Especialização em
Auditoria e Controle Interno

Gestão de Risco e *Compliance*

Ana Raquel Silva Rocha Sudério

Especialização em Auditoria e Controle Interno

Especialização em Contabilidade Pública

Especialização em Controladoria Pública

Especialização em Gestão Pública

Especialização em Gestão Pública Municipal

Especialização em Alfabetização e Multiletramento

Especialização em Tecnologias Digitais na Educação Básica

Especialização em EaD

Especialização em Gestão Pedagógica

Especialização em Língua Inglesa

Especialização em Educação Física na Educação Básica

Especialização em Audiodescrição

Especialização em Legendagem

Especialização em Artes

Especialização em
Auditoria e Controle Interno

Gestão de Risco e *Compliance*

Ana Raquel Silva Rocha Sudério

Fortaleza
EdUECE
2024

Especialização em Auditoria e Controle Interno
Especialização em Contabilidade Pública
Especialização em Controladoria Pública
Especialização em Gestão Pública
Especialização em Gestão Pública Municiapl
Especialização em Alfabetização e Multiletramento
Especialização em Tecnologias Digitais na Educação Básica
Especialização em EaD
Especialização em Gestão Pedagógica
Especialização em Lingua Inglesa
Especialização em Educação Física na Educação Básica
Especialização em Audiodescrição
Especialização em Legendagem
Especialização em Artes

Gestão de Risco e *Compliance*
©2024 *Copyright by* Autores/Orgnizadores

O conteúdo deste livro, bem como os dados usados e sua fidedignidade, são de responsabilidade exclusiva do autor. O download e o compartilhamento da obra são autorizados desde que sejam atribuídos créditos ao autor. Além disso, é vedada a alteração de qualquer forma e/ou utilizá-la para fins comerciais.

Presidenta da República
Luiz Inácio Lula da Silva

Ministro da Educação
Camilo Sobreira de Santana

Presidente da CAPES
Denise Pires de Carvalho

Diretor de Educação a Distância da CAPES
Suzana dos Santos Gomes

Governador do Estado do Ceará
Elmano de Freitas da Costa

Reitor da Universidade Estadual do Ceará
Hidelbrando dos Santos Soares

Vice-Reitor
Dárcio Italo Alves Teixeira

Pró-Reitora de Pós-Graduação
Ana Paula Ribeiro Rodrigues

Coordenador da SATE e UAB/UECE
Francisco Fábio Castelo Branco

Coordenadora Adjunta UAB/UECE
Eloísa Maia Vidal

Direção do CESA
José Joaquim Neto Cisne

Editora da EdUECE
Cleudene de Oliveira Aragão

Coordenação Editorial
Eloísa Maia Vidal

Assistente Editorial
Nayana Pessoa

Projeto Gráfico e Capa
Roberto Santos

Revisão Textual
Eleonora Lucas

Diagramador
Francisco Saraiva

Conselho Editorial
Ana Carolina Costa Pereira
Ana Cristina de Moraes
André Lima Sousa
Antonio Rodrigues Ferreira Junior
Daniele Alves Ferreira
Erasmo Miessa Ruiz
Fagner Cavalcante Patrocínio dos Santos
Germana Costa Paixão
Heraldo Simões Ferreira
Jamili Silva Fialho
Lia Pinheiro Barbosa
Maria do Socorro Pinheiro
Paula Bittencourt Vago
Paula Fabricia Brandão Aguiar Mesquita
Sandra Maria Gadelha de Carvalho
Sarah Maria Forte Diogo
Vicente Thiago Freire Brazil

Dados Internacionais de Catalogação na Publicação (CIP)
(Câmara Brasileira do Livro, SP, Brasil)

Sudério, Ana Raquel Silva Rocha
Gestão de risco e compliance [livro eletrônico] / Ana Raquel Silva Rocha Sudério. -- 1. ed. -- Fortaleza, CE : Editora da UECE, 2025.
PDF

Bibliografia
ISBN 978-65-83910-59-2

1. Administração 2. Compliance 3. Gestão de risco 4. Governança corporativa 5. Sustentabilidade organizacional I. Título.

25-310590.0 CDD-658.47

Índices para catálogo sistemático:

1. Gestão de riscos : Administração 658.47

Maria Alice Ferreira - Bibliotecária - CRB-8/7964

Editora da Universidade Estadual do Ceará – EdUECE
Todos os direitos reservados
Editora da Universidade Estadual do Ceará – EdUECE
Av. Dr. Silas Munguba, 1700 – Campus Itaperi – Reitoria – Fortaleza – Ceará
CEP: 60714-903 – Tel: (085) 3101-9893
www.uece.br/eduece – E-mail: eduece@uece.br

Editora filiada à
ABEU
ASSOCIAÇÃO BRASILEIRA DAS EDITORAS UNIVERSITÁRIAS

Sumário

Apresentação

Caro/a estudante,

Bem-vindo/a ao mundo da Gestão de Riscos e *Compliance*!

Este material didático, utilizado na disciplina de mesmo nome, tem como objetivo fornecer conhecimentos e habilidades que contribuam com a formação de profissionais aptos a identificar, avaliar e gerenciar os riscos que uma organização enfrenta, a lidar proativamente com os desafios de um ambiente cada vez mais regulamentado, e a garantir que as organizações – sejam públicas ou privadas – operem em conformidade com leis, regulamentos, políticas internas e padrões éticos, garantindo sua sustentabilidade e sucesso a longo prazo.

Você será guiado/a através de quatro capítulos fundamentais que facilitarão o seu processo de aprendizado.

O primeiro capítulo estabelece as bases para o entendimento do que é o risco e porque é tão importante conhecê-lo para desempenhar funções em qualquer organização. Serão explorados os elementos básicos que compõem o risco, bem como diferentes tipos de riscos que as empresas enfrentam e suas naturezas.

O segundo capítulo viabilizará um mergulho mais fundo na gestão estratégica de riscos. Você entenderá o que é gestão de riscos, conhecerá os princípios que fundamentam essa prática e será apresentado às principais fases que compõem um processo de gestão de riscos abrangente e eficaz.

O terceiro capítulo te conduzirá a um tema diretamente relacionado ao risco: o *compliance*. Serão descritos os pilares que sustentam as práticas de conformidade e compartilhados alguns dos principais desafios associados à implantação do *compliance* nas organizações.

O quarto capítulo lançará luz sobre uma ferramenta essencial para garantir a conformidade com as regulamentações e a minimização dos riscos: o controle interno. Você entenderá o que são controles internos, seus benefícios e importância, bem como verá quais são os seus componentes essenciais que contribuem para o funcionamento eficaz das práticas de controle.

Com uma abordagem acessível e prática, este livro é dedicado aos profissionais – do âmbito público e privado - e aos estudantes que desejam entender e dominar os fundamentos de Gestão de Riscos e *Compliance*.

Esperamos que você aproveite a jornada e busque conhecer cada vez mais sobre as temáticas aqui apresentadas para impulsionar o sucesso de sua carreira.

Boa leitura!

Capítulo 1

Introdução ao Risco

Objetivos

- Definir o conceito de risco sob uma perspectiva multidisciplinar;
- Identificar e explicar os elementos básicos que compõem o risco;
- Compreender as diferentes classificações de riscos;
- Avaliar criticamente a importância da compreensão sobre riscos para o sucesso empresarial.

Introdução

Desde os primórdios da civilização, o ser humano está cercado pelo risco, de forma voluntária e involuntária. Tal fato fundamenta a inferência de que, se ao longo tempo a civilização tem se desenvolvido e avançado, isso se deve à disposição anterior de alguém a enfrentar os riscos.

Ao conhecer, brevemente, uma perspectiva histórica sobre esse tema, com enfoque especial ao mundo dos negócios modernos, torna-se cada vez mais perceptível que o entendimento e o gerenciamento dos riscos são essenciais para a sustentabilidade e o crescimento das empresas em um ambiente que, ao longo do tempo, se desenvolve de formas mais voláteis e complexas.

Nesse sentido, compreende-se que a conceituação do risco pode variar entre diferentes áreas do conhecimento e de negócios, mas o que se estabelece é que há uma conscientização acerca da não limitação do risco a uma ideia simples de perda, suscitando dos tomadores de decisões, dos analistas profissionais e dos estudantes uma apreensão mais abrangente, que englobe diversas dimensões, como os elementos básicos que compõem o risco e as diferentes classificações existentes, as quais contemplam uma ampla gama de categorias, desde os riscos mais comuns até os mais específicos.

1. Breve histórico sobre o Risco

Falar sobre risco é falar sobre algo que é intrínseco à história da civilização. Autores como Bernstein (1997) e Damodaran (2009) nos apresentam particularidades dos diferentes períodos históricos que ilustram variadas for-

mas pelas quais os indivíduos – filósofos, matemáticos, cientistas, mercadores, jogadores, etc – auxiliaram o desenvolvimento de métodos que, na atualidade, viabilizam o olhar sobre riscos futuros a serviço do momento presente. De fato, não é de agora que a humanidade encara situações de risco para obter retornos:

- Nas sociedades primitivas, o homem era exposto, predominantemente, aos riscos físicos, como ataques de animais e fenômenos climáticos, enfrentando-os para o seu principal retorno: a sobrevivência;
- Na idade média e renascimento, o comércio e a exploração marítima lançaram luz sobre novos tipos de riscos. Além de encararem riscos ligados às guerras e aos novos tipos de doenças, os povos passaram a lidar também com riscos econômicos, especialmente relacionados a perdas de mercadorias dos comerciantes em roubos nas estradas, ataques piratas ou em naufrágios, mas que eram fonte de bons lucros quando as transações eram bem-sucedidas;
- Na revolução industrial, os riscos passaram a adquirir maior complexidade diante da industrialização, da urbanização e do crescimento do comércio. Estratégias para redução de riscos passaram a surgir com mais consistência, como o início dos seguros;
- Nos períodos das Guerras Mundiais e da Grande Depressão, os riscos econômicos e geopolíticos se destacaram, além do aumento da importância de serem investigados os riscos econômico-financeiros e seus retornos diante do desenvolvimento de mercados e instrumentos financeiros;
- No Pós-Guerra, houve a formalização da gestão de riscos, especialmente através de modelos matemáticos e estatísticos auxiliares. Tal cenário foi potencializado entre as décadas de 1970 e 1980, frente aos avanços associados à internacionalização do capital e sofisticação do mercado mundial;
- No século XXI, cenários de diversas naturezas – como a globalização, os avanços tecnológicos, as mudanças climáticas, crises econômicas e relações de poder – contribuem para a criação de regulamentações e para a evolução dos estudos e abordagens envolvendo o risco e suas possibilidades de retorno.

Assim, na contemporaneidade, observa-se que, no âmbito pessoal, profissional e organizacional, o homem continua a viver rodeado por riscos cada vez mais globalizados – acompanhando o ritmo do desenvolvimento tecnológico e da inovação – tendo em vista que adquiriram novas características e certo grau de complexidade.

Convém reforçar que os riscos físicos continuam sendo significativos, pois estamos sujeitos a eles em diferentes circunstâncias, seja atravessando

uma rua, praticando um esporte radical ou enfrentando uma pandemia global, como foi o caso da Covid-19. No entanto, com o passar do tempo, tem sido cada vez mais possível a separação do risco físico de riscos de outras naturezas – um indivíduo pode assumir riscos físicos sem recompensa econômica alguma, por exemplo, ao passo que também pode assumir riscos econômicos sem se expor a riscos físicos significativos.

Para fins didáticos, os riscos físicos não serão o foco deste material.

2. O que é risco?

Apesar de seu caráter onipresente – ou, talvez, por causa disso – não há consenso sobre o conceito de risco. De acordo com o Instituto Brasileiro de Governança Corporativa (IBGC, 2007), a terminologia "risco" deriva do latim *risicu* ou *riscu*, que tem o sentido de ousar.

De acordo com o *Blackwell Encyclopedic Dictionary of Finance*, o risco significa a exposição à mudança, referindo-se à probabilidade de um evento, ou vários, ocorrerem no futuro e resultarem em impactos organizacionais ou em carteiras de investimentos. Assim como a ocorrência, ou não, de determinados eventos evidencia um atributo objetivo do risco, esse também é uma construção sociocultural (Assi, 2021).

Tal definição, sob uma perspectiva interdisciplinar, encontra ainda mais distinções. Na área de finanças, por exemplo, o risco é associado ao grau de incerteza dos retornos de um ativo, com enfoque na probabilidade de perdas financeiras (Gitman, 2010). Além disso, o mesmo autor aponta que, entre os tomadores de decisões financeiras, podem ser identificados diferentes perfis de reação aos riscos, especialmente influenciados pelas perspectivas de retorno, tais como:

- Indiferença ao risco: quando o retorno exigido não muda a qualquer variação do risco;
- Aversão ao risco: quando o retorno exigido aumenta para compensar aumentos do risco;
- Propensão ao risco: quando o retorno exigido pode ser reduzido diante do aumento do risco;

Porém, a aversão ao risco se destaca como um perfil predominante entre os administradores (Gitman, 2010). Nessa conjuntura, parte-se do pressuposto de que quanto maior o risco tomado, maior deve ser a expectativa de retorno para o tomador (IBGC, 2007).

Na área de engenharia, o risco é definido a partir de uma perspectiva predominantemente quantitativa, sendo resultado do produto entre a probabili-

dade de ocorrência de um acidente ou evento negativo e o prejuízo resultante disso, financeiramente ou em vidas (Damodaran, 2009). Enquanto isso, no contexto do empreendedorismo, tem-se o risco como um fator intrínseco ao próprio exercício do negócio, envolvendo a capacidade de tomar boas decisões, de gerenciar a organização e a busca pelo retorno financeiro adequado aos riscos enfrentados, podendo acarretar na prosperidade ou no fracasso (IBGC, 2007).

Contudo, mesmo diante da diversidade de significados apresentada, há uma característica que costuma uni-los: a típica conotação negativa que predomina sobre o conceito de risco, associando-o apenas à probabilidade de os resultados não saírem conforme o esperado. Não é incomum a utilização de sinônimos como "probabilidade", "ameaça" ou "resultado negativo" para se referir ao que, na realidade, é um risco.

De acordo com Damodaran (2009), o risco vai além de uma probabilidade, pois ele envolve não apenas a probabilidade de um evento se concretizar, mas também a consequência desse fato, e se diferencia da "ameaça", pois enquanto ela possui pouca probabilidade de ocorrência e fortes consequências negativas, o risco pode ser um episódio mais provável de acontecer, com efeitos passíveis de desvios, seja para melhor ou para pior. Logo, em sua essência, o risco guarda relação com a incerteza e não se resume à crise, mas sim a combinação dela com a oportunidade (IBGC, 2017).

Nesse sentido, as observâncias e decisões associadas aos riscos envolvem elementos objetivos e subjetivos que, separadamente, não são suficientes para garantir a medição do risco, mas que, analisados em conjunto, podem esclarecer as expectativas em torno das perdas ou ganhos, pois o risco não é um destino, mas sim uma decisão (Bernstein, 1997).

Saiba Mais

Diversos estudos e pressupostos foram desenvolvidos, ao longo da história, com o objetivo de reduzir, ou até mesmo eliminar, o risco e a exposição dos sujeitos e organizações a ele. Porém, o risco é um elemento intrínseco ao processo decisório, seja ele de curto ou de longo prazo, e quaisquer caminhos que não o incorporem nas decisões possuem um alto potencial de equívocos e prejuízos ao negócio (Gitman, 2010).

Embora esse entendimento sobre a relevância do risco seja evidenciado, em especial, em discussões associadas ao contexto de mercados e relações financeiras, a complexidade do comportamento humano em relação ao risco tem desencadeado discussões que vão para além de modelos matemáticos (Farias; Salim; Santos, 2021).

Uma dessas discussões abrange a aversão ao risco e o pressuposto de que grande parte dos agentes econômicos direcionam suas escolhas para a maximização da utilidade esperada e não propriamente da riqueza. Isso pode ser evidenciado, por

exemplo, no âmbito pessoal, quando o ganho de um real é mais importante para uma pessoa que possui poucos recursos do que para um indivíduo acostumado com a riqueza; ou no âmbito organizacional, quando os gestores optam por não implementar um determinado projeto de alto potencial de retorno por ele ser arriscado (Farias; Salim; Santos, 2021).

Outro aspecto evidenciado ao longo do tempo se refere aos comportamentos irracionais que os indivíduos podem assumir ao encarar os riscos, podendo ser avessos a ele e, ao mesmo tempo, ter preferência por ele em determinados segmentos. Para Farias, Salim e Santos (2021), esse comportamento guarda relação com a forma como o risco é apresentado, de modo que um risco exposto junto às suas possibilidades de ganhos é encarado de forma diferente do que quando as evidências circulam em torno das possibilidades de perdas decorrentes de sua concretização, acarretando diferentes condutas por parte dos tomadores de decisões.

3. Elementos básicos do risco

A compreensão acerca do que é um risco é perpassada por alguns elementos que compõem os cenários de incerteza: as fontes de risco, as causas, os eventos e as consequências (ABNT, 2018).

3.1. Fontes de Risco

As fontes de risco, como o próprio nome indica, são meios potenciais de originar riscos, tanto de forma individual, como combinados entre si (ABNT, 2018). De acordo com dados do IBGC (2017), os riscos podem ser oriundos de fontes externas, internas ou de estratégias.

