentos, como determinados relatórios da ouvidoria ou relatórios de gestão, apresentam menor incidência, com apenas uma ou duas ações registradas. Essa variação indica que alguns instrumentos institucionais desempenham papel central na formalização e no acompanhamento dessas políticas, enquanto outros cumprem função mais pontual ou complementar.

No conjunto, o gráfico evidencia a importância estratégica de determinados períodos e documentos na consolidação de ações ligadas a compliance e gestão de riscos. Ele também sugere que a análise histórica das fontes pode revelar momentos de maior esforço institucional na implementação dessas políticas, permitindo identificar possíveis ciclos de planejamento e execução dentro da organização. Esse esforço no tempo pode ser melhor visualizado no gráfico 2, abaixo.

Gráfico 2. Distribuição das ações por Ano

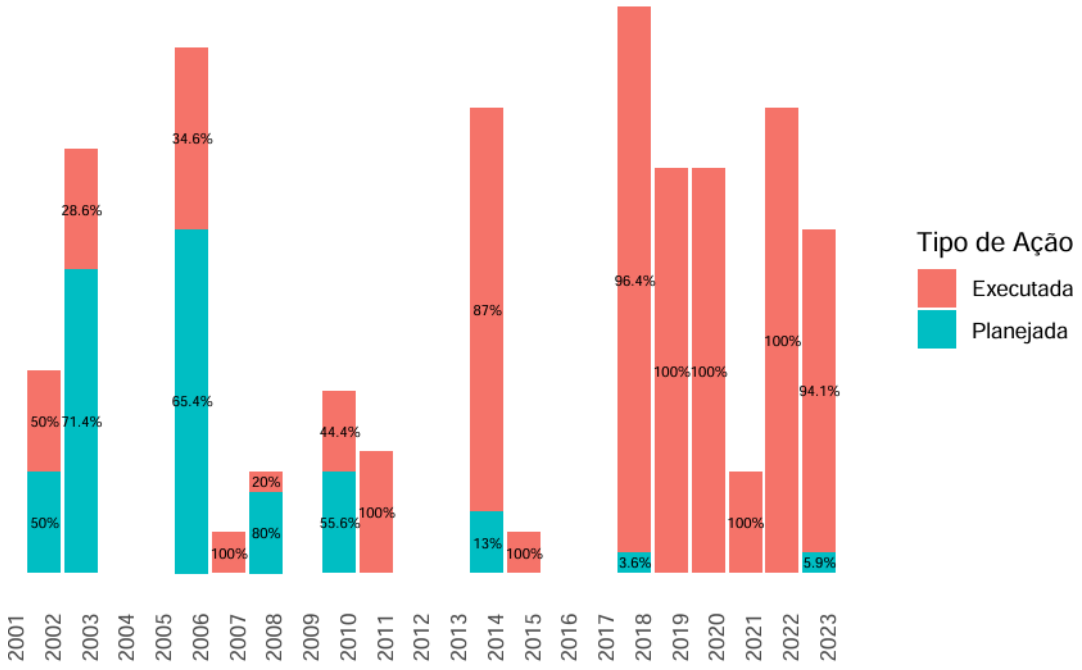


Fonte: Elaboração própria, baseada em diversos documentos institucionais.

Apresenta-se a distribuição das ações de *Compliance* e Gestão de Riscos identificadas na base de dados, organizadas por ano de referência. Cada barra corresponde ao número total de ações registradas em um determinado ano, permitindo visualizar a intensidade de registros ao longo do tempo. Os valores numéricos no topo das barras indicam a contagem exata de ações em cada ano, enquanto a escala do eixo X cobre o período de 2001 a 2023.