As fontes de risco de natureza externa são associadas a aspectos exteriores à empresa, mas que possuem força suficiente para exercer algum impacto sobre a organização. Fatores como novas regulamentações, aumento da competitividade, dependência excessiva de determinado público ou de fornecedores, instabilidades econômicas e problemas no sustento de vantagens competitivas são algumas das várias fontes de riscos que podem afetar severamente os objetivos e estratégias empresariais, dificultando a sustentabilidade do negócio (IBGC, 2017).

As fontes de risco de natureza interna são associadas a aspectos oriundos da própria organização, especialmente decorrentes de problemas nos processos de negócio, como a ausência de controles e de processos bem definidos, a falta de alinhamento desses processos com os objetivos estratégicos da empresa, o uso indevido de recursos financeiros, problemas de conformidade e baixa capacitação de pessoal (IBGC, 2017).

As fontes de risco de natureza estratégica são associadas ao uso das informações no processo de tomada de decisões, tendo em vista que os administradores correm o risco de se fundamentarem em informações sem vera-

cidade e deliberarem sobre aspectos estratégicos, operacionais e financeiros, comprometendo a compatibilidade dos objetivos com a realidade organizacional. Tal fato pode ocorrer pela ausência de alinhamento entre as medidas de desempenho e as estratégias da empresa, ou pela definição de indicadores e metas incompatíveis com a realidade, dificultando a compreensão do foco e dos planos empresariais (IBGC, 2017).

3.2. Causas

As causas dos riscos representam o "quê" e o "por quê" da ocorrência de um evento, ou da possibilidade de ele se concretizar (Brasil, 2020). A partir da análise das fontes de riscos, é possível identificar suas causas, ou seja, os aspectos que contribuem para a manifestação de um risco (ABNT, 2018).

Dados da Controladoria Geral da União (Brasil, 2018) apontam para a importância de analisar questões organizacionais ligadas a processos, infraestrutura, recursos humanos e financeiros, bem como o ambiente externo à organização, favorecendo a compreensão holística dos riscos do ambiente como um todo.

3.3. Eventos

Um evento representa qualquer situação, com envolvimento do impacto das fontes de risco em sua ocorrência. Algumas características dos eventos são: podem abranger um ou mais episódios; podem ser permeados por várias causas e várias consequências; possuem variadas probabilidades de ocorrência e de impacto, pois podem ser algo não esperado, mas que acontece, bem como algo já esperado, mas que não se concretiza; em alguns casos, pode ser também uma fonte de risco (ABNT, 2018).

3.4. Consequências

As consequências traduzem-se nos resultados ou impactos que podem ocorrer se os eventos se materializarem, gerando efeitos sobre a organização (Brasil, 2020).

Tal desfecho possui características variadas a depender de cada circunstância, podendo ser consequências:

- certas ou incertas;
- positivas ou negativas;
- diretas ou indiretas.

Além disso, as consequências podem ser representadas de forma quantitativa, em termos numéricos, ou qualitativas, em termos não numéri-

cos, sendo importante sua análise para evitar efeitos cascata e cumulativos nos objetivos empresariais (ABNT, 2018). Diante disso, evidencia-se que o conhecimento acerca dos componentes do risco é uma fonte estratégica de informação para a efetividade da gestão do conhecimento do negócio, favorecendo que a administração da organização aprenda as possíveis fontes, causas, eventos e consequências mais comuns dos riscos inerentes ao seu ambiente de atuação, viabilizando ações preventivas e corretivas.

Nesse contexto, ao lidar com riscos, os administradores devem estar cientes de que estão lidando com decisões que abrangem aspectos do passado, do presente e do futuro, as quais exigem responsabilidade e confiança nas informações de suporte (Assi, 2021).

Saiba Mais

"*Black swan thinking*": a teoria do Cisne Negro

A teoria do Cisne Negro se refere aos eventos que possuem baixa probabilidade de se concretizarem, mas que sua ocorrência pode gerar efeitos de altíssimo impacto, tornando-os perigosos e difíceis de prever. A alusão ao Cisne se deve à história de que, em meados de 1967, acreditava-se cientificamente que todos os cisnes existentes eram de cor branca, até que uma espécie de cor preta foi descoberta na Austrália, tornando questionável o pensamento dominante de se ancorar sempre no passado para prever comportamentos futuros.

Essa perspectiva lança luz sobre o entendimento de que, ainda que haja avanços tecnológicos nas mais diversas áreas do conhecimento, os riscos invisíveis são sempre presentes e elucidam a fragilidade que ainda impera no mundo dos negócios quando se trata dos acontecimentos futuros e suas emergentes adversidades.

Diante disso, o "*Black swan thinking*" é um convite para que os gestores de riscos reflitam, honestamente, sobre todas as possibilidades de riscos aos quais o negócio está vulnerável, mesmo as mais inimagináveis, de modo a fomentar o desenvolvimento de uma ampla gama de respostas aos riscos que podem acelerar as reações organizacionais e, em alguns casos, verdadeiramente salvar uma organização.

Dentre as sugestões de práticas para a identificação dos Cisnes Negros, estão:

- Estar atento ao que, dentro e fora da organização, parece estar indo bem;
- Analisar as áreas que aparentam ser sólidas e rever seus fluxos e processos;
- Monitorar as atividades mais representativas do negócio, especialmente as que apresentarem crescimento em volume e importância ao longo do tempo;
- Desarquivar assuntos que estão pausados por algum motivo e revisitá-los sempre que possível;
- Investigar possíveis segredos da empresa;
- Evitar menosprezar assuntos considerados menos importantes;
- Estar atento ao que for desenvolvido de forma demasiado complexa no negócio.

Ao ir além do comumente imaginável e aplicar a lógica do Cisne Negro, não se exclui a possibilidade de associar à ela o raciocínio de aprendizado normalmente uti-

lizado – pautado nas experiências passadas e suas lições – pois o objetivo é que, com uma gestão de riscos mais abrangente, sejam reduzidas as possibilidades de sucesso das armadilhas que poderiam ser evitadas.

Fonte: Candeloro (2014).

4. Classificações dos Riscos

Assim como não há um consenso sobre o conceito de risco, também não há homogeneidade acerca dos tipos de riscos existentes, pois eles dependem da natureza do negócio e de como cada negócio lida com a existência dos riscos (Assi, 2021). No entanto, existem algumas classificações que refletem os riscos mais comuns que podem ser identificados no âmbito organizacional. São eles:

- **Riscos Operacionais:** consistem em riscos ligados às atividades da organização as quais podem ser comprometidas pela deficiência ou pela falta de processos e de controles internos, bem como por falhas humanas, de infraestrutura ou de sistemas, resultando em perdas diretas e indiretas. Como exemplos, têm-se casos de fraudes, erros de sistemas de informações, falhas em equipamentos elétricos, perdas por omissão ou negligência de funcionários, equívocos decorrentes da ausência de qualificação profissional, falhas de atendimento ou de qualidade, incêndios, catástrofes, problemas com infraestrutura e falta de controle sistêmico (Assi, 2021; Brasil, 2020).
- **Riscos Financeiros:** consistem em riscos que têm o potencial de resultar em perdas financeiras e/ou de afetar a capacidade de uma organização, ou de um sujeito, de acessar os recursos financeiros necessários para honrar seus compromissos. Como exemplos, têm-se casos de falência, perdas decorrentes de flutuações nos preços de ativos financeiros, endividamento em excesso, transações impróprias, falta de liquidez, não pagamento de empréstimos, multas ou penalidades (Assi, 2021; Brasil, 2020).
- **Riscos Estratégicos:** consistem em riscos relacionados à incerteza presente nas decisões tomadas durante o planejamento da estratégia organizacional, os quais podem impactar os objetivos do negócio em diferentes horizontes de tempo. Tais riscos, sejam eles incertezas ou oportunidades, emergem em cenários de consecutivos ciclos de ajustes e desdobramentos dos objetivos e metas (Assi, 2021). Como exemplos, tem-se a falta de alinhamento estratégico com as necessidades do mercado, dificuldades em inovar, falhas na capacidade de atração e retenção de talentos e desatenção às demandas de responsabilidade socioambiental.
- **Riscos de Conformidade:** consistem em riscos que, quando não há o cumprimento de leis, normas ou políticas pré-estabelecidas, resultam em penali-

dades legais para a organização, as quais podem refletir em perdas financeiras e danos à reputação do negócio (Assi, 2021). Como exemplos, tem-se multas, processos judiciais por falta de conformidade, perda de confiança dos consumidores e investidores, e suspensão de licenças comerciais.

- **Riscos de Integridade:** consistem em riscos que, em decorrência de fragilidades organizacionais, favorecem a ocorrência de violações de integridade e de conformidade. Como exemplos, tem-se fraudes, abuso de poder, desvios de verbas para finalidades diferentes da destinação original, subornos e conflitos de interesses (Brasil, 2020; ITI, 2018).

Além da categorização supracitada, existem classificações de outras naturezas que podem complementá-la, potencializando a compreensão sobre os riscos em diferentes circunstâncias. Segundo Damodaran (2009), os riscos também podem ser:

- **De mercado ou específicos**: estão associados a fatores de mercado que, consequentemente, afetam grande parte das organizações e não são facilmente eliminados através de diversificações. Como exemplos, tem-se contextos de inflação ou de guerras. Os riscos específicos atingem uma ou um pequeno quantitativo de organizações, podendo ser minimizados ou eliminados através de diversificações. Como exemplos, tem-se greves e regulamentações setoriais.
- **Contínuos ou de evento**: os riscos contínuos são frequentes, aos quais organizações e pessoas estão sujeitas constantemente, como a volatilidade das taxas de juros. Os riscos de evento estão associados a eventos ocasionais que acarretam consequências, especialmente econômicas, como uma revolução política ou os desastres naturais.
- **Catastróficos ou menores:** os riscos catastróficos estão associados aos consideráveis impactos que podem exercer, principalmente, no lucro e no valor da organização. Os riscos menores, em contrapartida, exercem um impacto menos representativo sobre a empresa. Logo, trata-se de percepções variáveis sobre os níveis de impacto do risco para cada organização, respeitando suas respectivas particularidades.
- **De curto prazo ou de longo prazo:** os riscos de curto prazo ocorrem em um período de tempo relativamente curto, como é o caso das flutuações de preços. Os riscos de longo prazo manifestam-se em um horizonte de tempo prolongado, como é o caso de alterações em estruturas demográficas e em padrões climáticos.

Nesse sentido, convém esclarecer que, com o transcorrer do tempo, um risco pode mudar de classificação, fato que não anula a importância de classificá-los (Damodaran, 2009). Ademais, as diversas categorias dos riscos

apresentadas representam formas de facilitar a identificação de seus diferentes tipos, além de favorecer o aculturamento da organização, pois os sujeitos podem analisar as possibilidades de concretização dos eventos e como diferentes riscos podem impactar em seus processos (Assi, 2021).

Síntese do Capítulo

Chegamos ao fim do primeiro capítulo! Nele pudemos resgatar, brevemente, a trajetória do risco como um elemento intrínseco ao nosso cotidiano, dentro e fora das organizações, seguida da apresentação de algumas conceituações acerca do que é, de fato, o risco, ressaltando variações existentes entre diferentes áreas do conhecimento. Em seguida, foram esclarecidos os elementos básicos que compõem os riscos, bem como as diferentes classificações que podem ser identificadas na literatura, as quais vão desde a relação dos riscos mais comuns no âmbito organizacional, aos riscos que, representados por pares dialéticos – como riscos catastróficos *versus* riscos menores; ou riscos de curto prazo *versus* riscos de longo prazo –, auxiliam a avaliação crítica dos eventos para posteriores tratativas.

No próximo capítulo, você se aprofundará um pouco mais no mundo dos riscos, conhecendo os caminhos para gerenciá-los de forma estratégica. Até lá!

Atividades de avaliação

1. Dentre os conceitos de risco apresentados, avalie qual, ou quais, você já conhecia e responda: como você define o conceito de risco? Sua percepção sobre o risco considera as possibilidades de perdas e ganhos, ou um dos dois aspectos se sobressai? Explique.
2. Quais são os elementos básicos que compõem o risco e como eles interagem entre si?
3. Por que é importante para uma empresa entender as diferentes classificações do risco?

Leituras, filmes e sites

Livros

- Desafio aos Deuses: A Fascinante História do Risco. De autoria de Peter L. Bernstein. O livro explora, de forma abrangente e acessível, o papel do risco na história da humanidade, apresentando teorias associadas ao tema e sua importância para o progresso econômico, social e tecnológico. Ele destaca como a compreensão e a gestão do risco são essenciais para enfrentar os desafios do mundo moderno.
- *The Black Swan: The Impact of the Highly Improbable*. De autoria de Nassim Nicholas Taleb, esse livro explora com maior profundidade a Teoria do Cisne Negro, apresentada anteriormente neste primeiro capítulo. Leitura interessante para quem quiser obter novos insights sobre lidar com eventos inesperados de alto impacto.

Capítulo 2

Gestão Estratégica dos Riscos

Objetivos

- Definir o conceito de gestão de riscos e apresentar os principais atores organizacionais envolvidos nesse processo;
- Descrever os princípios fundamentais da gestão de riscos;
- Analisar os diferentes estágios do processo de gestão de riscos, identificando suas interações e impactos na tomada de decisão;
- Refletir sobre a importância da gestão de riscos para uma empresa, identificando suas vantagens competitivas e os desafios associados à assunção de riscos.

Introdução

A gestão de riscos é uma prática essencial para qualquer organização que busca sustentabilidade em um ambiente de negócios dinâmico e incerto. É natural que, ao longo das atividades, os envolvidos em um contexto organizacional se deparem com surpresas que, com seus variados potenciais de recorrência e de impacto, exigem reações tempestivas e adequadas para a sobrevivência da corporação. Essa é a essência da gestão de riscos.

Embora existam estruturas e modelos de gestão de riscos corporativos consolidados no mercado, como o proposto pelo *Committee of Sponsoring Organizations of the Treadway Commission* (COSO) e pela norma ISO 31.000, as organizações podem desenvolver seus próprios métodos de administração dos riscos, fundamentando-se nas fases mais representativas: identificação, classificação, avaliação, resposta e monitoramento dos riscos.

De modo geral, constata-se que o sucesso empresarial não se restringe a um movimento constante de fuga dos riscos, pelo contrário, trata-se de explorá-los para aproveitar oportunidades de crescimento e de inovação. Nesse contexto, a gestão de riscos é primordial para que os riscos sejam assumidos de forma saudável e estratégica.

1. Introdução à Gestão de Riscos

A gestão de riscos tem sido parte integrante das rotinas organizacionais desde épocas remotas, mas sua importância tem crescido significativamente desde o final do século XX, em decorrência da maior interconexão entre os mercados e, consequentemente, da crescente complexidade das organizações e das instituições financeiras (IBGC, 2017).

Sendo um processo contínuo e interativo que abrange toda a organização, dos mais diversos tipos e setores, a gestão de riscos atua através de estratégias de identificação dos eventos que possuem um considerável potencial de impacto sobre o negócio, bem como por meio da administração dos riscos para que o apetite aos riscos esteja sempre compatível com a realidade organizacional (COSO, 2007).

Assim, ao administrar riscos, a organização constrói uma estrutura favorável à assunção de riscos calculados, alcançando resultados menos voláteis e previsões mais consistentes que contribuirão para sua sustentabilidade, especialmente em tempos de crise (IBGC, 2017). Para tanto, busca-se eliminar, reduzir ou prevenir a ocorrência de danos na organização como um todo, através da análise das possíveis falhas e de sugestões de aprimoramento (Assi, 2021).

Nas organizações contemporâneas, incentiva-se a construção de uma cultura de assunção de riscos, pautada na flexibilidade, na inovação e na velocidade das respostas aos eventos, contando, para isso, com um sistema que orienta a direção, o monitoramento e o estímulo das empresas, mais conhecido como a Governança Corporativa. Desse modo, a gestão de riscos, aliada à uma estrutura de governança, converge para a implementação de boas práticas internas, como prestações de contas, maior responsabilidade empresarial e engajamento de diferentes níveis hierárquicos nas decisões (IBGC, 2017).

De acordo com o COSO (2007), para que esse processo seja possível, diversos agentes desempenham funções valiosas, sejam eles externos à organização – como auditores externos, terceirizados, parceiros comerciais, mídia jornalística, dentre outras potenciais fontes de informações – ou, especialmente, agentes internos.

No âmbito interno da organização, embora todos os funcionários possuam algum nível de responsabilidade na gestão de riscos, podemos destacar alguns agentes ativos nesse processo: i) o conselho de administração, que atua como elo entre gestores e proprietários, bem como supervisiona a eficiência da gestão de riscos, podendo intervir quando necessário; ii) a diretoria executiva, sobre a qual recai a responsabilidade direta por todas as operações da empresa, cabendo a ela monitorar se a implementação de todos os ele-

mentos do gerenciamento de riscos foi realizada e está em pleno funcionamento; iii) pessoas ou departamentos que têm como função principal a gestão de riscos, trabalhando junto aos gestores a comunicação das informações relevantes sobre os riscos; iv) os auditores internos, que analisam a eficácia da administração dos riscos e dos controles, sugerindo melhorias (COSO, 2007).

Tal diversidade de atuações é essencial para o equilíbrio e eficácia da administração de riscos, tendo em vista a parcela de subjetividade envolvida nesse processo, como, por exemplo, comportamentos de aversão e de atração pelo risco (Damodaran, 2009). Ademais, diante da amplitude de possibilidades de gerir riscos, contar com processos bem definidos e com controles internos consistentes faz-se essencial para a redução de perdas e para a exploração de oportunidades inovadoras (IBGC, 2017).

Saiba Mais

A Governança Corporativa é um tema recorrente quando se trata de gestão de riscos, *Compliance* e controles internos. Logo, convém conhecer um pouco mais sobre esse sistema tão importante para as instituições.

De acordo com o Instituto Brasileiro de Governança Corporativa (IBGC, 2024), a governança consiste em um sistema composto por estruturas, regras, princípios e processos que guiam e supervisionam todas as partes envolvidas na organização – clientes, fornecedores, parceiros, comunidades, reguladores, investidores, governo – para um equilíbrio entre seus interesses, criando valor para essas partes, para a organização e para a sociedade.

Tal sistema emergiu para amenizar os conflitos de agência e as quebras de confiança ocasionadas por diversos escândalos de corrupção ocorridos no mundo (Assi, 2021). No que tange à gestão de riscos, ela se destaca como um instrumento fundamental para que, através do conhecimento dos riscos e da definição de metodologias úteis, o processo decisório seja alimentado de forma eficiente e o caminho para o cumprimento dos princípios básicos desse sistema seja facilitado, sendo eles:

- Integridade: praticando e fomentando uma cultura ética na organização;
- Transparência: compartilhamento de informações fidedignas, tempestivas, claras e coerentes, independentemente de serem positivas ou não, para todas as partes interessadas.
- Equidade: tratamento justo de todas as partes interessadas, evitando privilégios e discriminações, considerando seus interesses, expectativas direitos e deveres.
- Responsabilização (Accountability): cumprimento de funções de forma cuidadosa e independente, prestando conta de suas decisões e atitudes, bem como assumindo a responsabilidade pelos seus resultados.
- Sustentabilidade: observância da interdependência do negócio em relação às dimensões sociais, econômicas e ambientais, reduzindo riscos e aumentando as oportunidades de curto, médio e longo prazos, especialmente no tocante à viabilidade econômico-financeira da organização.

Diante disso, para o IBGC (2017) a Governança define o tom da gestão de riscos, responsabilizando os diferentes níveis hierárquicos pelo desempenho de atividades associadas a esse processo e estimulando debates e reflexões, tais como:

- O que pode comprometer o cumprimento das estratégias e metas?
- Onde estão as maiores oportunidades, ameaças e incertezas?
- Quais são os principais riscos?
- Quais os riscos a explorar?
- Qual a percepção desses riscos?
- Qual a exposição desses riscos?
- Como a organização responde aos riscos?
- O que é feito para assegurar que os riscos estejam em um nível aceitável de acordo com o apetite a riscos aprovado?
- Os executivos e gestores têm consciência da importância do processo de gestão de riscos?
- A organização tem as competências necessárias para gerir riscos assumidos?
- Quem identifica e monitora ativamente os riscos da organização?
- Que padrões, ferramentas e metodologias são utilizados?

Saiba mais em: https://www.ibgc.org.br/conhecimento/governanca-corporativa

2. Princípios da Gestão de Riscos

De forma prática, a gestão eficiente de riscos é um elemento presente nas organizações de sucesso. Para tanto, Damodaran (2009) apresenta 10 princípios fundamentais a serem seguidos para garantir que administração dos riscos seja consistente e condizente com os objetivos empresariais. São eles:

i) O risco está presente em todas as esferas da atividade humana.

Sendo o risco onipresente, ao gerenciá-lo as organizações podem focar no desenvolvimento de estratégias para reduzir o impacto do risco, ao invés de apenas evitá-los, tendo em vista que, muitas vezes, eles emergem onde e quando menos se espera.

ii) O risco, ao mesmo tempo, representa tanto uma ameaça quanto uma oportunidade.

Uma boa gestão de riscos envolve uma abordagem realista, a qual admite que, ao assumir um risco, não há como alcançar uma consequência positiva sem aceitar a possibilidade de ocorrer um efeito negativo, pois o risco é a associação de possíveis ganhos com consideráveis perdas.

iii) As pessoas frequentemente mantêm uma postura ambígua em relação ao risco, e suas avaliações e respostas nem sempre são totalmente racionais.

A qualidade da gestão de riscos está diretamente relacionada à qualidade das pessoas que a realizam, pois, ainda que o homem seja, de modo geral, avesso ao risco, o nível de aversão varia de pessoa para pessoa, o que pode resultar em decisões contraditórias.

iv) Os riscos não são originados de uma única maneira.

Para uma correta administração, os riscos devem ser avaliados – entre os diferentes níveis de gestão – sob a ótica mais adequada a cada circunstância, pois gerentes, diretores da alta administração e investidores podem divergir na forma de enxergar determinadas incertezas. Enquanto um risco pode ser insignificante para os investidores, que podem livrar-se dele através da diversificação, ao mesmo tempo ele pode ser catastrófico para gerentes intermediários envoltos pela necessidade de tomar decisões imediatas.

v) O risco pode ser objeto de mensuração e análise.

As ferramentas para gestão dos riscos devem ser cuidadosamente escolhidas, avaliando de que forma cada uma delas pode contribuir com a realidade organizacional, como a análise de cenários e a análise SWOT. Com os avanços tecnológicos, o volume de dados é cada vez maior e desenvolvem-se ferramentas cada vez mais sofisticadas, as quais favorecem que diversos riscos sejam identificados e avaliados, mesmo que as ferramentas variem de acordo com cada um deles.

vi) Uma adequada mensuração, identificação e avaliação do risco são fundamentais para a tomada de decisões aprimoradas.

O processo de tomada de decisão não deve ser adaptado às ferramentas de gestão de riscos, mas sim o oposto: as ferramentas e seus resultados é que devem ser adequados ao processo decisório. Para que haja uma eficaz contribuição das ferramentas para melhores decisões, alguns pontos são fundamentais: i) se há diferença entre quem identifica e avalia os riscos através das ferramentas, e quem toma as decisões, ambas as partes precisam conhecer as principais necessidades e restrições do contexto sob risco, para que os resultados sejam coerentes com a realidade; ii) ainda que existam muitos riscos, as ferramentas devem ser direcionadas aos que possuem maior potencial de impacto no momento, pois estes são mais úteis aos tomadores de decisões, evitando análises abrangentes e incoerentes; iii) os diagnósticos resultantes do uso das ferramentas não devem se limitar ao lado negativo dos riscos, embora seja o ponto de maior preocupação no processo decisório, mas também contemplar aspectos positivos que podem ser explorados. Logo, não adianta ter a melhor ferramenta sem o adequado envolvimento dos tomadores de decisões no processo de identificação e avaliação dos riscos.

vii) A eficácia da gestão de riscos reside na habilidade de discernir quais riscos devem ser evitados, transferidos ou explorados.

A gestão de riscos tem como elemento-chave a capacidade de compreender quais riscos devem ser explorados, por serem fonte de vantagens competitivas, e quais riscos não serão explorados. No caso desses últimos, que não são usados em vantagem da organização, cabe a avaliação de como

eles podem ser minimizados ou eliminados em suas operações, ou se é necessário dispender recursos para proteger-se deles.

viii) Uma melhor gestão de riscos se traduz em uma valorização superior da empresa.

A gestão de riscos possui uma relação direta com o valor do negócio: se for bem realizada, pode elevar o valor da empresa, se for falha, pode reduzir o valor da empresa. Logo, é fundamental compreender as alavancas que estabelecem o valor do negócio. Algumas funções mais tradicionais de quão boa é a gestão de riscos de uma empresa partem da análise, por exemplo, dos fluxos de caixa e das taxas de desconto, almejando entender as consequências de explorar, ou não, um risco. No entanto, faz-se necessário incorporar métodos de avaliação mais abrangentes para contemplar todos os efeitos da administração de riscos, como aspectos qualitativos.

ix) A responsabilidade pela gestão do risco é compartilhada por todos os membros da organização.

Ainda que a organização possua um setor voltado à gestão dos riscos, os demais setores não devem ser eximidos de participar desse processo. A depender das características de um risco, a decisão sobre sua assunção, ou não, pode necessitar de percepções e de habilidades de diferentes áreas funcionais da empresa, assim como as decisões tomadas em cada departamento podem acarretar novos riscos para a organização como um todo. Logo, a prática adequada dos negócios depende da administração eficaz dos riscos, a qual deve ser uma responsabilidade compartilhada por todos os envolvidos.

x) O sucesso na gestão de riscos não é um resultado aleatório.

O êxito da gestão de riscos fundamenta-se no aculturamento de toda a organização, através: do alinhamento de interesses entre tomadores de decisões e proprietários; de um confiável sistema de informações estratégicas; do correto manuseio de ferramentas analíticas, resultando em avaliações consistentes; da flexibilidade das estruturas organizacionais para se adaptar às mudanças; de pessoas que reagem aos riscos com sabedoria, motivando-as com reconhecimento financeiro ou com dinâmicas culturais.

Nota-se, portanto, que os princípios supracitados refletem a essência do processo de gestão de riscos em qualquer tipo de organização, representando verdadeiros pilares para que, de forma resiliente, seja consolidada uma cultura de conscientização, de responsabilidade e de compromisso com a longevidade do negócio.

2.1. Processo de Gestão de Riscos

O funcionamento da gestão de riscos deve levar em consideração as características de cada organização: a complexidade de suas atividades, a natureza do negócio, o mercado em que atua, sua cultura, suas estratégias, sua capacidade de administrar riscos, etc. Diante de suas particularidades, cabe às organizações a missão de introduzir a gestão de riscos como uma prática consistente, que pode ser aperfeiçoada ao longo do tempo, desde que possua alinhamento com as estruturas e estratégias da empresa (IBGC, 2017).

Embora existam modelos prévios de gestão de riscos que podem ser adotados pelas organizações, como a ISO 31.000 e o Modelo Coso ERM, é possível construir uma metodologia personalizada para o negócio a partir da adaptação das potencialidades das práticas já existentes, prezando pela simplicidade e clareza das atividades envolvidas (Assi, 2021).

Saiba Mais

As principais estruturas e modelos de gestão de riscos corporativos existentes que, de forma genérica, podem ser adaptadas a diferentes contextos organizacionais são a ISSO 31.000 e o Modelo COSO ERM.

ISO 31.000: A ISO 31000 é uma norma técnica de abrangência internacional estabelecida, inicialmente, em 2009, que fornece instruções e princípios gerais para a gestão de riscos de qualquer organização, sem enfoques setoriais ou de atividades específicas. Assim, tal norma é projetada para ajudar as empresas a atingirem seus objetivos de forma mais consistente e segura, por meio de um forte e estratégico comprometimento da administração do negócio com a gestão de riscos (Brasil, 2020).

Nesse contexto, o processo de gestão de riscos compreende as seguintes etapas:

i) entendimento do contexto externo e interno da organização;
ii) processo de avaliação de riscos, onde ocorre a identificação, a análise e a avaliação dos riscos aos quais o negócio está vulnerável;
iii) tratamento de riscos.

Essas três etapas são envolvidas por atividades de comunicação e consulta, bem como de monitoramento e análises críticas, almejando a identificação de ameaças, de oportunidades e a incorporação dessas práticas à cultura organizacional (Brasil, 2020).

Em 2018, a norma ISO foi atualizada, ampliando sua perspectiva de gestão de riscos para abranger aspectos voltados à estratégia e ao comprometimento das lideranças. Nesse sentido, a norma se volta aos gestores de riscos que criam e protegem o valor das organizações, ressaltando que uma administração de riscos é eficiente, eficaz e consistente quando ocorre:

- Integrada a todas as atividades da organização;
- De forma estruturada e abrangente;
- Personalizada ao contexto e aos objetivos do negócio;

- Inclusiva, considerando as percepções das diversas partes interessadas, de forma apropriada e oportuna;
- Dinâmica, correspondendo às mudanças internas e externas;
- Com a melhor informação possível, com base em dados históricos, atuais e expectativas para o futuro;
- Envolvendo fatores humanos e culturais nos diferentes níveis de desenvolvimento da gestão de riscos;
- Sob a perspectiva de melhoria contínua, considerando aprendizados e novas experiências.

Diante disso, a nova ISO propõe uma estrutura de gestão de riscos cíclica, na qual a liderança e o comprometimento ocupam o centro, enquanto são rodeadas pelas etapas de: integração, concepção, implementação, avaliação e melhoria da gestão de riscos. Tais etapas podem funcionar de forma personalizada de acordo com a realidade de cada negócio (ABNT, 2018).

COSO ERM: O Modelo COSO ERM, desenvolvido pelo *Committee of Sponsoring Organizations of the Treadway Commission*, trata-se de um framework específico para auxiliar as organizações na gestão dos riscos que podem afetar a capacidade de alcance dos seus objetivos. Assim, são apresentados oito componentes da administração de riscos:

1. Ambiente Interno, como condutas, valores e a cultura organizacional;
2. Definição de objetivos organizacionais, em diferentes níveis hierárquicos;
3. Identificação de eventos que representem oportunidades e ameaças;
4. Avaliação de riscos, com base em sua probabilidade e impacto;
5. Resposta aos riscos, pautada na decisão de aceitar, evitar, reduzir ou transferir os riscos;
6. Atividades de controle, para garantir a eficácia das respostas aos riscos e a conformidade das políticas e normas estabelecidas;
7. Informações e Comunicações acerca da administração de riscos para todas as partes interessadas;
8. Monitoramento contínuo do processo de administração de riscos (COSO, 2012).

Preservando a existência desses componentes no contexto organizacional, os gestores têm a oportunidade de adaptá-los a cada negócio e garantir que as atividades associadas à gestão dos riscos sejam desenvolvidas em conformidade com os padrões e regulamentos existentes.

Contudo, embora não haja uma regra específica para a implementação dessa estrutura, alguns passos fundamentais podem ser percorridos, tais como: identificação e classificação dos riscos, avaliação, resposta e monitoramento (IBGC, 2017).

2.2. Identificação e Classificação dos riscos

Processualmente, o primeiro passo da gestão de riscos é a identificação e classificação dos riscos (IBGC, 2017). Tal etapa envolve um profundo levantamento de todos os eventos de risco e possibilidades que podem impactar nos processos de trabalho para posterior avaliação de suas causas e consequências (Brasil, 2020).

Nesse contexto, é fundamental o engajamento das pessoas que vivenciam o dia a dia corporativo, atuantes nos mais diversos departamentos, pois são elas que realizam as atividades e, consequentemente, que conhecem com mais detalhes os problemas, as possibilidades de falhas e inconsistências, contribuindo com a busca pela proteção do negócio (Assi, 2021). Para Assi (2021), quanto mais as pessoas entendem e identificam os riscos próprios de suas atividades, melhor os riscos serão gerenciados.

A identificação dos riscos pode ser bem-sucedida através da existência de informações consistentes e oportunas, bem como do uso adequado de ferramentas (Damodaran, 2009). No tocante à obtenção de informações de qualidade, Damodaran (2009) ainda afirma que, quando essas informações são coletadas, conforme os riscos se desenvolvem, a organização possui menores chances de ser surpreendida por eles.

De fato, a obtenção de informações acessíveis, detalhadas, fidedignas e oportunas é crucial para que os responsáveis pela identificação dos riscos possam cumprir seus objetivos de maneira eficaz (Brasil, 2020).

Outro importante fator é a utilização de ferramentas adequadas à identificação dos riscos, as quais devem viabilizar a coleta de dados relevantes e tempestivos (Brasil, 2020). Ao longo do tempo, a evolução tecnológica tem favorecido a otimização das ferramentas, as quais podem disponibilizar, por exemplo, informações em tempo real (Damodaran, 2009), sofisticação essa que é crucial para a rapidez da identificação dos riscos e, posteriormente, para a abrangência das análises.

Dentre algumas ferramentas comumente utilizadas, estão:

- Brainstorming: trata-se de um método que incentiva a geração de várias soluções para uma questão, como uma verdadeira tempestade de ideias, eficaz especialmente quando realizado em grupo. O método não admite críticas às ideias durante a reunião e incentiva a combinação de soluções para resultados inovadores (Bolsonello et al., 2023). Assim, é possível que, através do brainstorming com um grupo de pessoas de diversos setores da organização, seja obtida uma lista de riscos consistente (Brasil, 2020);
- Entrevistas: pode-se realizar entrevistas com especialistas, gestores dos departamentos, dentre outras partes interessadas que possam favorecer o entendimento sobre os processos, a identificação dos riscos existentes e até mesmo um diagnóstico sobre a existência de controles (Assi, 2021);
- Diagrama de causa e efeito: também nomeado de diagrama de Ishikawa ou de espinha de peixe, o diagrama de causa e efeito trata-se de uma técnica através da qual são analisadas as possíveis causas de um problema,

objetivando detectar sua causa raiz (Brasil, 2020). Assim, podem ser identificados diferentes riscos e suas respectivas causas;

- Análise de listas de verificação de riscos: caso a organização já possua listas de riscos de períodos anteriores, pode ser realizada uma verificação para detecção dos riscos persistentes já conhecidos e para coletar lições aprendidas (Brasil, 2020).

É essencial que os gestores de riscos reflitam sobre a adoção de boas ferramentas, especialmente para que sejam incluídos os riscos mais difíceis de serem identificados e avaliados, como os demasiadamente qualitativos e os que possuem impactos de baixa previsibilidade (Damodaran, 2009).