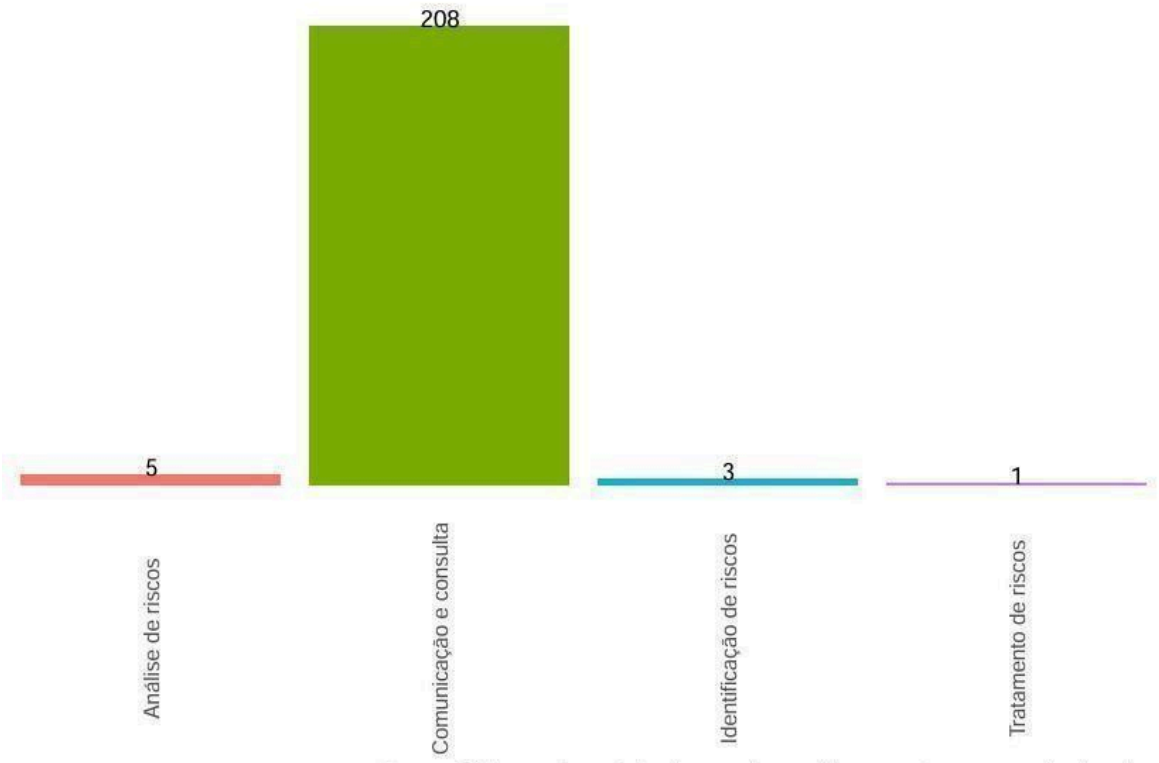
Observa-se que determinados anos concentram picos relevantes, como 2006 (26 ações), 2014 (23 ações), 2018 (28 ações) e 2022 (23 ações), sugerindo momentos de maior produção ou formalização de medidas institucionais ligadas a essas políticas. Em contrapartida, alguns anos apresentam registro mínimo ou inexistente, como 2004, 2005, 2009, 2012 e 2016. Esses anos que não apresentam políticas identificadas não são, necessariamente, lacunas ou variações na quantidade de iniciativas documentadas, mas, sim, o fato de que alguns documentos analisados apresentam planos bienais ou trienais. Para facilitar a análise dos dados, foram considerados, na classificação de anos, apenas os anos iniciais desses documentos. Essa distribuição temporal reflete ciclos de planejamento estratégico, mudanças regulatórias, revisões de PDI ou resposta a demandas de órgãos de controle.

Gráfico 3. Distribuição das Ações por Ano e Tipo (%)



Fonte: Elaboração própria, baseada em diversos documentos institucionais.

Gráfico 4. Distribuição das ações por Ano. Segundo Classificação ISO 31000



Fonte: Elaboração própria, baseada em diversos documentos institucionais.

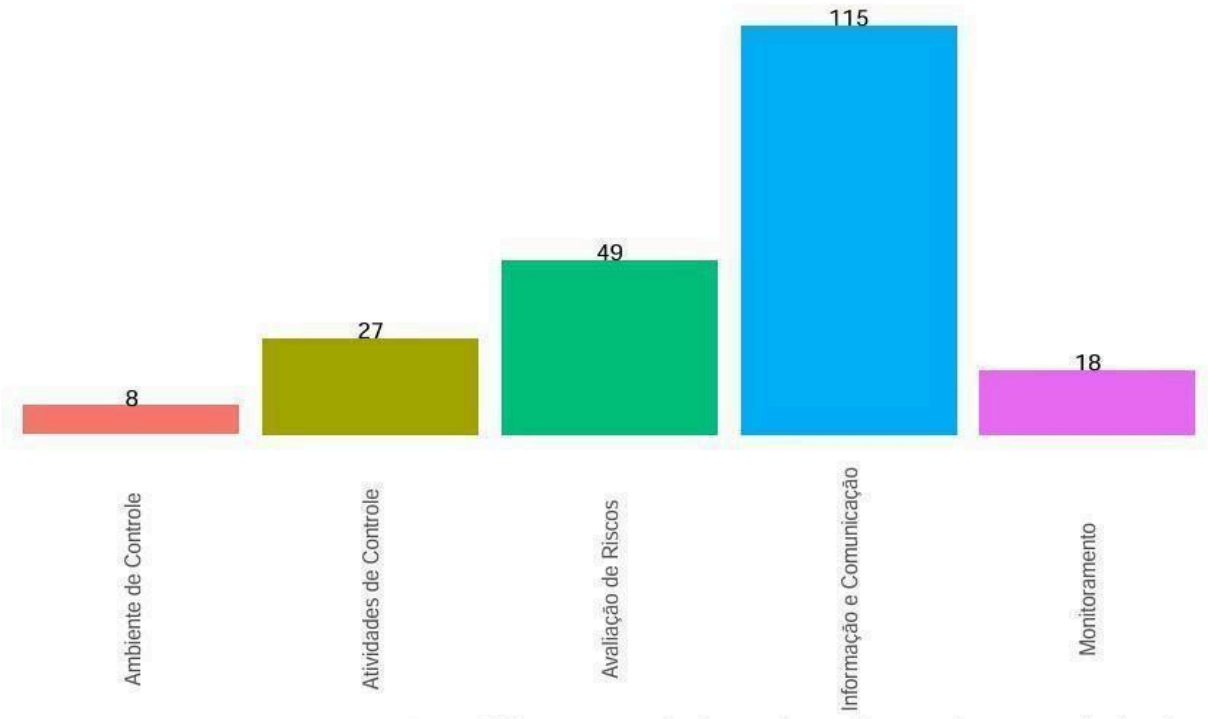
O gráfico apresenta a distribuição das ações de gestão de risco, segundo a classificação ISO 31000. Na UnB, evidencia-se concentração na categoria “Comunicação e consulta”. Esta classe reúne 208 registros, o que demonstra que a maior parte das iniciativas institucionais voltou-se para o compartilhamento de informações, o envolvimento de partes interessadas e a promoção da transparência no processo de gestão de riscos. Esse dado sugere que essa organização priorizou estratégias de engajamento e disseminação de conhecimento como fundamento para o sucesso das demais etapas do processo de gerenciamento.