Nessa fase, considera-se uma boa prática que não apenas os riscos sejam listados, mas também que sejam identificadas suas respectivas causas e consequências, ampliando a compreensão dos administradores sobre a origem dos eventos e seus efeitos, caso se concretizem. Para tanto, uma ferramenta bastante conhecida é a análise SWOT, em que são definidas forças, fraquezas, ameaças e oportunidades que representam elementos concretos para o diagnóstico das causas dos eventos de riscos (Brasil, 2020).

Assim, após o reconhecimento dos riscos, bem como de suas causas e consequências, torna-se possível classificá-los, a partir de reflexões sobre a forma como cada risco pode impactar na organização, bem como sobre os potenciais de falhas nos processos de trabalho e suas respectivas consequências para a gestão de riscos (Assi, 2021).

A classificação dos riscos é uma estratégia fundamental, principalmente quando a lista de riscos identificados é expressiva, pois torna viável que os riscos sejam gerenciados através de categorias mais abrangentes (Damodaran, 2009). As possibilidades de classificações são extremamente variáveis, mas algumas perspectivas estão apresentadas no capítulo 1 deste material, na seção "Classificações dos Riscos", as quais devem ser utilizadas nessa etapa.

Por fim, indica-se a elaboração de uma síntese descritiva de cada risco, contendo suas respectivas fontes, causas, consequências, classificações e, para eventos de riscos vigentes, se existem controles implementados (Brasil, 2020). Soma-se a isso a possibilidade de implantação de um manual de riscos, com o objetivo de socializar os conceitos e as nomenclaturas ligadas aos riscos, contribuindo para que toda a organização se envolva em uma cultura de administração de riscos (Assi, 2021).

Com isso, há um fechamento da etapa inicial com insumos organizados para a etapa seguinte, na qual os riscos serão avaliados. Porém, é fundamental que o processo de identificação e classificação dos riscos seja aperfeiçoado e repetido periodicamente, de modo a envolver novos casos (IBGC, 2017).

2.3. Avaliação dos riscos

Após uma boa identificação e classificação dos riscos, os resultados obtidos devem ser avaliados. De acordo com Assi (2021), é fundamental que os envolvidos na gestão de riscos possuam conhecimento sobre os processos do negócio, pois a avaliação dos riscos passa pela dinâmica de cada atividade, e sobre aspectos que podem interferir, principalmente de forma negativa, nesses processos, como a complexidade, o porte e o quantitativo de operações.

Nessa perspectiva, a avaliação dos riscos identificados é fundamentada em dois elementos: na probabilidade de ocorrência e no potencial de impacto do risco, caso ele se materialize (Brasil, 2020).

A chance de um risco se concretizar é avaliada com base na sua frequência – já conhecida ou esperada – e em suas causas, enquanto o impacto é averiguado com base no efeito negativo do evento de risco sobre os objetivos almejados (Brasil, 2020). Tais avaliações podem ocorrer com o uso de métodos qualitativos, quantitativos, ou combinando ambas as perspectivas (Damodaran, 2009).

A avaliação qualitativa dos riscos pode ser realizada com o auxílio das mesmas ferramentas exemplificadas na etapa de identificação, como brainstorming e entrevistas, assim como podem ser utilizadas escalas qualitativas para inferir probabilidades e impactos, através de julgamentos como, por exemplo: quase impossível, raro, provável e quase certo (Brasil, 2020).

Para o IBGC (2017), a análise do impacto dos riscos pode se basear em fatores diversos, como socioambientais, econômico-financeiros, estratégicos e de conformidade, incorporando não só os aspectos tangíveis, mas também os intangíveis, como danos à reputação e perda de oportunidades.

O ponto de vista qualitativo é interessante para a obtenção de avaliações subjetivas, sobretudo com fins estratégicos, envolvendo dados históricos, conhecimentos, percepções e experiências dos indivíduos relacionadas a probabilidade e ao impacto dos riscos (Damodaran, 2009). Contudo, o autor salienta que a subjetividade pode acarretar adversidades no processo avaliativo, pois pode-se obter diferentes julgamentos sobre um mesmo risco, subestimando ou superestimando suas chances de ocorrência e seus efeitos sobre a organização.

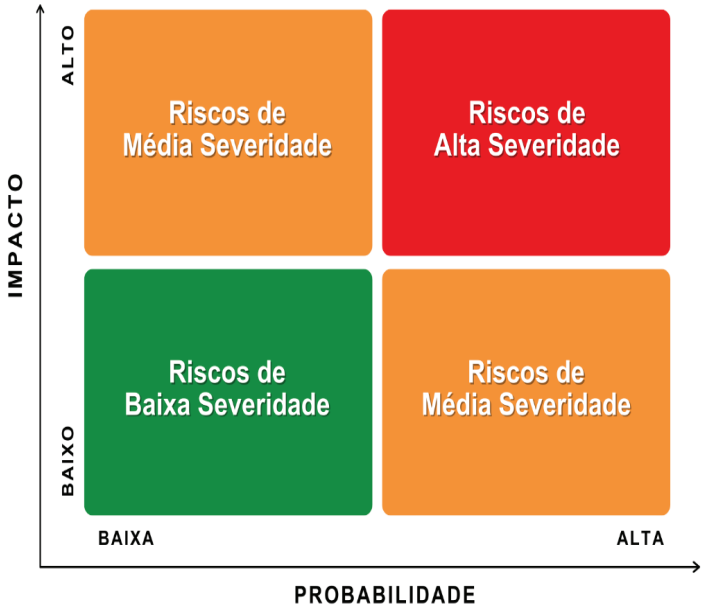
No tocante à avaliação quantitativa, essa também pode ser beneficiada com o uso das ferramentas de identificação dos riscos, com o uso de escalas e com consultas aos dados históricos, mas contemplando numericamente a exposição da organização aos riscos. Nessa conjuntura, realiza-se a investigação de quais aspectos podem potencializar tal exposição e de que forma o fazem, seja através do exame de histórias passadas, refletidas no comporta-

mento das variações dos lucros e do valor da empresa, ou através de dados sobre os efeitos e a sensibilidade de outras empresas do mesmo setor aos riscos similares enfrentados (Damodaran, 2009).

Ademais, também existem dificuldades ao optar pela avaliação quantitativa dos riscos, pois alguns eventos têm a capacidade de gerar diferentes impactos em diferentes áreas, exigindo que a administração considere a probabilidade de todos os eventos de risco ocorrerem ao mesmo tempo, de modo a diagnosticar os impactos financeiros e suas chances de adequação à realidade da empresa (IBGC, 2017).

Após as avaliações, pode-se documentar os resultados em uma matriz de riscos, instrumento esse que combina os fatores avaliados – probabilidade e impacto – e, com ênfase aos eventos de perda, viabiliza a definição do nível de cada risco, conforme Figura 1.

Figura 1: Matriz de Riscos



Fonte: elaborado pela autora, adaptado de IBGC (2017).

O nível do risco é ilustrado na matriz pelo seu grau de severidade, elemento que vai ao encontro das possibilidades de perdas financeiras e mobiliza os gestores das organizações a refletirem sobre a segurança do negócio (Assi, 2021). O autor explica a severidade dos riscos da seguinte forma:

- **Riscos de baixo impacto e baixa probabilidade: baixa severidade -** Tais riscos não possuem tanta relevância, em termos de tratamento e monito-

ramento, mas é essencial revisar periodicamente seus níveis para garantir que estejam atualizados e adequados continuamente.

- **Riscos de baixo impacto alta probabilidade: média severidade -** Recomenda-se analisar o custo-benefício associado a esses riscos e, sempre que possível, revisá-los periodicamente para se certificar de que eles não elevaram seu nível de impacto.
- **Riscos de alto impacto e baixa probabilidade: média severidade -** Tais riscos são pontos de atenção, pois possuem o potencial de afetar consideravelmente a estratégia e os objetivos do negócio, ainda que possuam menor chance de ocorrência.
- **Riscos de alto impacto e alta probabilidade: alta severidade -** Recomenda-se o tratamento adequado desses riscos, pois ameaçam abalar consideravelmente a organização e a sustentabilidade de seus objetivos.

De modo geral, um alto risco não representa, necessariamente, um problema, desde que seja gerenciado com controles internos coerentes e efetivos (Assi, 2021). A realização dessa etapa de avaliação dos riscos é uma oportunidade interessante para também ser avaliada a existência e a atuação dos controles internos como instrumentos de minimização dos riscos identificados na etapa anterior (Brasil, 2020).

2.4. Resposta aos Riscos

Tendo avaliado os riscos e conhecido seus níveis, o processo de gestão de riscos segue para a etapa em que as respostas devem ser estabelecidas. Nesse momento, são identificadas as possibilidades de respostas adequadas ao perfil de riscos da empresa, o qual é caracterizado pelo seu apetite a riscos, ou seja, aos níveis dos riscos assumidos (IBGC, 2017).

De acordo com o COSO (2007), a resposta dada aos riscos envolve as seguintes decisões:

- **Evitar**: quando, geralmente, não foi encontrada nenhuma alternativa viável para minimizar o impacto e a probabilidade do risco a um nível tolerável. Assim, implica na interrupção, substituição ou não execução das atividades que geram riscos.
- **Reduzir**: quando podem ser implementadas medidas para minimizar tanto a probabilidade quanto o impacto dos riscos, ou ambos. Assim, busca-se diminuir o risco remanescente para um nível que esteja de acordo com a tolerância da empresa.

- **Transferir ou compartilhar**: quando, assim como na opção por reduzir, busca-se diminuir o nível de risco para que esteja adequado à tolerância desejada. Porém, as medidas de diminuição da probabilidade e do impacto dos riscos envolvem a transferência ou compartilhamento desse risco com as partes interessadas, objetivando um maior grau de proteção, como através da contratação de seguros, terceirizações ou da utilização de contratos futuros.
- **Aceitar**: quando não há, como condição necessária, a implementação de medidas para influenciar a probabilidade ou o grau de impacto dos riscos, pois eles já estão em conformidade com as tolerâncias estabelecidas pela empresa para o nível de risco aceitável. Assim, a empresa pode utilizar suas competências para explorar o risco e obter vantagens com isso.

Nesse sentido, a gestão de riscos deve contribuir para que as opções supracitadas sejam avaliadas e selecionadas de acordo com o perfil de riscos de cada organização, buscando a manutenção do equilíbrio entre os níveis de recusa, redução, transferência e aceite dos riscos. O respeito à particularidade de cada negócio na fase de resposta aos riscos é importante, pois, mesmo que exista, por exemplo, uma padronização na avaliação dos riscos em um determinado setor, a definição do perfil e do apetite aos riscos envolve aspectos subjetivos que podem variar entre organizações desse mesmo ramo de negócio (IBGC, 2017).

A matriz de riscos apresentada na etapa anterior é uma ferramenta importante para auxiliar o desenvolvimento das respostas, pois, reconhecendo os níveis dos riscos, recomenda-se que as respostas sejam atribuídas ao longo dos graus de severidade, iniciando pelos riscos de alta severidade, até os de menor severidade. Importante destacar que esses últimos, embora não envolvam probabilidades e impactos elevados, não devem ser eximidos de respostas (IBGC, 2017).

Além disso, é significativo que a etapa de resposta aos riscos seja associada à implementação ou aperfeiçoamento de controles internos, como indicadores de desempenho e controles de acesso à informação, que assegurem que os riscos recebam o devido tratamento, a depender das respostas definidas para cada um deles. Para tanto, pode ser elaborado um plano de implementação de controles, contemplando os recursos necessários, o custo-benefício de cada controle, o cronograma de execução, as pessoas responsáveis pela implementação e os aspectos regulatórios (Brasil, 2020).

2.5. Monitoramento dos Riscos

Sabendo quais riscos serão evitados, reduzidos, transferidos e aceitos, devem ser estabelecidos fluxos permanentes de monitoramento, de modo a analisar se todo o processo de administração de riscos está funcionando de forma eficaz e de acordo com o perfil do negócio (IBGC, 2017). Com isso, o monitoramento viabiliza que as deficiências existentes na gestão dos riscos sejam identificadas e tratadas, de modo que seus efeitos sobre a estratégia e desempenho organizacional sejam poucos ou nulos (COSO, 2007).

De acordo com o IBGC (2017), é possível diagnosticar a necessidade de avaliações e revisões particulares em determinadas etapas da gestão de riscos através de procedimentos de monitoramento, tais como:

- **Definição de medidas de desempenho:** por meio das medidas de desempenho é possível avaliar se os riscos assumidos estão se comportando conforme o esperado, de acordo com o apetite ao risco pré-estabelecido, e se os planos de ação e os controles implementados estão sendo eficazes. Caso contrário, indica-se a revisão do processo decisório e da gestão de riscos. É comum o uso de indicadores, mas recomenda-se limitar sua quantidade ao essencial para decisões consistentes, evitando a sobrecarga do monitoramento.
- **Elaboração de relatórios periódicos:** os relatórios sobre os riscos e a efetividade dos controles possuem diversas finalidades, como medir o progresso das diversas áreas, sinalizar a necessidade de ações corretivas, alertar os diretores e conselheiros sobre áreas de risco, divulgar melhores práticas e notificar os auditores internos sobre riscos que possam exigir a revisão dos controles internos. Tais relatórios podem ter sua frequência variada de acordo com o tipo de risco ou com a estrutura da organização, mas são importantes para manter os gestores e conselheiros cientes dos resultados.
- **Registro e a quantificação das perdas resultantes da ocorrência dos eventos de risco:** por meio da elaboração de uma base histórica sobre as perdas oriundas da concretização dos riscos, é possível reportá-las e auxiliar as decisões que envolvem a assunção de riscos e de controles. Podem ser utilizados também indicadores de tolerância à perda por riscos, para que quaisquer excessos sejam logo percebidos e comunicados.

Cabe salientar que a comunicação de possíveis deficiências no processo de gestão de riscos deve ocorrer de forma clara, explicitando as implicações da falha e as necessidades de reavaliação. Para tanto, pode-se contar com canais de comunicação internos para que as falhas sejam relatadas para os responsáveis envolvidos na atividade e suas chefias – propiciando pos-

síveis medidas corretivas – e canais alternativos para casos mais sensíveis, como denúncias de práticas impróprias ou ilegais (COSO, 2007).

3. Por que assumir riscos?

Não é novidade que o desafio de lidar com riscos envolve uma série de incertezas e receios, pois as consequências podem ser desagradáveis. No entanto, tais inquietações não devem ser sempre as condutoras das decisões, pois afastam a organização das possibilidades de explorar retornos positivos oriundos dos riscos assumidos.

Nesse sentido, embora o conceito de risco seja reconhecido, predominantemente, pela perspectiva negativa, a assunção de riscos é um canal importante para novas oportunidades, quando feito com consciência e responsabilidade. Através da gestão dos riscos, estes podem se tornar aliados do desenvolvimento organizacional, especialmente quando se tem uma visão realista sobre a sua probabilidade de ocorrência, sobre seus resultados esperados e sobre as abordagens mais adequadas para lidar com eles (Damodaran, 2009).

Segundo Damodaran (2009), existem diferentes formas de servir-se da assunção de riscos para alcançar vantagens competitivas frente aos concorrentes, especialmente a partir de fatores como:

i) Ter acesso, de forma rápida, a informações mais atualizadas e detalhadas sobre eventos e suas consequências possibilita a formulação de respostas de maior qualidade para as situações enfrentadas. Investimentos em tecnologia são bons aliados para garantir a vantagem informacional das organizações.

ii) Responder, mais rápido do que os concorrentes, às circunstâncias, adaptando métodos e locais de negócios, pois essa velocidade pode ser crucial para a conversão de ameaças em oportunidades. Para tanto, deve-se considerar o papel da estrutura organizacional na agilidade das reações, assim como a clareza sobre o público-alvo ao qual se dirigem as respostas.

iii) Considerar as lições aprendidas em crises semelhantes do passado e o entendimento de como essas crises impactaram o mercado são caminhos para reagir de maneira mais eficaz do que outras empresas do mesmo setor.

iv) Possuir recursos financeiros e de pessoal para enfrentar períodos de crise, e seus resquícios em períodos subsequentes, com mais serenidade em comparação com outras empresas do setor.

v) Dispor de flexibilidade financeira e operacional, incluindo a capacidade de ajustar a base tecnológica e estruturas administrativas do negócio em res-

posta a mudanças no ambiente, vantagem essa que é significativa entre empresas disruptivas, quando comparadas com as tradicionais.

Ainda que existam tamanhas oportunidades, é essencial considerar a quantidade de riscos assumidos, de modo que o gerenciamento não se torne excessivamente dispendioso ou desafiador para a organização. Assim, é fundamental que a empresa realize uma avaliação detalhada da sua gestão de riscos para determinar a melhor maneira de realizá-la, mantendo uma constante vigilância sobre as externalidades resultantes de suas atividades, considerando seu impacto tanto para a própria organização quanto para a sociedade (IBGC, 2017).

Síntese do Capítulo

O segundo capítulo chegou ao fim! Nele pudemos conhecer o que é a gestão de riscos, seus benefícios e atores envolvidos no desenvolvimento desse processo, ressaltando que toda a organização deve se sentir responsável por isso! Em seguida, foram apresentados os 10 princípios fundamentais que ilustram a essência da gestão de riscos e que, se respeitados, potencializam uma administração consistente, adequada e comprometida com a sustentabilidade da organização. Vimos também que o processo de gestão de riscos deve se adequar à realidade de cada organização, podendo ser fundamentado em modelos já existentes – como propõe a norma ISO 31000 e o modelo COSO ERM – ou na construção de uma metodologia personalizada ao negócio, prezando pela adaptação de boas práticas pré-existentes e de etapas basilares, tais como: identificação e classificação dos riscos, avaliação, resposta e monitoramento dos riscos. Por fim, objetivou-se expor diferentes motivos pelos quais as organizações podem assumir riscos e, com isso, conquistar diferenciais competitivos, desde que tomem essa decisão com prudência e respaldo de todo o processo de administração de riscos realizado. No próximo capítulo, você conhecerá um outro elemento crucial para a sustentabilidade das organizações: o *Compliance!* Dessa vez, com enfoque em questões associadas à conformidade e à integridade das operações do ambiente de negócios.

Atividades de avaliação

1. Por que a gestão de riscos é importante para as organizações? Explique com o auxílio de pelo menos um dos conceitos estudados.
2. Quais são, princípios fundamentais da gestão de riscos? Escolha um, justifique sua escolha e discorra sobre a importância dele, em particular, para o contexto organizacional.
3. Quais as etapas do processo de gestão de riscos? Como elas interagem entre si?
4. Cite as principais vantagens competitivas relacionadas à assunção de riscos e reflita: quais são os desafios associados à assunção de riscos como estratégia competitiva?

Leituras, filmes e sites

Documentário

Overdose – The Next Financial Crisis: o documentário aborda as causas e consequências da crise financeira global de 2008 e adverte sobre os riscos de uma crise financeira futura. Dentre as causas, pode-se perceber a ganância e complacência que prevaleciam no sistema financeiro antes da crise, com bancos e instituições financeiras tomando riscos excessivos em busca de lucros cada vez maiores.

Capítulo 3

Introdução ao *Compliance*

Objetivos

- Definir o conceito de *Compliance* e expor como ele contribui para a geração de valor organizacional;
- Compreender o papel das regulamentações no desenvolvimento do *Compliance*, destacando sua importância na definição de padrões éticos e legais para as empresas;
- Descrever os pilares do *Compliance* e seus respectivos papéis na promoção de uma cultura de integridade e conformidade dentro da organização;
- Compreender os desafios na implantação do *Compliance* e refletir como eles podem ser trabalhados para garantir uma implementação bem-sucedida do programa de *Compliance.*

Introdução

O termo *Compliance* é constantemente associado ao ato de estar em conformidade com as leis, regulamentos e padrões éticos. Contudo, isso não se deve apenas ao foco em evitar penalidades legais, mas também às significativas contribuições do *Compliance* para a geração de valor organizacional, refletindo na construção de uma reputação sólida, na confiança dos stakeholders, na redução de riscos e na promoção de um ambiente de trabalho ético e transparente.

De acordo com dados disponibilizados pela Deloitte (2022) em seu relatório sobre a evolução do *Compliance* no Brasil, entre os anos de 2019 e 2021 foram diversos os tipos de irregularidades descobertas: conflitos de interesses não divulgados, favores de cunho pessoal, subornos, uso de influência para obter vantagens sobre funcionários públicos, repasse de propinas, compartilhamento de informações confidenciais a terceiros e manipulação de licitações.

Contudo, a maioria dos casos supracitados foram descobertos com o auxílio de instrumentos de *Compliance*, como canais de denúncia e processos de controles internos, o que evidencia a importância crescente desse tema no contexto organizacional.

1. O que é *Compliance*?

O termo *Compliance* é derivado do inglês "*to comply*", que significa cumprir, estar em conformidade com o que foi imposto, lançando luz, especialmente, sobre aspectos legais e princípios éticos que auxiliam a redução ou eliminação de riscos associados à reputação de uma instituição. Não é incomum o uso do termo "integridade" como um sinônimo de *Compliance* na língua portuguesa, pois o ato de ser íntegro remete à honestidade, retidão e ausência de corrupção (ITI, 2018).

Na derivação do latim "complere" o *Compliance* significa a vontade de realizar o que for solicitado, de cumprir as normas e aspectos legais, definição que, quando abordada no contexto institucional, trata-se de estar em conformidade com o cumprimento das regulamentações internas e externas à organização, priorizando condutas éticas e íntegras. No Brasil, o termo costuma estar associado à denominação de um departamento ou de práticas de auditoria interna, contemplando também os esforços direcionados a políticas de governança corporativa que reduzam os riscos de perda da reputação do negócio (Blok, 2023).

De fato, o *Compliance* guarda uma forte relação com a governança corporativa, tendo em vista que é uma das ferramentas de governança que auxilia o exercício das boas práticas de administração e dos seus pilares: transparência, equidade, prestação de contas e responsabilidade corporativa (IBGC, 2020). Ao longo do tempo, cada vez mais o *Compliance* tem ido além do cumprimento das legislações, incluindo a cultura organizacional e o comportamento dos sujeitos inseridos nas organizações (Mendonça, 2018).

Para assegurar que as atividades da organização estejam em conformidade com as normas e com as legislações, faz-se necessário um programa que viabilize o acompanhamento periódico das políticas e dos procedimentos internos, abrangendo a avaliação do engajamento da alta gestão, a rápida resolução dos diagnósticos de ações ilícitas, a efetividade dos controles internos, a comunicação tempestiva e a capacitação das partes interessadas (Blok, 2023).

Nessa perspectiva, um programa de *Compliance*, também conhecido como programa de integridade, é um sistema processual e ordenado, desenvolvido para que as organizações – dos mais diversos setores e estruturas hierárquicas de decisão – sejam capazes de implementar ações que as conduzam a estar em conformidade com as políticas, regulamentações e condutas éticas (ITI, 2018). Tais programas contam com mecanismos, metodologias e controles voltados à prevenção, constatação, exame e tratamento dos riscos de corrupção, além de políticas sancionatórias que visam punir e modificar eventuais comportamentos ilícitos (Souza, 2018).

Ademais, é um equívoco limitar o *Compliance* à uma ferramenta de verificação de conduta, pois ele permeia toda a organização e atua como um guardião da imagem organizacional e de sua longevidade. Tal longevidade pode ser associada não apenas ao controle dos riscos, mas também à manutenção de recursos financeiros, os quais são conservados quando a instituição não precisa reduzir seu fluxo de caixa para arcar com multas, sanções e processos em decorrência de quebras de *Compliance* (Candeloro, 2014).

Dessa forma, muitos profissionais defendem que o custo de implementação de um programa de *Compliance* é menor do que o custo de não tê-lo, pois não são poucos os casos de organizações e de indivíduos que, ao se envolverem em casos de corrupção, enfrentam punições consideráveis, como multas de valor expressivo, danos irreversíveis a reputação da marca, sanções, cassações de licenças e diversos processos criminais (Blok, 2023). Nesse contexto, a autora lista algumas das diversas contribuições para a geração de valor institucional, tais como:

i) potencialização da gestão de riscos, pois viabiliza a identificação e tratamento dos riscos;

ii) conquista de vantagem competitiva, pois as organizações que possuem programas de *Compliance* se tornam mais atraentes para os stakeholders;

iii) valorização da imagem e da reputação do negócio, comunicando credibilidade e confiança ao mercado;

iv) tendência ao alcance de maiores investimentos, pois a solidez e a boa reputação são características valorizadas pelos investidores;

v) aumento da eficiência e da produtividade nas operações, pois a organização funciona dentro dos padrões técnicos adequados;

vi) respaldo jurídico, pois a organização conta com ciclos de auditoria e monitoramento contínuo em um programa de *Compliance,* além de claras consequências aos atos fraudulentos;

vii) construção de uma consciência coletiva voltada a prevenção de não-conformidades, através da capacitação dos funcionários sobre o programa de *Compliance* e sobre a importância de um âmbito laboral ético.

Com isso, salienta-se que o *Compliance* é benéfico para que as pessoas jurídicas e físicas sejam estimuladas a desenvolver e fortalecer princípios éticos, boas condutas, ações honestas e um caráter íntegro, os quais devem ser refletidos para toda a sociedade e para as partes interessadas com quem convivem e estabelecem algum tipo de vínculo (Assi, 2018).

2. O papel das regulamentações no desenvolvimento do *Compliance*

A importância atribuída à normatização de valores e princípios éticos no âmbito das organizações, especialmente no que diz respeito ao combate à corrupção, tem se destacado como uma pauta significativa em nível global ao longo do tempo. De acordo com Souza (2018), os efeitos dos diversos escândalos de corrupção ocorridos pelo mundo apresentam efeitos que podem romper fronteiras e se expandir para além do território no qual a organização está situada, conferindo aos crimes de corrupção um caráter, por vezes, transnacional e, consequentemente, a necessidade de medidas extraterritoriais para lidar com eles.

Diante disso, por volta da década de 70, iniciou-se o surgimento de marcos legais que, por sua vez, contribuíram para que aspectos éticos e de conformidade fossem incentivados e consolidados nas empresas (Souza, 2018). Dentre esses marcos, Blok (2023) destaca alguns exemplos globais, a saber:

- A lei FCPA (*Foreign Corrupt Practices Act*), foi promulgada como um desdobramento do caso Watergate, em 1977, nos Estados Unidos da América (EUA). Ela estabelece a aplicação de punições, como sanções criminais e multas significativas, às pessoas físicas e jurídicas que, possuindo relações comerciais com os EUA ou ações negociadas na Bolsa de Nova York, pratiquem atos de corrupção envolvendo atores públicos governamentais no estrangeiro.
- A lei UKBA (*United Kingdom Bribery Act*) promulgada em 2010 no Reino Unido como um desdobramento da crise financeira de 2008 dos EUA. Ela também impõe penalidades significativas em circunstâncias de corrupção, como subornos diretos e indiretos, promessas e obtenção de vantagens, sejam elas financeiras ou não, mas compreende as pessoas físicas e jurídicas do Reino Unido, bem como as que mantém relações comerciais com o país, tanto do âmbito público quanto no âmbito privado.

No Brasil, a discussão sobre *Compliance* teve seus embriões na década de 90, quando o país buscava se alinhar ao mercado mundial, onde pairava a preocupação sobre a implementação de regulamentações mercadológicas internacionais (Blok, 2023). Nesse contexto, o país esteve envolvido, em 1997, na Convenção sobre o Combate da Corrupção de Funcionários Públicos Estrangeiros em Transações Comerciais Internacionais da Organização para a Cooperação e o Desenvolvimento Econômico (OCDE), momento em que os envolvidos assumiram, publicamente, a responsabilidade compartilhada de manter transações comerciais internacionais íntegras (Souza, 2018).

A partir disso, a convenção supracitada foi internalizada na legislação

brasileira através do decreto nº 3.678/2000 e, assim como muitas nações promulgaram suas leis anticorrupção, o Brasil também aprovou uma série de leis voltadas à integridade de suas entidades públicas e privadas, tais como: a Lei de Defesa da Concorrência (nº 12.529/2011); a Lei de Lavagem de Dinheiro (nº 9.613/1998 e nº 12.683/2012); a Lei de Conflito de Interesse (nº 12.813/2013); e a Lei Anticorrupção (nº 12.846/2013), sendo essa última a de maior destaque no tocante ao fomento da integridade (Vieira; Barreto, 2019).

Foi através da Lei Anticorrupção nº 12.846/2013 e do seu decreto regulamentador nº 8.420/2015 (revogado pelo decreto nº 11.129/2022) que o *Compliance*, de fato, passou a ser conhecido no Brasil e inseriu a nação no rol das detentoras de legislações inovadoras e avançadas sobre o enfrentamento da corrupção (Blok, 2023). De acordo com o artigo 5º da lei nº 12.846/2013, são atos lesivos à administração pública, no Brasil ou no estrangeiro, todos os que agirem contra o patrimônio e princípios da administração pública ou contra os compromissos assumidos pelo país em âmbito internacional. Na lei são listados, de forma não exaustiva, tais atos:

> I - prometer, oferecer ou dar, direta ou indiretamente, vantagem indevida a agente público, ou a terceira pessoa a ele relacionada;
>
> II - comprovadamente, financiar, custear, patrocinar ou de qualquer modo subvencionar a prática dos atos ilícitos previstos nesta Lei;
>
> III - comprovadamente, utilizar-se de interposta pessoa física ou jurídica para ocultar ou dissimular seus reais interesses ou a identidade dos beneficiários dos atos praticados;
>
> IV - no tocante a licitações e contratos:
>
> a) frustrar ou fraudar, mediante ajuste, combinação ou qualquer outro expediente, o caráter competitivo de procedimento licitatório público;
>
> b) impedir, perturbar ou fraudar a realização de qualquer ato de procedimento licitatório público;
>
> c) afastar ou procurar afastar licitante, por meio de fraude ou oferecimento de vantagem de qualquer tipo;
>
> d) fraudar licitação pública ou contrato dela decorrente;
>
> e) criar, de modo fraudulento ou irregular, pessoa jurídica para participar de licitação pública ou celebrar contrato administrativo;
>
> f) obter vantagem ou benefício indevido, de modo fraudulento, de modificações ou prorrogações de contratos celebrados com a administração pública, sem autorização em lei, no ato convocatório da licitação pública ou nos respectivos instrumentos contratuais; ou
>
> g) manipular ou fraudar o equilíbrio econômico-financeiro dos contratos celebrados com a administração pública;

> V - dificultar atividade de investigação ou fiscalização de órgãos, entidades ou agentes públicos, ou intervir em sua atuação, inclusive no âmbito das agências reguladoras e dos órgãos de fiscalização do sistema financeiro nacional (Brasil, 2013, on-line).

Tal marco legal estimula a implementação de programas de integridade no âmbito corporativo e impõe punições não só aos atos corruptos e de subornos contra os órgãos públicos e privados, mas também pune fraudes de contratos e licitações (Abreu; Urnikes, 2018), sendo este último um diferencial em relação às leis FCPA e UKBA mencionadas anteriormente.

Ademais, em 2014 emergiu o escândalo da Petrobrás no Brasil, um caso grave de corrupção que envolveu a estatal em um esquema de irregularidades, subornos e desvio de verbas públicas (Assi, 2021). Consequentemente, publicou-se a Lei Geral de Responsabilidade das Estatais, nº 13.303/2016, com o objetivo de que as estruturas de governança corporativa fossem aprimoradas e que o governo estabelecesse o *Compliance* público, exigindo que as organizações que têm relações comerciais com ele tenham um programa de integridade que garanta a existência de princípios éticos (Vieira; Barreto, 2019).

Outro importante marco regulatório que reforçou o papel do *Compliance* no Brasil foi a promulgação da Lei Geral de Proteção de Dados (LGPD), nº 13.709/2018, a qual entrou em vigor em 2020 e estabelece exigências sobre a proteção de dados pessoais, diante de um cenário em que o acelerado desenvolvimento tecnológico tem favorecido que as organizações coletem e armazenem dados sensíveis de seus consumidores. Assim, a nação se insere ainda mais nas discussões sobre o direito de privacidade e suscita práticas que auxiliem as organizações a estarem em conformidade com as exigências legais (Blok, 2023).

Saiba Mais

Além das regulamentações apresentadas anteriormente, existem normas técnicas que auxiliam as instituições na implementação dos programas de *Compliance*, através de diretrizes aceitas amplamente e que não possuem o objetivo de serem modelos fixos, mas sim parâmetros para um *Compliance* efetivo. São exemplos:

ISO 37301:2021 - Sistema de Gestão de *Compliance*

A ISO 37301 é considerada uma evolução da norma ISO 19600:2014 e oferece uma abordagem mais específica e detalhada para a implementação de um sistema de gestão de *Compliance*. Ela se concentra em fornecer orientações específicas para desenvolver, implementar, manter, aperfeiçoar e avaliar um sistema de *Compliance* eficaz (ABNT, 2021).

Nessa perspectiva, a ISO 37301 estabelece que um bom sistema de gestão de *Compliance* é pautado nos seguintes princípios: integridade, boa governança, proporcionalidade, transparência, responsabilização e sustentabilidade. Assim, tal sistema é composto por 18 elementos, distribuídos sob a lógica do PDCA (do inglês "*plan–do–check–act*", que significa planejar, fazer, verificar e agir) a saber:

- Planejar: comprometimento em todos os níveis; determinação do escopo do sistema de *Compliance*; elaboração da política de *Compliance*; definição de papéis e responsabilidades; levantamento das principais obrigações e riscos de *Compliance*.
- Fazer: apoio; competência e conscientização; comunicação e treinamento; operação; controles e procedimentos; documentação.
- Verificar: auditoria interna; análise crítica pela direção; monitoramento e medição; levantamento de preocupações; processo de investigação.
- Agir: gerenciando não *Compliance*; melhoria contínua.

Cabe destacar que a organização pode determinar não apenas o escopo do seu sistema de gestão de *Compliance*, mas também a sua amplitude de aplicação, observando as necessidades do contexto legal, social, cultural, digital, financeiro, ambiental, bem como das estruturas e das partes interessadas (ABNT, 2021).

ISO 37001:2016 - Sistema de Gestão Antissuborno

A ISO 37001 é mais específica e se concentra na prevenção, detecção e tratamento de um aspecto específico de *Compliance*: o suborno. De fato, o suborno ainda é uma prática disseminada no mundo inteiro, gerando impactos negativos diversos: instabilidades políticas, aumento dos custos dos negócios, desmotivação dos funcionários, barreiras às relações comerciais, etc (ABNT, 2016).