As demais categorias apresentam participação significativamente menor. “Análise de riscos” contabiliza apenas 5 ocorrências, “Identificação de riscos” registra 3 e “Tratamento de riscos” apenas 1. Essa discrepância pode indicar que, embora o mapeamento e a comunicação sejam amplamente realizados, as ações mais voltadas para a avaliação e mitigação efetiva de riscos ainda não estão no mesmo nível de desenvolvimento. Tal cenário pode refletir limitações de recursos, priorização estratégica ou mesmo a etapa de maturidade atual do sistema de gestão

de riscos.

Assim, o panorama exposto pelo gráfico reforça a importância de equilibrar esforços entre todas as fases da gestão de riscos previstas na ISO 31000. Embora a comunicação seja essencial, um sistema robusto exige que identificação, análise e tratamento recebam atenção proporcional, permitindo que a instituição avance para um ciclo completo e contínuo de prevenção e mitigação de riscos, com base em dados, avaliação técnica e ações corretivas efetivas.

Gráfico 5. Distribuição das ações por Ano. Segundo Classificação COSO ERM



Fonte: Elaboração própria, baseada em diversos documentos institucionais.

O gráfico apresenta a distribuição das ações segundo a classificação COSO ERM, revelando maior concentração na categoria “Informação e Comunicação”, que soma 115 registros. Esse resultado indica que, também sob a égide da metodologia COSO, grande parte das iniciativas analisadas está relacionada à disseminação de informações, canais de comunicação internos e externos, e à garantia de que dados relevantes sobre riscos e controles cheguem aos tomadores de decisão. Em seguida, destacam-se “Avaliação de Riscos” com 49 ações e “Atividades de Controle” com 27, sugerindo que há um volume expressivo de medidas diretamente ligadas à análise e implementação de mecanismos de mitigação.

Outras categorias, como “Monitoramento” (18 ações) e “Ambiente de Controle” (8

ações), aparecem com menor frequência, embora sejam fundamentais para a manutenção da integridade e da eficácia do sistema de gestão de riscos. A menor quantidade nessas áreas pode indicar que, apesar de haver preocupação com a supervisão e a cultura de controle, essas ações são menos documentadas ou estão menos consolidadas em comparação com os esforços de comunicação e avaliação. Em resumo, o padrão observado reforça que, dentro da estrutura COSO, há uma ênfase considerável na comunicação como elo central do gerenciamento de riscos, mas também se percebe uma distribuição mais equilibrada entre outras fases do processo.

Em relação ao gráfico da ISO 31000, a diferença mais marcante está na dispersão das ações pelas categorias. No modelo ISO, a categoria “Comunicação e consulta” concentra quase todas as ações, enquanto “Identificação”, “Análise” e “Tratamento” aparecem de forma muito residual. Já no COSO ERM, embora “Informação e Comunicação” também lidere, há uma distribuição mais equilibrada, com destaque para “Avaliação de Riscos” e “Atividades de Controle”, que apresentam volumes expressivos. Ademais, o COSO ERM incorpora categorias não previstas na ISO 31000, como “Ambiente de Controle” e “Monitoramento”, o que amplia o espectro de classificação e permite captar ações que, no modelo ISO, poderiam ter sido absorvidas de forma genérica pela categoria dominante.

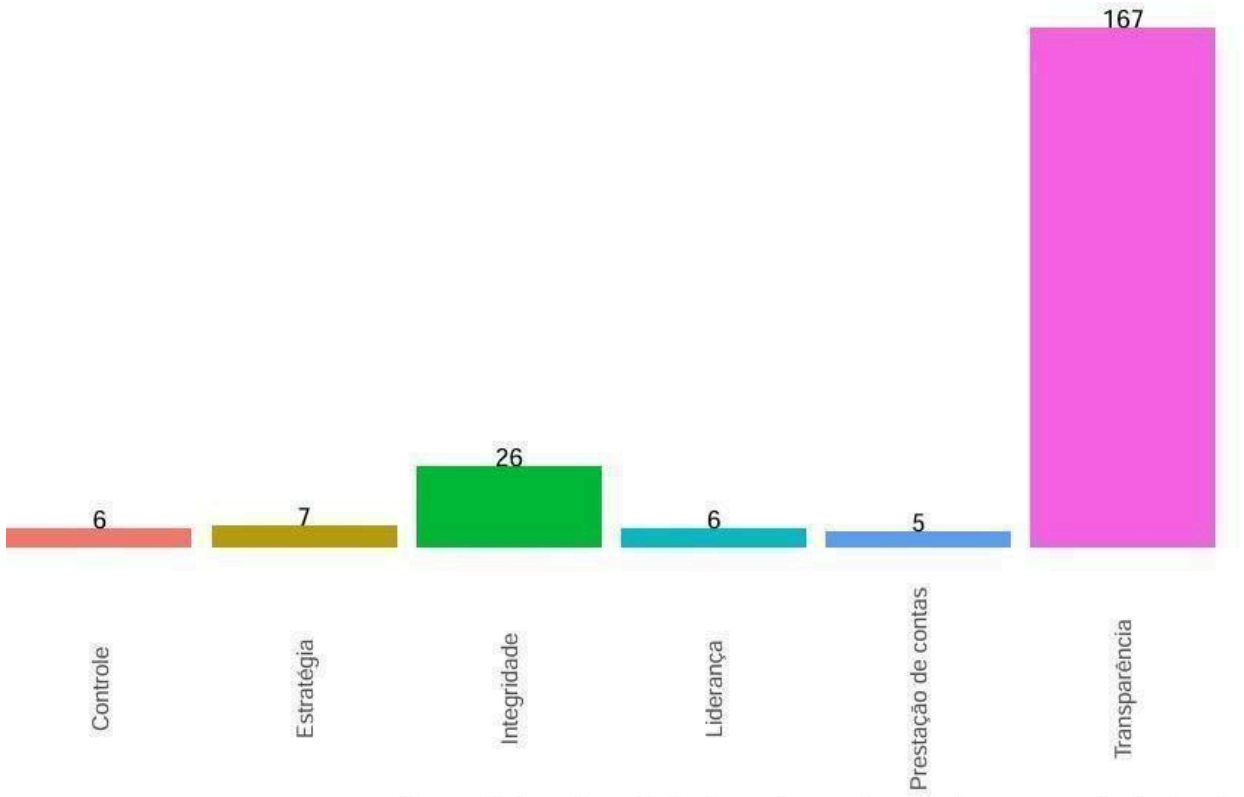
As diferenças supracitadas decorrem, principalmente, das abordagens distintas entre os dois referenciais. A ISO 31000 estrutura a gestão de riscos em um ciclo contínuo de etapas (comunicação, identificação, análise, avaliação e tratamento), enfatizando a integração desses elementos no processo decisório. Nesse sentido, ações que envolvem troca de informações, sensibilização e registro acabam absorvendo grande parte dos registros, especialmente quando a documentação institucional não descreve de forma clara as atividades técnicas de análise e tratamento.

Por outro lado, o COSO ERM adota uma visão mais abrangente e corporativa do gerenciamento de riscos, integrando-o à governança e ao controle interno. Isso permite que atividades relacionadas ao ambiente organizacional, monitoramento de desempenho e implementação de controles sejam reconhecidas e classificadas de forma independente, aumentando a diversidade nas categorias.

É possível que a predominância da “Informação e Comunicação” no ISO 31000 seja fruto de um viés documental, no qual a ênfase está em registrar esforços de sensibilização e

envolvimento de partes interessadas. No COSO ERM, essa mesma documentação é interpretada de maneira mais granular, permitindo que uma ação seja alocada em categorias como “Atividades de Controle” ou “Avaliação de Riscos” quando o conteúdo sugere ações operacionais ou de análise técnica.

Gráfico 6. Distribuição das ações por Ano. Segundo Classificação TCU



Fonte: Elaboração própria, baseada em diversos documentos institucionais.

O gráfico ilustra a distribuição das ações segundo a classificação do Tribunal de Contas da União (TCU), evidenciando a predominância da categoria “Transparência”, com 167 ações registradas. Esse resultado indica que a maior parte dos esforços documentados esteve voltada para ampliar a visibilidade das informações, fortalecer o acesso público a dados institucionais e garantir a publicidade de processos e decisões. Em seguida, a categoria “Integridade” surge com 26 ações, demonstrando atenção à promoção de condutas éticas, conformidade e combate a práticas ilícitas.

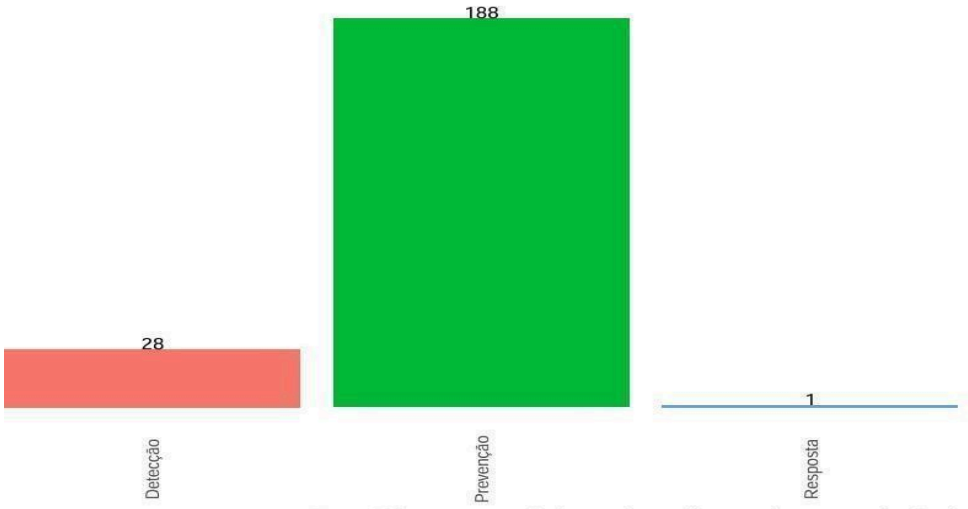
As demais categorias apresentam ocorrência reduzida: “Estratégia” (7 ações), “Controle” (6), “Liderança” (6) e “Prestação de contas” (5). Essa distribuição sugere que, apesar da relevância dessas dimensões para a boa governança, o foco predominante das iniciativas esteve

concentrado em mecanismos e práticas de transparência, possivelmente por exigências normativas e pela crescente demanda social por maior acesso à informação.