Ainda que muitos governos tenham instituído leis antissuborno e práticas preventivas, faz-se necessário que as organizações estabeleçam medidas antissuborno que complementem as ações governamentais, contribuindo para o aculturamento dessa pauta. Diante disso, o sistema de gestão antissuborno é apresentado como uma alternativa para que sejam implementados ou reforçados controles que minimizem as possibilidades dessa inconformidade ocorrer, fomentando uma cultura antissuborno nos setores público, privado e sem fins lucrativos (ABNT, 2016).

Dentre as medidas emergentes desse sistema, tem-se:

- adoção de políticas antissuborno;
- definição de um responsável pela supervisão do funcionamento das políticas;
- acompanhamento e treinamento dos funcionários;
- avaliações de riscos em iniciativas e terceiros;
- implementação de controles financeiros e comerciais;
- instituição de procedimentos de investigação e relatórios.

Logo, essa norma auxilia a mitigação de riscos de suborno, podendo ser integrada a um sistema de gestão de *Compliance* mais amplo (ABNT, 2016).

Com isso, as instituições possuem caminhos para construir um sistema de *Compliance* robusto e promover uma cultura de integridade e conformidade em toda a empresa.

Desse modo, o *Compliance* foi ganhando cada vez mais espaço e importância nas legislações por todo o mundo, fato perceptível nas principais leis aqui mencionadas, as quais representam apenas uma parte dos marcos legais existentes e possuem, em sua essência, o incentivo à implementação

de programas de integridade que, de forma preventiva e corretiva, podem contribuir com a filosofia anticorrupção das nações.

3. Pilares do *Compliance*

Para que a implantação e manutenção dos programas de *Compliance* sejam realizadas de forma eficiente e compreensível no âmbito das instituições brasileiras, a Controladoria Geral da União (Brasil, 2017) estabeleceu os cinco pilares fundamentais que tais programas devem possuir. São eles:

3.1. Comprometimento da alta administração

A alta administração – como diretores e, em alguns casos, o conselho de administração – possui papel central no aculturamento da organização sobre as práticas de *Compliance*, não apenas através do encaminhamento de políticas e exigências de conformidade aos integrantes da empresa, mas também por meio de comportamentos éticos que sirvam de exemplo e estímulo para os demais níveis hierárquicos (Andrade, 2024).

Por ocupar o topo da hierarquia, a alta direção, muitas vezes, está sob os holofotes dos funcionários, os quais analisam, e até mesmo imitam, suas filosofias e ações, seja por admirá-los ou por temê-los, fato que exige comprometimento das lideranças com o cumprimento dos programas de *Compliance* (ITI, 2018). Ainda que a organização possua políticas internas, código de conduta, auditoria interna, dentre outros instrumentos de conformidade, esses não garantem a ausência de inconformidades se não forem aliados a uma atuação ética e exemplar dos administradores (Andrade, 2024).

De acordo com o Instituto Nacional de Tecnologia da Informação (2018), esse comprometimento pode ser demonstrado de várias formas: participando e apoiando todo o processo de implementação do programa de *Compliance*; sendo éticos em suas relações; conscientizando toda a organização e seus stakeholders da importância da conformidade; e direcionando recursos financeiros e de pessoal para o desenvolvimento e implementação do programa. Outro exemplo se dá quando membros da alta administração cometem infrações e aceitam ser submetidos às punições vigentes (Assi, 2018).

3.2. Instância responsável pelo programa de integridade

Além da responsabilização da alta administração, é fundamental que haja uma alçada encarregada do acompanhamento de todas as ações relacionadas ao programa de *Compliance*, para que ele se desenvolva de forma adequada, podendo ser uma pessoa ou um grupo de pessoas (ITI, 2018).

A função de *Compliance* deve abranger as seguintes responsabilidades:

- Viabilizar a identificação das obrigações;
- Providenciar a documentação da avaliação dos riscos;
- Garantir o alinhamento entre o sistema de gestão com os objetivos;
- Acompanhar e mensurar o desempenho;
- Examinar o desempenho do sistema de gestão e identificar necessidades corretivas ou preventivas;
- Desenvolver um histórico de documentações;
- Estimular que o sistema de gestão seja analisado periodicamente de forma crítica;
- Levantar preocupações e assegurar que elas sejam analisadas e endereçadas (ABNT, 2021).

Em algumas organizações existe a função de *Compliance Officer*, sujeito responsável por instruir as diversas áreas da organização sobre os regulamentos e políticas aplicáveis ao contexto de atuação do negócio, comprometendo-se com a busca e manutenção de uma cultura pautada em elevados padrões éticos (Candeloro, 2014). Para a autora, iniciativas como o estabelecimento relações externas e a coordenação de auditorias devem ser comandadas pelo *Compliance Officer*.

Contudo, independentemente de a alçada responsável ser um *Compliance Officer* ou um grupo de pessoas, tais indivíduos devem dispor de atributos como autonomia, imparcialidade e recursos – financeiros e de pessoal – para desempenhar com eficiência seu papel (ITI, 2018). Além disso, também se faz necessário um contato direto desses atores com a alta administração, sem intermediários, para evitar desvios nas informações e interferências pessoais no cumprimento das normas, facilitando a imposição adequada de orientações e de punições aos sujeitos que cometerem infrações (Andrade, 2024).

3.3. Análise de Riscos

O desenvolvimento de um programa de *Compliance* deve ser fundamentado em uma boa administração dos riscos, pois conhecendo os riscos aos quais o negócio está vulnerável é que os responsáveis pelo programa podem buscar mitigá-los ou eliminá-los através da definição de políticas, controles, capacitações e monitoramentos adequados. Convém destacar que, para garantir a efetividade do programa, a análise dos riscos deve ser periódica, pois novos riscos podem emergir após o seu período de estruturação (ITI, 2018)[1].

No âmbito corporativo e governamental, especialmente nesse último, há a necessidade de uma atenção maior aos riscos de corrupção, os quais

[1] As classificações dos riscos estão dispostas no primeiro capítulo deste material – sendo de interesse do *Compliance*, principalmente, os riscos de conformidade e de integridade – e o processo de gestão de riscos está apresentado no segundo capítulo.

podem ser tratados pela Lei Anticorrupção (Assi, 2018), apresentada anteriormente neste capítulo. O autor salienta que a corrupção emerge com facilidade nas organizações, de diferentes formas, como através de fraudes em licitações, concessões de alvarás de funcionamento, licenças, fiscalizações de produtos e em decisões judiciais.

Ademais, de acordo com o porte da organização e com os recursos disponíveis para a cobertura dos riscos, o programa de *Compliance* pode contemplar, inicialmente, apenas os riscos de alta severidade e, ao longo do tempo, através de reavaliações sucessivas, considerar os demais riscos, tornando o nível do programa cada vez mais avançado (Assi, 2018).

3.4. Estruturação das regras e instrumentos

Nesta etapa, a alçada responsável pelo programa de *Compliance*, já ciente dos riscos aos quais a organização está submetida, deve definir as diretrizes disciplinares e de remediação para os casos de irregularidades, bem como os instrumentos que melhor auxiliarão a comunicação e a detecção desses casos. Lista-se abaixo, de forma não exaustiva, alguns dos principais instrumentos que podem compor essa etapa:

a) Código de Conduta

O código de conduta é um instrumento essencial para o esclarecimento dos direitos e deveres de todas as partes envolvidas na organização – sejam internas ou externas – tornando formais as expectativas acerca da conduta esperada desses stakeholders. Nesse sentido, as diretrizes e normas pré-estabelecidas podem ser registradas em um código, ou manual, e comunicadas para facilitar a prevenção das quebras de integridade ou a penalização por desobediência (Assi, 2018).

b) Canal de denúncias

O canal de denúncias é um importante instrumento de comunicação para que todos os sujeitos envolvidos na organização, de forma interna e externa, possam manifestar irregularidades ou denunciar problemas diversos. Através das denúncias, riscos importantes podem ser identificados, investigados e solucionados, sendo imprescindível que pessoas capacitadas conduzam esse instrumento, tendo em vista que quaisquer falhas podem prejudicar a manutenção da credibilidade da organização (Candeloro; Benevides, 2013).

Para que tal canal seja eficiente, é essencial que esteja disponível em meios de comunicação variados, que ofereça a possibilidade de anonimato e proteções contra retaliações aos usuários, e que o acesso às queixas seja restrito, garantindo a confiabilidade do processo (Assi, 2018). Assim, periodicamente a alta gestão pode ser atualizada sobre as denúncias recebidas,

sobre como elas estão sendo investigadas e quais as punições sugeridas, viabilizando retornos aos usuários.

c) Due Diligence

A *due diligence* – ou gestão de terceiros – trata-se de uma investigação prévia sobre pessoas físicas e jurídicas com as quais a administração da organização pretende realizar transações e estabelecer vínculos (Assi, 2018). Segundo Bittencourt (2014), tal prática potencializa a evolução do programa de *Compliance*, pois contempla desde as relações com fornecedores e parceiros a fusões e aquisições de empresas, fornecendo informações valiosas para a gestão de riscos e para a tomada de decisões associadas a transações comerciais.

Tal prática pode ser desenvolvida desde a etapa de análise de riscos.

3.5. Mecanismos de incentivo e sanções

A adesão de toda a organização ao programa de *Compliance* passa pelo incentivo às boas condutas e pela aplicação de sanções aos casos de inconformidade, de acordo com a gravidade de cada caso. A detecção e o tratamento das infrações recorrentes são importantes para que a credibilidade e a segurança jurídica da organização não sejam prejudicadas (Candeloro; Benevides, 2013).

Para tanto, faz-se necessário que todos os funcionários tenham acesso às regras e às consequências do não cumprimento delas, assim como deve ser bem estabelecido qual será a área responsável pela comunicação e pela aplicação dos incentivos ou das sanções, como, por exemplo, o setor de recursos humanos ou jurídico (Candeloro; Benevides, 2013).

A existência de todas as regras e instrumentos deve ser de fácil acesso e constantemente abordada em treinamentos de compliance, pois quaisquer atos ilícitos que persistirem, mesmo com a ampla divulgação das diretrizes, devem ser corrigidos para desestimular a ocorrência de novas infrações (ITI, 2018).

a) Controles Internos

Um ambiente munido de controles internos é fundamental para o bom funcionamento do programa de *Compliance*, pois eles envolvem metodologias e ferramentas que auxiliam o desempenho correto dos processos organizacionais, contemplando o que deve ser feito, como deve ser feito e as motivações para tal, dificultando a recorrência de erros comuns e de fraudes nas operações do negócio (Façanha et al., 2020).

Diante de diversas formas de realizar as atividades no âmbito organizacional, os controles internos atuam como uma forma de estabelecer padrões

e conscientizar os indivíduos de suas respectivas responsabilidades, especialmente no tocante à qualidade e conformidade (Assi, 2018). Tais controles não objetivam tornar os processos mais burocráticos, mas sim contribuir com o fomento de boas práticas internas, com a proteção do negócio e com sua longevidade (Candeloro, 2014).

A temática dos controles internos será abordada com maior detalhamento no capítulo 4 deste material.

b) Instrumentos de comunicação e treinamento

Cumpre destacar que são ínfimas as chances de eficácia de um programa de *Compliance* e dos instrumentos supracitados se não forem comunicados de forma clara e direta para todos os atores organizacionais, pois são as ações de comunicação e de treinamento que podem contribuir com o aculturamento do *Compliance* na organização (ITI, 2018).

Diante disso, as diretrizes e fundamentos devem ser consultadas, comunicadas e esclarecidas, periodicamente, às partes interessadas – os riscos identificados, as normas e políticas pré-estabelecidas para controlá-los, as mudanças em quaisquer processos, etc – para que os planejamentos se tornem uma realidade e para que todos os envolvidos sintam-se motivados a alcançar os objetivos propostos (Assi, 2018). Segundo o mesmo autor, muitos casos de corrupção acontecem por agentes externos contratados, sendo válido o estímulo ao compartilhamento das normas e políticas, de fato, com todos que possuírem vínculos com o negócio.

A realização de treinamentos pode auxiliar a redução de muitos riscos, tendo em vista que a capacitação pode ser direcionada aos processos e controles prioritários, bem como ao reforço das normas que forem, repetidas vezes, infringidas (ITI, 2018). A constância dos treinamentos contribui para a internalização dos benefícios de prezarem pela integridade e para a construção de uma consciência coletiva favorável (Candeloro; Benevides, 2013).

c) Monitoramento Contínuo

O monitoramento do programa de *Compliance* consiste em uma etapa crucial para que a eficácia e a dinâmica do seu funcionamento sejam favorecidas, pois permite que sejam diagnosticadas as necessidades de revisões e atualizações nas diretrizes e nos processos, bem como a identificação de novos riscos e oportunidades (ITI, 2018).

Quaisquer mudanças organizacionais, como novos processos, setores e áreas de atuação, podem implicar alterações no cenário de riscos e nas ações de prevenção, fato que exige um monitoramento contínuo e consistente de todos os pilares do programa, abrangendo todos os níveis hierárquicos, de modo a tornar o cumprimento do *Compliance* uma prática diária e prioritária no contexto de trabalho (Candeloro; Benevides, 2013).

Nessa etapa é importante a definição da periodicidade e dos responsáveis por realizar o monitoramento, bem como quais serão os mecanismos que auxiliarão essa função, como indicadores de desempenho e sistemas de controle, os quais devem ser distribuídos entre os diferentes pilares do programa de *Compliance* (ITI, 2018).

4. Desafios na implantação do *Compliance*

A implementação de um programa de *Compliance* não é realizada de forma padrão entre as organizações, nem se trata de uma ferramenta já pronta para ser adquirida, pois as diferenças estruturais e culturais, os objetivos e as características de cada negócio devem ser levados em consideração para a construção de um programa efetivo (Candeloro, 2014).

Assim, o *Compliance* se revela como um processo gradual que, cotidianamente, vai sendo construído, refinado e inserido na cultura da organização, sob o custo de muita dedicação, paciência e conhecimentos sobre a dinâmica do negócio – seus valores, particularidades, limites, processos, objetivos de curto e longo prazo, etc – de modo que, quando bem fundamentado, torna-se um grande parceiro do sucesso empresarial (Mendonça, 2018).

Diante disso, são inúmeros os desafios que permeiam a implementação e a atuação do *Compliance,* pois suscita mudanças culturais, por vezes, representativas. Uma dessas mudanças é o alcance de um maior engajamento dos atores organizacionais com a execução do programa de *Compliance,* fato consideravelmente difícil, pois depende da conscientização de todos os envolvidos acerca da importância e dos benefícios do *Compliance,* bem como do esclarecimento das consequências que podem atingi-los caso o programa não seja implementado (Candeloro, 2014).

Além disso, Candeloro (2014) também destaca que a dificuldade supracitada é potencializada pelas barreiras à inovação de pensamentos que, muitas vezes, são impostas por sujeitos que negligenciam seu comprometimento com os objetivos da organização e se mantém apegados ao seu *modus operandi* pessoal, preferindo desempenhar suas atividades seguindo os mesmos ritmos e métodos de sempre, sem transformações.

Outros desafios enfrentados estão associados à adequação e operacionalização dos instrumentos de *Compliance*, tais como:

- Obter o comprometimento dos indivíduos com análises de riscos periódicas;
- Garantir a execução e atualização do código de conduta;
- Se adequar à complexidade crescente das regulamentações;
- Absorver os custos de implantação e de não-conformidade;

- Definir os mecanismos e a periodicidade do monitoramento do programa;
- Manter a independência e a autonomia dos responsáveis;
- Assegurar a confidencialidade do conteúdo dos canais de denúncias e políticas de não retaliação diante de punições;
- Definir, de acordo com os riscos de *Compliance*, quem serão os sujeitos que receberão treinamentos e capacitações, além de estabelecer mecanismos para mensurar a eficácia dessa capacitação.

Acerca desse último desafio mencionado, que abrange a necessidade de treinamentos para mitigar riscos de integridade e *Compliance*, cabe salientar que essa capacitação vai além do âmbito interno, pois os terceiros com quem a organização estabelece vínculos interferem em sua reputação. Dados do relatório da Deloitte (2022), já mencionado neste material, apontam que o principal desafio relacionado ao *Compliance* é o monitoramento de terceiros, seguido da integração do *Compliance* aos demais departamentos da organização e, em terceiro lugar, a ampliação do escopo da área.

De fato, no mesmo relatório supramencionado, constata-se que, apesar de muitas empresas investirem em treinamentos de integridade para seus profissionais, em apenas 9% delas os contemplados são, em maioria, terceiros, enquanto 74% das organizações focam sua capacitação nos membros da alta gestão.

Nessa conjuntura, o incentivo da alta gestão e das lideranças, de modo geral, faz-se essencial para o enfrentamento desses desafios, promovendo um bom trabalho de conscientização sobre o papel do *Compliance* na estratégia, na cultura e na rentabilidade do negócio, bem como as consequências de sua ausência e das práticas fraudulentas. Além disso, a comunicação top down, quando contínua e compreensível, favorece que – seja por interesse, seja por obediência – as práticas de *Compliance* sejam priorizadas como algo intrínseco aos padrões operacionais e estratégicos da organização, fortalecendo condutas positivas e desencorajando quebras de integridade passíveis de punição (Candeloro, 2014).