Em comparação aos modelos ISO 31000 e COSO ERM, a abordagem TCU mostra um viés mais orientado a princípios de governança e accountability do setor público. Enquanto na ISO 31000 predominou "Comunicação e consulta" e no COSO ERM houve uma distribuição mais equilibrada entre "Informação e Comunicação" e "Avaliação de Riscos", o modelo do TCU concentra fortemente suas ações em "Transparência", deixando as demais dimensões com peso consideravelmente menor. Ainda, a classificação do TCU não é estruturada em etapas de processo ou componentes técnicos de gestão de riscos, mas em eixos de governança, o que leva a uma categorização mais política e institucional das ações.

Ações que no ISO ou no COSO poderiam ser registradas como "comunicação" ou "monitoramento" podem ser classificadas no TCU como "transparência" ou "integridade", uma vez que o enquadramento se dá pelo valor institucional promovido, e não apenas pela função técnica do processo. Isso explica porque a categoria "Transparência" aparece tão dominante — muitas iniciativas que visam comunicação ou prestação de informações podem ser interpretadas, à luz do modelo TCU, como medidas de promoção da transparência. Enfim, a ênfase do TCU também reflete demandas regulatórias e pressões externas próprias do setor público brasileiro, especialmente no contexto de combate à corrupção e fortalecimento da governança, o que não é central nos frameworks internacionais como a ISO 31000 e o COSO ERM.

Gráfico 7. Distribuição das ações por Ano. Segundo Melhor Literatura



Fonte: Elaboração própria, baseada em diversos documentos institucionais.

O gráfico apresenta a distribuição das ações de acordo com a categoria “Melhor Literatura” identificada nessa dissertação, evidenciando forte predominância da Prevenção, com 188 registros. Esse resultado mostra que a maior parte das iniciativas institucionais documentadas se concentra na adoção de medidas proativas para evitar a ocorrência de riscos, fraudes ou problemas operacionais, alinhando-se às melhores práticas internacionais que enfatizam a prevenção como eixo central de políticas de integridade e governança.

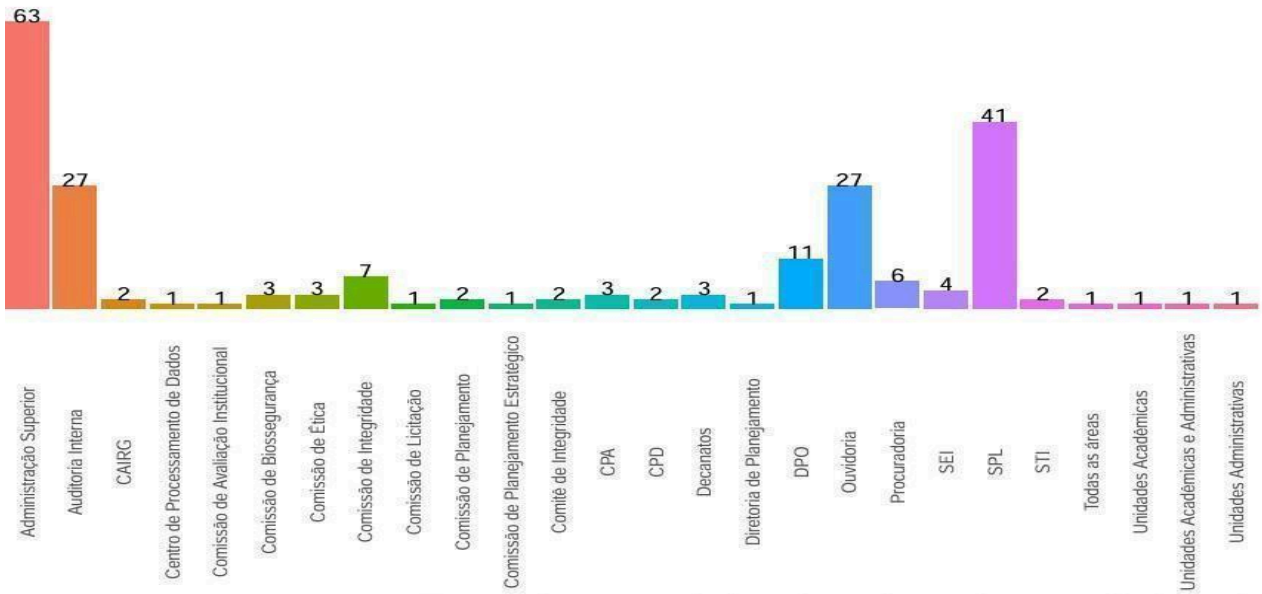
A categoria Detecção aparece com 28 ações, demonstrando que há também um investimento considerável em mecanismos de monitoramento, auditoria e identificação precoce de irregularidades, mas ainda em volume significativamente menor do que a prevenção. Por fim, Resposta registra apenas 1 ação, o que indica baixa ênfase em medidas corretivas ou reativas, possivelmente por priorizar uma abordagem antecipatória que busca evitar a necessidade de respostas emergenciais.

Quando comparado aos modelos ISO 31000, COSO ERM e TCU, observa-se que o enfoque da “Melhor Literatura” é mais sintético e orientado para o ciclo temporal de enfrentamento de riscos (prevenção → detecção → resposta), enquanto os outros frameworks distribuem as ações por funções organizacionais ou princípios de governança. Assim como no ISO e no TCU, há forte concentração em uma única categoria, mas aqui essa categoria dominante é “Prevenção”, reforçando o caráter preventivo da abordagem. Além disso, diferentemente do COSO ERM, que apresentou uma distribuição relativamente mais equilibrada entre várias dimensões, o modelo da “Melhor Literatura” mantém um viés concentrado, o que pode indicar uma priorização explícita por estratégias proativas e de mitigação antes do surgimento de problemas.

A ênfase em “Prevenção” decorre da própria filosofia das boas práticas compiladas em referências internacionais, que recomendam investir prioritariamente em mecanismos que evitem a materialização de riscos. Isso leva a um desenho de políticas mais voltado à antecipação, educação, controles internos robustos e cultura organizacional voltada à integridade. Deve-se ressalvar que a baixa incidência de ações em “Resposta” não indica, necessariamente, fragilidade; mas a possibilidade de que em um sistema preventivo eficaz, há menos demanda por intervenções emergenciais. Em muitos casos, as respostas estão integradas aos próprios protocolos de prevenção e detecção, aparecendo de forma indireta na documentação institucional.

A proporção relativamente menor em “Detecção” pode estar relacionada à priorização de medidas preventivas como barreira primária, deixando os mecanismos de monitoramento como suporte. Ainda assim, o equilíbrio entre prevenção e detecção é considerado essencial para um

Gráfico 8. Distribuição das ações por Ano. Segundo Melhor Literatura



Fonte: Elaboração própria, baseada em diversos documentos institucionais.

sistema maduro, e o dado sugere espaço para fortalecer instrumentos que identifiquem riscos residuais ou novas ameaças não previstas no planejamento inicial.

O gráfico apresenta a distribuição das ações por unidade responsável, evidenciando forte concentração em instâncias centrais de governança. “Administração Superior” lidera com 63 registros, seguida por “SPL” (41), “Ouvidoria” (27) e “Auditoria Interna” (27). Também se destacam, em menor escala, o “DPO” (11) e a “Procuradoria” (6).

Esse padrão indica que a maior parte das iniciativas esteve coordenada por áreas estratégicas e de controle, típicas de agendas transversais como integridade, gestão de riscos e transparência. As demais categorias reúnem frequências reduzidas e dispersas, como comissões temáticas (Integridade, Ética, Biossegurança, Licitação), como instâncias de planejamento e avaliação (CPA/CPD/Comissão de Planejamento), como áreas técnico- operacionais (STI, SEI, CPD) e como unidades acadêmicas/administrativas. Essa distribuição diversa sugere ações mais pontuais ou focalizadas, muitas vezes de natureza executiva ou de apoio, enquanto as áreas centrais concentram diretrizes, normatizações e marcos institucionais.

Cabe-se ressalvar que, para melhorar a visualização e evitar sobrecarga de rótulos, utilizou- se o principal responsável por cada ação (isto é, a unidade líder do processo); contudo, várias iniciativas contam com corresponsáveis. Todos esses podem ser identificados na Tabela 1, no apêndice, permitindo rastreabilidade completa e conferência detalhada.

5.2. Uma proposta de mensuração

O objetivo dessa secção é finalizar a metodologia com uma proposta de teste para analisar se as políticas implementadas produziram efeitos relativamente maiores justamente nas contas mais sensíveis às políticas de compliance/gestão de risco. A hipótese de trabalho é: as contas classificadas com alta sensibilidade apresentam variações mais "racionais" (p. ex., reduções proporcionais de dispêndios em itens onde o risco é controlável, como precatórios/sentenças, fraudes, ineficiências) quando comparadas às contas de média e baixa sensibilidade.

Para isso, seria necessário cruzar duas bases de dados: a primeira, contendo as ações de gestão de risco e compliance, com informações sobre o ano de execução, tipo (gestão de risco ou compliance), descrição, metas e responsáveis, como a construída a partir dos relatórios institucionais; e a segunda, composta pela despesa desagregada da UnB consolidada para cada ano, a qual seriam classificadas quanto a sensibilidade (alta, média ou baixa), bem como valores orçamentários anuais. Inicialmente, proceder-se-ia à harmonização temporal (garantindo consistência no formato de datas e anos) e à criação de um dicionário de correspondência semântica entre palavras-chave presentes nas metas e ações e os grupos de despesa da PLOA. Essa vinculação é essencial para associar cada ação a uma ou mais contas, permitindo avaliar a coerência entre as políticas implementadas e as áreas de maior potencial impacto.