Síntese do Capítulo

O terceiro capítulo chegou ao fim! Nele pudemos conhecer o que é o *Compliance*, apresentado como sinônimo de integridade no contexto brasileiro, e as diversas formas através das quais ele gera valor institucional. Vimos também que os debates em torno do *Compliance* possuem raízes no desen-

volvimento de diversas regulamentações, no Brasil e no mundo, com destaque para a Lei Anticorrupção que marcou a inserção oficial do Brasil no rol de legislações inovadoras voltadas ao enfrentamento da corrupção, especialmente no que tange à implementação dos programas de integridade. Evidenciamos também que a implantação dos programas de *Compliance* são permeadas por desafios, que vão desde a adequação e operacionalização dos instrumentos de *Compliance*, até barreiras pessoais e mudanças culturais. Tais desafios podem e devem ser trabalhados, especialmente pela alta gestão e conselhos de administração, viabilizando que as quebras de integridade sejam passíveis de punição e que as condutas positivas sejam encorajadas. No próximo capítulo, você aprenderá sobre um conceito essencial para a gestão de riscos e para a garantia das práticas de *Compliance*: O Controle Interno!

Atividades de avaliação

1. O que é *Compliance*? Como ele contribui para a geração de valor organizacional?
2. Através de qual marco legal o *Compliance* passou a ser conhecido, de fato, no Brasil? Realize uma breve pesquisa e disserte sobre os principais benefícios dessa lei.
3. Quais são os pilares do *Compliance* e qual o papel de cada um deles na promoção de uma cultura de integridade e conformidade dentro da organização?
4. Quais são alguns dos desafios presentes na implantação do *Compliance* em uma organização? Escolha um deles e responda: colocando-se no papel de um gestor que necessita solucionar esse desafio, como você o enfrentaria?

Leituras, filmes e sites

Filmes:

- A lavanderia (*The Laundromat*): o filme retrata os escândalos financeiros revelados pelos *Panama Papers*, que expuseram a extensa rede de corrupção, evasão fiscal e lavagem de dinheiro envolvendo figuras políticas, empresariais e celebridades ao redor do mundo, lançando luz sobre a importância do *Compliance* na prevenção e detecção de atos fraudulentos, especialmente em relação à lavagem de dinheiro e evasão fiscal.

- Polícia Federal – A Lei é Para Todos: o filme retrata a Operação Lava Jato, uma das maiores investigações de corrupção da história do Brasil, deflagrada em março de 2014, pela Polícia Federal do Brasil, em conjunto com o Ministério Público Federal (MPF) e outras autoridades, que teve como objetivo desmantelar um vasto esquema de corrupção envolvendo a Petrobras, grandes empreiteiras, políticos e seus partidos. Ele oferece várias lições sobre ética, corrupção, justiça e o papel das instituições na luta contra o crime.

Série:

- *Dirty Money* – Na rota do dinheiro sujo: a 1ª temporada da série aborda uma variedade de casos reais de corrupção, fraude financeira e má conduta empresarial em diferentes setores e países. É uma oportunidade para refletir e obter valiosos insights e lições sobre a importância do *Compliance* na prevenção e detecção de atividades ilícitas e antiéticas dentro das organizações. Disponível na Netflix.

Documentário:

- Enron – Os mais espertos da sala: o documentário narra a ascensão e queda da *Enron Corporation*, uma das maiores fraudes corporativas da história, gerando reflexões sobre a importância do *Compliance* na prevenção de fraudes e má conduta empresarial.

Capítulo 4

Controles Internos: um caminho para a conformidade

Objetivos

- Descrever o que são controles internos, bem como sua importância para as organizações e para a efetividade do *Compliance*;
- Compreender os componentes dos controles internos;
- Avaliar o nível de maturidade dos controles internos em uma organização;
- Reconhecer os desafios associados aos controles internos e refletir como eles podem ser trabalhados em diferentes dimensões organizacionais.

Introdução

Os Controles Internos são elementos fundamentais para a sustentabilidade organizacional, pois representam um caminho para a otimização de processos, para a identificação de fraudes, dentre outros eventos que auxiliam a efetividade de práticas importantes, como a gestão de riscos e o *Compliance*, anteriormente contextualizados. Nesse sentido, faz-se necessário investir na compreensão acerca do que são controles internos e por que implementá-los, reiterando seu papel basilar nas práticas de gestão.

Ademais, a garantia de que os controles internos estão estruturados de forma eficiente passa pelo entendimento acerca dos elementos que o compõem, de modo a constatar se todos estão implementados e funcionando de forma adequada à realidade do negócio. No entanto, cabe aos gestores a constante reflexão: "em que nível de controles internos o meu negócio está?" e, obtendo respostas honestas, deve ser providenciado um tratamento que eleve o empreendimento ao nível mais alto de controle e conformidade.

Embora cientes dos benefícios que podem ser obtidos através da implementação de controles internos, muitas organizações enfrentam desafios associados a essa decisão, como a complexidade das legislações, a resistência organizacional e a evolução tecnológica constante. Contudo, alternativas podem e devem ser cada vez mais exploradas para superar esses desafios e garantir a implementação e manutenção eficazes dos controles internos em toda a organização.

1. Definição e importância dos Controles Internos

O conceito de controle interno pode apresentar definições particulares quando aplicado de forma específica à determinados contextos organizacionais, como no caso da esfera pública. No âmbito da administração pública, em particular, pode-se conceituar o controle interno como um grupo de práticas de supervisão que objetiva garantir a observância das normas e o cumprimento das políticas públicas, por parte dos gestores e servidores, através da prevenção de irregularidades, fraudes ou mau uso de recursos públicos, além de abranger o combate à corrupção, a fiscalização dos processos e suporte ao controle externo (Cruvinel; Ribeiro; Oliveira, 2022).

Além disso, no Brasil, especialmente após a Constituição Federal de 1988, os poderes executivo, legislativo e judiciário puderam estabelecer seus mecanismos de controle interno que, quando bem integrados, auxiliam a fiscalização de seus próprios atos e agentes e buscam garantir a execução eficiente, eficaz e regular das políticas públicas e das ações governamentais (Cruvinel; Ribeiro; Oliveira, 2022).

Contudo, trataremos nesse capítulo do controle interno enquanto conceito que abrange tanto a esfera pública, como a esfera privada, pois, em ambos os casos, tem-se o objetivo comum de garantir a eficácia, eficiência, integridade e conformidade das operações da organização.

Logo, de modo geral, o controle interno pode ser definido como um conjunto de métodos, planos, atividades e políticas administrativas que, de forma interligada, objetivam a proteção do patrimônio da organização, o exame da veracidade dos dados contábeis, o alcance da eficiência operacional e o estímulo ao engajamento dos indivíduos às diretrizes estabelecidas pela alta administração. Em outras palavras, compreende-se que o controle interno abrange toda a administração da organização – seja ela pública ou privada – para que os objetivos sejam alcançados, sendo meios de controle, por exemplo, sistemas, comitês, planos de contas, manuais, treinamentos, divisão do trabalho, formulários, etc (Attie, 2018).

Os debates sobre controles internos têm sido incentivados ao longo do tempo, em virtude do seu valor agregado à redução dos riscos, ao gerenciamento de crises e à melhoria dos processos. Assim, diversas regras e legislações foram desenvolvidas para nortear a implementação de controles internos, como no Brasil, onde a resolução nº 2.554/98 do Banco Central dispôs sobre a implantação de sistemas efetivos de controles internos e de gestão de riscos em instituições financeiras (Rocha, 2018).

Outros exemplos podem ser mencionados em diferentes tipos de atividades:

- Empresas com ações negociadas na Bolsa de Valores podem seguir as diretrizes de governança corporativa fiscalizadas pela Comissão de Valores Mobiliários – CVM;
- Empresas com ações negociadas nos Estados Unidos podem se orientar pela Lei Sarbanes-Oxley;
- Operadoras de planos de saúde devem seguir os direcionamentos da Agência Nacional de Saúde Suplementar – ANS.

E as organizações que não possuem, necessariamente, um vínculo com os órgãos reguladores supracitados, podem se inspirar em modelos existentes e criar uma estrutura que melhor atenda suas necessidades específicas (Assi, 2021).

De modo geral, busca-se alcançar com a implantação de controles internos:

- A execução das operações de forma ética, eficiente, eficaz e econômica;
- O suporte à missão e à sustentabilidade da organização através do alcance dos objetivos estratégicos;
- A efetivação das obrigações de accountability;
- A observância das leis e regulamentos, governamentais e da própria instituição;
- A proteção dos recursos contra danos e perdas (Brasil, 2016).

Na definição dos controles internos, bem como em sua operacionalização, é importante considerar os riscos associados a eventos internos ou externos, visando reduzir sua probabilidade de ocorrência ou seus impactos sobre os objetivos organizacionais. Para tanto, os controles não devem ser implantados de forma relativa, mas sim de forma pensada, contínua e integrada às atividades e esforços de toda a organização (Brasil, 2016).

Não é incomum a presença de controles internos nas empresas, porém, nem sempre esses controles são os mais adequados para a realidade do negócio. Soma-se a isso o fato de que muitos gestores negligenciam a importância dos controles internos e depositam sua confiança apenas em funcionários eficientes, oportunizando a ocorrência de irregularidades e fraudes, sejam elas voluntárias ou não (Attie, 2018).

Os benefícios da implantação de controles internos eficazes são facilmente percebidos, tais como: maior confiança na administração do negócio pelo cumprimento dos requisitos legais; socialização de relatórios operacionais e financeiros pautados em informações de qualidade e confiáveis; aumento da eficiência dos processos; melhor fundamentação das decisões, especialmente quando envolvem julgamentos subjetivos; aumento da confiança

de investidores e parceiros de negócios, contribuindo para a consolidação de boas relações comerciais (COSO, 2012).

Ademais, a implementação de controles internos não deve ser vista apenas como uma ferramenta incremental de checagens, aprovações, registros, autorizações e monitoramento das operações, mas sim como um modelo precedido pela compreensão e pelo mapeamento dos processos para que, então, esses fluxos possam ser controlados (Assi, 2021). Portanto, a finalidade dos controles não é engessar a organização, mas sim protegê-la de si mesma e garantir sua longevidade (Candeloro, 2014).

No Brasil, entre os principais motivos para o fortalecimento do ambiente de controles internos, segundo a Delloite (2022), estão a busca pelo aumento da sustentabilidade do negócio, a minimização de riscos associados à imagem, a criação de programas de *Compliance* bem estruturados, e o atendimento às regulamentações locais.

Viu-se no capítulo anterior que a essência protetiva do *Compliance* no contexto empresarial se insere através de diretrizes e regulamentações que mitigam riscos e fomentam a conscientização de todos os agentes envolvidos no negócio, na busca por uma cultura de integridade (Candeloro, 2014).

Diante disso, a implementação de controles internos assume um papel prático e fundamental na identificação, prevenção e correção de inconformidades, pois o ambiente empresarial e as inúmeras incertezas que o rodeiam são fontes potenciais de danos irreparáveis, principalmente em empreendimentos que se preocupam apenas com o cumprimento mínimo das normas exigidas pelos órgãos reguladores, sem atenção estratégica à implementação de processos e controles adequados ao negócio (Assi, 2021).

Logo, é essencial que a atuação dos controles se dê nos diversos ramos de atividades e em todos os níveis da estrutura organizacional, além de serem constantemente revisados e atualizados – pela área de *Compliance*, de controles internos ou de auditoria interna – para garantir que todos os riscos aos quais a empresa está exposta estejam cobertos por controles internos e que *o Compliance* funcione de forma efetiva (Assi, 2021).

2. Componentes dos Controles Internos

Diante da crescente relevância dos controles internos como mecanismos estratégicos no âmbito corporativo, o COSO (2012) estabeleceu um modelo estrutural de controles internos que atenda aos mais diversos tipos de organizações de forma eficaz, o qual é composto por cinco elementos essenciais que devem funcionar em conjunto.

Saiba Mais

Um exemplo concreto da importância de controles internos e práticas de *Compliance* ocorreu em 2016, quando o banco Wells Fargo protagonizou um grande incidente financeiro nos Estados Unidos, ao ter seus funcionários acusados de abrirem contas bancárias e de cartões de crédito sem conhecimento e autorização dos clientes. A justificativa apresentada pelos funcionários foi pautada na agressividade das metas de vendas, motivando as práticas fraudulentas e antiéticas para obter bônus e promoções.

Em 2016, reguladores e pesquisadores descobriram tal cenário, que já ocorria desde 2011, e realizaram intensas investigações, resultando em demissões, ações legais, multas bilionárias e mudanças de pessoal, incluindo o CEO.

Percebe-se que as falhas abrangeram a cultura organizacional (ao enfatizar as metas de forma agressiva) e tornaram explícitas as necessidades de *Compliance* (diante das diversas condutas antiéticas, fraudulentas e de inconformidade) e de controles internos que detectassem e prevenissem as atividades fraudulentas.

Fonte: Exame (2016).

2.1. Ambiente de controle

Para que os controles internos sejam implementados, faz-se necessário preparar o ambiente organizacional para recebê-los. Isso envolve o estabelecimento de estruturas, bem como de determinados padrões e processos, que devem ser socializados para toda a organização – através da alta administração – de modo a esclarecer a importância da realização dos controles e as expectativas associadas ao comprometimento e envolvimento de todos nesse processo (COSO, 2012).

O ambiente de controle deve ser alicerçado em cinco princípios:

i) Conduta íntegra e ética por parte dos funcionários e servidores, prezando pelo apoio à manutenção dos controles internos em toda a organização;

ii) Comprometimento com a atração, retenção e desenvolvimento de pessoal capacitado e alinhado aos objetivos da organização;

iii) Independência dos responsáveis e órgãos reguladores, em relação aos gestores, para supervisionar a performance dos controles;

iv) Definição de estruturas organizacionais claras e de responsabilidades dos níveis hierárquicos sobre os controles para o alcance dos objetivos do negócio ou da política pública;

v) Responsabilização dos sujeitos sobre suas funções, no que concerne ao alcance dos objetivos por meio dos controles internos, através de políticas de gestão de pessoas e prestações de contas (Brasil, 2016).

2.2. Avaliação de riscos

Conforme visto no capítulo 2 desse material, a avaliação de riscos é uma etapa crucial no processo de gestão de riscos. Compreendendo que os controles internos agem sobre os riscos aos quais a organização está submetida, faz-se necessário que a identificação e a avaliação dos riscos sejam realizadas de forma adequada para que sejam definidos quais riscos serão administrados, prioritariamente, de acordo com seu grau de severidade e, a partir disso, quais controles serão exigidos[2].

De acordo com a Estrutura COSO (2012), a avaliação de riscos deve ser alicerçada em quatro princípios:

i) Clareza nos objetivos para que sejam diagnosticados os riscos que impactam em cada um deles;

ii) Identificação e análise dos riscos associados aos objetivos organizacionais, acompanhadas da seleção de quais riscos serão administrados;

iii) Ponderação da possibilidade de atos fraudulentos no processo de avaliação dos riscos;

iv) Exame de possíveis mudanças que possam alterar o funcionamento do sistema de controles internos.

[2] Sugestão: releia a seção "Processo de gestão de riscos" presente no capítulo 2 deste material.

2.3. Atividades de controle

Além de um ambiente propício à implantação de controles internos, faz-se necessária uma gama de atividades de controle que garanta o cumprimento das diretrizes por todos os envolvidos no negócio, em seus diversos estágios de desenvolvimento. Em outros termos, as atividades de controle são ações que auxiliam o cumprimento das políticas e normas de gestão, favorecendo a redução dos riscos e o alcance dos objetivos da entidade ou das políticas públicas (COSO, 2012).

Convém esclarecer que as atividades de controle podem ser classificadas de diferentes formas, a saber:

- **Pelo tipo de controle**:
  - Controle Preventivo: possui foco na prevenção de falhas e na minimização dos eventos de risco.
  - Controle Corretivo: possui foco na identificação de falhas e eventos de risco que já ocorreram.
  - Controle Compensatório: possui foco na redução temporária dos eventos de riscos, enquanto controles definitivos não são implementados.

- **Pela natureza do controle**:
  - Controle Manual: são realizados por pessoas, manualmente.
  - Controle Automático: são realizados através de sistemas.
  - Controle Híbrido: são realizados através da união de atividades manuais e automáticas.
- **Pela frequência do controle**: indica se o controle é realizado mais de uma vez ao dia, diariamente, semanalmente, mensalmente, trimestralmente, semestralmente, anualmente, etc.
- **Pela relação que o controle estabelece com o risco**:
  - Controle Direto: está relacionado aos controles operacionais, com foco na redução dos riscos associados.
  - Controle Indireto: está relacionado ao ambiente de controles, com foco na prevenção e detecção de eventos de riscos, como forma de auxiliar na redução desses (Brasil, 2017).