Utilizar-se-ia, então, uma base unificada com (conta, ano, valores por fonte/total e sensibilidade da conta). Antes da análise estatística, proceder-se-ia, também, a padronização temporal por meio do deflacionamento dos valores monetários em relação a Dezembro de 2023 (útlimo ano da série histórica). Dividir-se-ia essa série em quatro blocos, alinhados aos ciclos de planejamento encerrados: 2006–2010, 2011–2014, 2015–2018, 2019–2023. Para cada conta = i e período p, calcular-se-ia um impacto percentual que resumiria a variação dentro do quadriénio. A forma canônica é a variação entre o primeiro e o último ano do período, conforme fórmula I, a seguir:

$$FórmulaI.Impacto_{i,p} = \frac{V_{i,t_{fim}}(p) - V_{i,t_{ini}}(p)}{max[\epsilon, V_{i,t_{ini}}(p)]}$$

Na fórmula I, acima, v é o valor deflacionado da conta e $\epsilon > 0$ é um pequeno termo de estabilidade para evitar divisão por zero. O resultado desta etapa são quatro colunas de impacto (uma por quadriénio) para cada conta, preservando sua classificação de sensibilidade. Com os impactos por conta e período, seguir- se-ia a comparação entre as distribuições de impacto entre os níveis alto, médio e baixo. Inicialmente, a comparação seria feita dentro de cada quadriénio (para não misturar conjunturas distintas) e, posteriormente, em um painel agregado (todos os quadriênios).

Em hipóteses, assumir-se-ia a não normalidade e a presença de heteroscedasticidade nos dados, o que poderia ser avaliado por meio de um Teste de Shapiro-Wilk. Confirmada essas hipóteses, aplicar-se-ia um Teste de Mann-Whitney (U), cuja abordagem não paramétrica se encaixa nas hipóteses levantada. Ademais, como os p-valores, isoladamente, não quantificam a magnitude prática, buscar-se-ia o valor do efeito de Clif's delta e, para o controle de múltiplas comparações, aplicar-se-ia o ajuste de Holm ao conjunto de p- valores dentro de cada quadriênio.

Como nosso $H0$ é que as contas classificadas com alta sensibilidade apresentam variações mais "racionais", evidenciando o êxito das políticas institucionais, esperar-se- ia que os impactos médios/medianas em alta sensibilidade sejam mais favoráveis (p. ex., reduções proporcionais maiores em despesas "controláveis" ou estabilização quando a meta for contenção de crescimento), e os testes entre alto e (médio/baixo) indicassem diferença estatisticamente significante (nível $\alpha = 0,05$, com ajuste por múltiplos testes), com tamanho de efeito pelo menos moderado.

Na ausência de significância, há três leituras possíveis: (i) as políticas ainda não se traduziram em resultados mensuráveis, (ii) a classificação de sensibilidade precisa ser refinada, ou (iii) choques exógenos (legais, macrofiscais) mascaram o efeito. Nessas situações, análises complementares (p. ex., regressões em painel com efeitos fixos e variáveis de "tratamento"/exposição por período) podem aumentar a potência inferencial.

Como etapa final, a análise poderia ser enriquecida por visualizações: boxplots ou violinplots comparando a distribuição dos impactos por sensibilidade em cada quadriénio, linhas do tempo evidenciando a implementação de políticas e sua correlação com variações

orçamentárias, e heatmaps para destacar padrões de impacto. Essas representações facilitam a compreensão de tendências e outliers.

A execução ordenada dessas etapas — higienização e deflação dos dados, vinculação semântica entre ações e contas, cálculo de impactos por quadriénio, estratificação por sensibilidade, aplicação de testes estatísticos e interpretação contextualizada — fornece um método transparente e reprodutível, alinhado a práticas robustas de avaliação de políticas públicas. Assim, será possível fundamentar com rigor se as políticas de gestão de risco e compliance estão, de fato, promovendo uma alocação orçamentária mais racional, concentrando ganhos nas áreas onde seu efeito potencial é maior.

6. CONCLUSÃO

Esta dissertação analisou os benefícios, as diferenças conceituais e a aplicabilidade dos programas de compliance e de gestão de riscos na Universidade de Brasília (UnB), evidenciando a existência de um núcleo comum de práticas voltadas ao fortalecimento da governança pública. Os resultados indicam que a integração dessas abordagens contribui para a prevenção de irregularidades, o aumento da transparência e o aprimoramento da tomada de decisão institucional, em consonância com a Lei nº 12.846/2013 e com referenciais amplamente adotados na literatura e na prática, como a ISO 31000 e o COSO ERM.

O mapeamento institucional identificou 217 ações relacionadas à integridade e à gestão de riscos, com predominância de iniciativas preventivas (188 ações). Observou-se significativa ênfase em comunicação e transparência, refletida nos registros associados à ISO (208 ocorrências) e ao TCU (167 ocorrências). Em contrapartida, as dimensões de detecção (28 ações) e, sobretudo, de resposta a eventos de risco (1 ação) apresentaram menor desenvolvimento, indicando um estágio de maturidade organizacional ainda assimétrico, com maior concentração em controles *ex ante* (preventivos), caracterizados por normas, treinamentos, orientações, procedimentos formais e ações de comunicação institucional, em detrimento de mecanismos voltados à detecção de problemas em curso (*ex post*) e à resposta a eventos já materializados.

No que se refere à mensuração e ao apoio à decisão, o estudo demonstrou a viabilidade da utilização de métodos estatísticos aplicados à análise de despesas sensíveis. Essa abordagem apresenta potencial para auxiliar a alocação mais eficiente de recursos públicos e para o fortalecimento dos mecanismos de monitoramento, sem demandar elevados custos de implementação, aspecto particularmente relevante no contexto das instituições públicas de ensino superior.”

Entre as principais contribuições do trabalho, destaca-se a consolidação dos principais frameworks normativos e gerenciais em uma estrutura analítica rastreável, permitindo diferenciar o compliance, com foco ético-legal e normativo, da gestão de riscos, voltada à antecipação de impactos operacionais e estratégicos. Adicionalmente, a pesquisa propõe instrumentos de análise mensurável aplicáveis às Instituições Federais de Ensino Superior (IFES), ampliando as

possibilidades de avaliação da maturidade institucional em governança, integridade e controle.

No contexto específico da UnB, os achados oferecem subsídios concretos para o aperfeiçoamento de um programa de integridade alinhado à realidade institucional, às capacidades organizacionais existentes e às demandas por maior accountability. As recomendações priorizam o fortalecimento gradual das dimensões de monitoramento, resposta e mensuração de riscos, de forma integrada aos processos preventivos já consolidados.

Como limitações, reconhece-se a dependência de documentos institucionais com diferentes níveis de detalhamento, bem como a disponibilidade parcial de dados para análises mais aprofundadas de custo-benefício, o que restringe generalizações imediatas. Estudos futuros podem ampliar a validação empírica das ferramentas propostas, tanto na UnB quanto em outras IFES, bem como aprofundar a integração entre compliance, gestão de riscos e práticas contemporâneas de governança pública orientada a evidências.

REFERÊNCIAS

ABRUCIO 2020

ABNT NBR ISO 31000:2018

AMORIM; GUEVARA; SANTOS 2013

ASSI 2018

ÁVILA (2014

AYRES, 2023

BATTESINI 2011

BARALDI 2005

BEASLEY *et al*. 2017

BLANCHET, 2023

BLOK, 2020

BOVAIRD; LOEFFLER; VAN RYZIN 2017

BOVAIRD *et al*. 2017

BRASIL, 2006

BRYMAN; BELL 2006

CARVALHO; MENDES 2017

CARVALHOSA, 2015

CATLETT 2013

CGU, 2022

CIEKALSKI 2019

CICCO 2017

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

COSTA 2009

COIMBRA, Marcelo de Aguiar; MANZI, Vanessa Alessi (coord.). **Manual de compliance**: preservando a boa governança e a integridade das organizações. São Paulo: Atlas, 2010.

COSTA; MENDES 2017

DAMODARAN 2019

DENZIN 1970

DIAS; RIBEIRO 2019

DI PIETRO 2019

FERRAZ JUNIOR, Tércio Sampaio 2015

FERREIRA, Almeida 2013

FERREIRA; QUEIROZ 2018

FRASER; SIMKINS 2010

FRAZÃO 2015

GABAN; DOMINGUES 2016

GABARDO; CASTELLA 2015

GALANTE 2015

HELDMAN 2006

HILLSON 2019

HILLSON; MURRAY-WEBSTER 2012

HOOD 1991

JORDACE 2017

JUNQUEIRA 2021

JUSBRASIL 2024

KAPLAN; MIKES 2012

KERZNER 2011

LEC 2018

MANZI 2008

MARTINS, Adriano Oliveira. **Gestão de risco de compliance** - principais entraves para as empresas brasileiras atingirem maior maturidade. Dissertação (Mestrado Profissional em Gestão e Negócios) — Universidade do Vale do Rio dos Sinos, Porto Alegre, 2018. Disponível em: http://www.repositorio.jesuita.org.br/ handle/UNISINOS/7339. Acesso em: 18 jan. 2026.

MEDAUAR 2018

MELLO, Bandeira de, 2021

MESQUITA 2019

MICELI; NEALE; NEALE 2009

MORAES 2010

MOELLER 2011

NERON; PORTELLA 2018

NIGLAS 2004

NOCÊRA 2009

OCDE 2009

OCDE, 2021

OLIVEIRA; SANTOS 2020

PMI 2012

POWER 2007

RAINHO 2023

RIBEIRO, Márcia Carla Pereira; DINIZ, Patrícia Daniella de Faria. Compliance e Lei Anticorrupção nas empresas. **Revista de Informação Legislativa**, Brasília, v. 52, n. 205, p. 87–105, jan./mar. 2015.

ROCHA; FERNANDES 2020

ROTSCH 2012

SANTOS, Renato Almeida dos. Compliance como ferramenta de mitigação e prevenção da fraude organizacional. **6º Concurso de Monografias** Controladoria Geral da União, 2011. Disponível em: http://repositorio.enap.gov.br/handle/1/5687. Acesso em: 18 jan. 2026.

SANTOS; HOYOS; AMORIM, 2013

SILVA 2015

SILVA, Carvalho Neto 2009

SILVA; COVAC, 2019

SILVA; CAMPOS, 2022

SILVEIRA; SAAD-DINIZ 2012

SOUZA, Machado de; VIANNA, Pontes 2020

TREVIÑO, Linda Klebe; WEAVER, Gary R.; BROWN, Michael E. It's lovely at the top: hierarchical levels, identities, and perceptions of organizational ethics. **Business Ethics Quarterly**, Cambridge, v. 18, n. 2, p. 233–252, 2008.

TRIBUNAL DE CONTAS DA UNIÃO (TCU). **Roteiro de avaliação de maturidade da gestão de riscos**. Brasília, DF: TCU, 2016

TYLER, Tom R. **Why people obey the law**. Princeton: Princeton University Press, 2006.

VASCONCELOS; SOARES 2022

VENOSA; Silvio de Salvo 2014

WOOLEY 2008