O quadro abaixo apresenta, de forma não exaustiva, exemplos de atividades de controle selecionadas pela Assessoria Especial de Controle Interno do Ministério do Planejamento, Desenvolvimento e Gestão, com base em alguns tipos de riscos que, comumente, emergem no âmbito organizacional (Brasil, 2017):

Quadro 1

Controles Básicos			
Categoria de Risco	**Fatores**	**Subfatores**	**Controles Básicos**
Risco de Integridade			Postura da alta administração
			Políticas e procedimentos anticorrupção
			Mapeamento dos Riscos de Corrupção
			Criação de indicadores dos riscos de corrupção
Risco de Conformidade			Acompanhamento e Análise de Normas e Regulamentos Externos
			Pareceres da Assessoria Jurídica
			Atividades de Treinamento
			Normas e Procedimentos

continuação do Quadro 1

Controles Básicos			
Categoria de Risco	**Fatores**	**Subfatores**	**Controles Básicos**
Risco Operacional	Pessoas	Carga de trabalho	Planejamentos de longo, médio e curto prazos
			Acordo de Trabalho
			Pesquisa de Clima Organizacional
			Reuniões Participativas
		Competências	Identificação da Necessidade de Conhecimento / Habilidades
			Atividades de Treinamento
			Normas e Procedimentos
			Ferramentas de autoavaliação de Conhecimentos / Habilidades
		Qualidade de Vida no Trabalho	Pesquisa de Clima Organizacional
			Condições Ambientais
			Comunicação com a Administração
			Processo de Gerenciamento de Equipes
		Conduta	Valores Éticos e Normas de Conduta do Órgão / Unidade
			Mecanismos de Motivação / Recompensa / Punição
			Reconhecimento de Responsabilidade por Escrito
			Conferências e Autorizações
			Rodízio de Funcionários
			Segregação de Funções
			Testes de Conformidade
			Canais de Comunicação com a Sociedade
Risco Operacional	Processos	Comunicação Interna	Canais de Comunicação com os Servidores
			Normas e Procedimentos
		Modelagem	Ferramentas para Análise e Melhoria Contínua de Processos
			Metodologia de Autoavaliação de Riscos e Controles
			Validações – Backtesting
		Segurança Física	Mecanismos de Segurança Física
			Controles de Acesso Físico
			Manutenção de Equipamentos
		Pontos de Controle	Normas e Procedimentos
			Metodologia de Autoavaliação de Riscos e Controles
			Mecanismos de Monitoramento e Reporte
		Adequação à Legislação	Testes de Conformidade
			Normas e Procedimentos

continuação do Quadro 1

Controles Básicos			
Categoria de Risco	**Fatores**	**Subfatores**	**Controles Básicos**
Risco Operacional	Sistemas	Segurança Lógica	Políticas e Diretrizes
			Controles de Acesso Lógico
			Arquivo e Preservação de Registros
		Hardware e Software	Manutenção de Equipamentos
			Layout de formulários e Sistemas
			Planos de Contingência
		Análise e Programação	Layout de Formulários e Sistemas
			Validações – Backtesting
			Atividades de Treinamento
		Rede de Comunicação	Planos de Contingência
			Manutenção de Equipamentos
Risco Operacional	Eventos Externos	Desastres Naturais e Catástrofe	Planos de Contingência
			Atividades de Treinamento
		Ambiente Regulatório	Análise da Conjuntura Política e Econômica Nacional e Internacional
		Ambiente Social	Análise da Conjuntura Política e Econômica Nacional e Internacional
		Fornecedores	Controles de Serviços Terceirizados
			Planos de Contingência
		Clientes	Controles de Acesso Lógico
		Meio Ambiente	Valores Éticos e Normas de Conduta da Empresa
Risco de Imagem			Valores Éticos e Normas de Conduta da Empresa
			Normas e Procedimentos
			Controles de Serviços Terceirizados
			Pesquisa de Satisfação
			Canais de Comunicação com a Sociedade
			Canais de Comunicação com os Servidores

Fonte: Brasil (2017).

De acordo com a Estrutura COSO (2012), as atividades de controle devem ser alicerçadas em três princípios:

i) Seleção e desenvolvimento de atividades de controle que auxiliem a redução de riscos;

ii) Seleção e desenvolvimento de atividades de controle gerais para a consecução dos objetivos;

iii) Implementação de atividades de controle através de políticas associadas às expectativas e aos procedimentos que viabilizam sua execução.

2.4. Informação e Comunicação

A qualidade das informações transmitidas no contexto organizacional compõe a base para que os controles e objetivos sejam pensados, assim como a comunicação desses elementos para todos os indivíduos envolvidos no negócio – seja interna, seja externa – é fundamental para que haja uma cultura de conscientização e responsabilização (COSO, 2012).

Nesse sentido, todos os atores organizacionais – diretores, funcionários, servidores, etc – devem prezar por informações tempestivas, consistentes e acessíveis, armazenando-as e comunicando-as dentro de períodos razoáveis ao cumprimento das funções e das atividades de controle interno. A clareza da comunicação, especialmente por parte da alta administração aos demais funcionários, no que tange à efetivação dos controles internos, é parte basilar para a eficácia desses controles (Brasil, 2016).

De acordo com a Estrutura COSO (2012), a informação e a comunicação devem ser alicerçadas em três princípios:

i) Obtenção e geração de informações fidedignas de apoio aos controles;

ii) Comunicação interna dos objetivos e responsabilidades associadas ao desempenho dos controles internos;

iii) Comunicação externa com todos os envolvidos em assuntos relacionados ao funcionamento dos controles internos.

a) Atividades de monitoramento

O monitoramento dos controles internos deve ocorrer continuamente ou através de revisões específicas, de modo a averiguar se todos os componentes aqui mencionados estão presentes de forma eficaz e baseada em seus respectivos princípios norteadores. Tal acompanhamento torna possível o diagnóstico de falhas nas práticas organizacionais e a necessidade de ajustes nos controles para que eles se mantenham apropriados (Vieira; Barreto, 2019).

O monitoramento contínuo é voltado às atividades cotidianas da organização, as quais são desenvolvidas sob a responsabilidade de cada funcionário ou servidor, abrangendo toda a estrutura de controles internos no combate aos atos fraudulentos, antiéticos e ineficientes. O monitoramento por meio de avaliações específicas é voltado aos casos menos frequentes, decorrentes da avaliação de riscos e do próprio monitoramento contínuo, abrangendo também as avaliações de auditorias internas acerca da eficácia dos controles (Brasil, 2016).

De acordo com a Estrutura COSO (2012), as atividades de monitoramento devem ser alicerçadas em dois princípios:

i) Desenvolvimento de avaliações contínuas e pontuais para certificar o funcionamento e a abrangência dos controles internos;

ii) Diagnóstico e comunicação tempestiva das falhas nos controles internos aos responsáveis pelas correções.

Desse modo, as organizações devem prover meios para que os componentes apresentados existam e funcionem de forma adequada, contribuindo para uma dinâmica de controles internos confiável e que suporta o processo decisório de forma consistente.

3. Nível de maturidade dos Controles Internos

Embora a importância dos controles internos não seja uma novidade no contexto da gestão empresarial, deve-se considerar que a maturidade desses controles – refletida, principalmente, na capacidade que o negócio apresenta de gerenciar seus riscos e de assegurar práticas de conformidade e de integridade – e o desenvolvimento dos seus componentes podem variar de acordo com as características de cada organização.

Assim, avaliação do nível de maturidade dos controles internos é fundamental para garantir a eficácia e a confiabilidade dos processos organizacionais. De acordo com Assi (2021), essa avaliação pode ser fundamentada em cinco níveis:

i) Não confiável: não há um mapeamento das atividades de controle.

ii) Informal: os controles existem, mas dependem essencialmente das pessoas para serem executados.

iii) Padronizado: há um mapeamento das atividades de controle e elas são implementadas no negócio.

iv) Monitorado: há uma padronização dos controles internos e testes periódicos são realizados.

v) Otimizado: as atividades de controle são executadas com auxílio de ferramentas de apoio e automações.

Em determinados casos, as perspectivas de avanços nos níveis de maturidade dos controles internos podem ser avaliadas em função dos custos envolvidos nesse processo, os quais podem incluir:

- Recrutamento e retenção de profissionais competentes e qualificados para a implantação e manutenção dos controles, fato que pode exigir maiores remunerações;
- Esforços de seleção, desenvolvimento, execução, incremento e atualização das atividades de controle;

- Esforços de seleção, desenvolvimento, manutenção e atualização associados à dependência tecnológica, em diferentes proporções;
- Investimentos voltados ao processamento de dados e aos sistemas de informação que viabilizem fluxos de informações tempestivas e adequadas às partes interessadas (COSO, 2012).

De modo geral, trata-se de uma avaliação básica, mas que pode orientar os responsáveis pela implementação de controles internos na identificação das necessidades de melhorias, na redução de vulnerabilidades e no fortalecimento de ações contra ameaças internas e externas, objetivando uma abrangência de controles adequada à realidade do negócio.

3.1. Desafios associados aos Controles Internos

A implementação e efetividade dos controles internos passam por diversos desafios no contexto corporativo, especialmente no tocante à complexidade das legislações. Um marco legal decisivo na temática de controles internos, segundo Assi (2021), foi a Lei Sarbanes-Oxley (SOX), criada para restaurar a confiabilidade do mercado de capitais após uma série de escândalos financeiros ocorridos nos Estados Unidos em meados de 2002, a qual instituiu que a conduta ética e as práticas de governança corporativa deixariam de ser apenas desejáveis e passariam a ser leis, privilegiando o controle interno como contribuição para sua efetividade.

Uma das exigências mais conhecidas e polêmicas da SOX está em sua seção 404, a qual obriga as organizações a apresentarem relatórios de suas demonstrações financeiras e dos controles internos associados a essas informações, além de apresentarem uma avaliação rigorosa desses controles, através de auditorias internas e externas. Logo, a adequação à SOX trata-se de um investimento milionário que vai desde a realização de um bom diagnóstico de fragilidades e de necessidades de controles até adequações tecnológicas, consultorias especializadas e auditorias (Assi, 2021).

Os impactos da lei exemplificada puderam ser vistos no Brasil, pois as organizações brasileiras que possuíam ações negociadas na bolsa de valores dos Estados Unidos precisaram se adaptar à legislação e aos padrões contábeis e de governança internacionais (Assi, 2021). Soma-se a isso a vasta gama de leis, regulamentos e normas existentes no país, que atingem diferentes aspectos estratégicos e operacionais dos negócios – como questões trabalhistas, tributárias, contábeis e ambientais – e requerem a constante vigilância dos gestores para manter seus controles internos alinhados com as últimas exigências legais.

Outro desafio emerge da realidade contemporânea, fundamentada em constantes avanços tecnológicos, na qual os processos administrativos e operacionais encontram-se permeados pelas inúmeras inovações decorrentes desse cenário e, consequentemente, pela necessidade de iniciativas de gestão do conhecimento, controle e segurança dos intensos fluxos de informações (Assi, 2021).

De fato, as inovações tecnológicas podem ser fontes de oportunidades, mas também de novos riscos, pois interferem – em diferentes graus de complexidade e de abrangência – na forma como as organizações implementam seus controles internos, envolvendo aspectos como a integração e a descentralização de sistemas, o processamento e o compartilhamento de informações em tempo real para tomada de decisões, a comunicação tempestiva de informações para todos os sujeitos inseridos no negócio e parceiros externos, dentre outros (COSO, 2012).

Além disso, como as tecnologias são, predominantemente, manipuladas pelos indivíduos, existem limitações no que tange à efetividade absoluta dos controles internos, pois esses controles podem ser contornados por decisões equivocadas, por falhas humanas, ou até mesmo pela capacidade que todos os envolvidos em um negócio podem ter de agir de forma corrupta (COSO, 2012).

Nesse sentido, outro desafio se sobressai: a questão cultural da organização. Diversas falhas no cotidiano, sejam elas de integridade ou operacionais, guardam relação com resistências a mudanças, as quais são mascaradas por sentenças como "Nós sempre fizemos dessa forma" ou "Aprendi assim, para quê mudar agora?".

Sob uma perspectiva individual, os sujeitos podem resistir às mudanças nos controles por medo, por insegurança, por dificuldades em reconhecer os benefícios dos novos hábitos e por enxergarem ameaças ao seu comodismo. Sob uma perspectiva organizacional, há receios associados aos conflitos de interesses, à necessidade de comprometimento dos departamentos, às ameaças aos vínculos de poder estabelecidos e aos traumas decorrentes de controles anteriores que não obtiveram êxito (Assi, 2021).

Entretanto, os gestores e o conselho de administração possuem um papel crucial no aculturamento de toda a organização, atuando através de políticas e do próprio exemplo prático no enfrentamento das barreiras cotidianas, fato que os aproxima de garantir que o negócio cumpre as regulamentações exigidas, socializa relatórios esclarecedores de prestação de contas, gerencia suas operações com base nos padrões internos e atinge seus objetivos operacionais em conformidade com as legislações (COSO, 2012). Além disso, os incentivos,

treinamentos e as práticas anteriormente apresentadas nesse material – como o monitoramento, a gestão de riscos e de *Compliance* – são elementos indispensáveis para lidar com os desafios de forma estratégica e resolutiva.

4. Considerações adicionais sobre Controles Internos

Compreendendo a importância dos controles internos para a sustentabilidade dos mais diversos tipos de negócio, convém pontuar que as abordagens de implementação desses controles se adequam a organizações de diferentes dimensões. Nessa conjuntura, de acordo com a estrutura COSO (2012), alguns elementos da dinâmica dos controles internos podem apresentar variações entre grandes e pequenas organizações, tais como:

- **Responsabilidade pela supervisão dos controles**: Enquanto grandes corporações ou empresas públicas possuem agências reguladoras ou órgãos governamentais que podem supervisionar seus controles, organizações menores e menos complexas podem contar com seus diretores para realizar a mesma função.
- **Interação e comunicação com pessoal**: Enquanto grandes corporações ou empresas públicas possuem a necessidade de mecanismos cada vez mais abrangentes de comunicação – como portais online, relatórios periódicos formais e reuniões periódicas entre departamentos – para alinhar questões relevantes ao desempenho operacional, organizações menores tendem a possuir maiores possibilidades de interação direta com o pessoal de diferentes níveis hierárquicos, assim como podem, de forma eficaz, contar com reuniões informais de pessoal para alinhar assuntos da mesma natureza.
- **Economia de escala**: Grandes corporações ou empresas públicas podem se beneficiar de economias de escala, não só para a aquisição de insumos, mas também para determinadas funções de apoio, como a implantação da função de auditoria interna através de contratação ou de pessoal interno já experiente. Já as organizações menores, considerando o mesmo cenário, tendem a não implementar essa função ou a dispender um alto percentual de recursos para isso, recorrendo, por vezes, a terceirizações.
- **Nível de documentações dos controles internos**: As documentações referentes aos controles internos – como manuais, políticas, fluxograma de processos, organogramas, descrições de cargos e salários, etc – devem existir de forma proporcional às necessidades e circunstâncias da organização. Grandes corporações ou empresas públicas, geralmente, possuem um sistema mais extenso e complexo de controles internos, fato que acarreta em documentações mais extensas, enquanto que empresas menores,

por vezes, contam com interações e comunicações mais estreitas, ou até mesmo com controles atuantes por meio da observação direta, cenário que exige um menor volume de documentações formais entre os níveis de gestão para garantir que os componentes dos controles internos estejam em funcionamento.

Desse modo, entende-se que as particularidades de cada organização não devem ser fatores limitantes à implementação de controles internos, sendo esta uma recomendação ampla no mundo dos negócios. Cabe às organizações uma análise de seus recursos – humanos e de capital – para conhecer seus limites e considerar as alternativas mais benéficas à administração e manutenção desses controles.

Síntese do Capítulo

No quarto capítulo, encerramos mais uma parte do nosso ciclo de aprendizado, imergindo na temática dos controles internos. Nele pudemos conhecer o que são esses controles e seus principais benefícios no funcionamento das organizações, ressaltando seu papel efetivo nas práticas de *Compliance,* pois auxilia a identificação, prevenção e correção de fraudes e inconformidades. Em seguida, vimos que existe um modelo estrutural de controles internos aplicável aos mais diversos tipos de organizações, composto por cinco elementos que podem ser periodicamente analisados, como forma de fiscalizar e garantir a eficácia e a abrangência dos controles internos. Fomos apresentados também à importância de refletirmos, honestamente, sobre os níveis de maturidade dos controles, que podem, naturalmente, variar de acordo com as necessidades organizacionais. Ademais, foram explicitados os desafios associados aos controles internos, que vão desde a complexidade das regulamentações, às transformações tecnológicas e aspectos culturais que devem ser contornados com incentivos, treinamentos e práticas favoráveis à adesão de toda a organização. Por fim, constatamos que, embora as instituições apresentem particularidades e significativas diferenças entre si, os controles internos são aplicáveis a todas elas, cabendo aos responsáveis por sua implantação analisar os aspectos que necessitam de adequação para que esses controles funcionem da forma mais eficaz possível.

Atividades de avaliação

1. O que são controles internos e por que são importantes para as organizações? Como eles se relacionam com as práticas de *Compliance*?
2. Quais são os componentes essenciais dos controles internos? Escolha um deles e discorra sobre a sua importância para o contexto organizacional.
3. Dentre os cinco níveis de maturidade dos controles internos, o quinto lança luz sobre um importante elemento: a tecnologia. Elabore e explique as possíveis relações entre a atuação dos controles internos e as crescentes inovações tecnológicas.
4. Quais os três principais desafios associados aos controles internos? Escolha um deles e explique como esse desafio pode ser enfrentado para a consolidação de controles internos efetivos.

Leituras, filmes e sites

Filme

- "Hacker" (ou "*Blackhat*"): o filme aborda como hackers podem explorar vulnerabilidades em sistemas de computador e redes para realizar ataques cibernéticos, afetando empresas, governos e indivíduos em todo o mundo. Nesse sentido, embora o filme não trate especificamente de controles internos, nele são exploradas questões éticas sobre o uso da tecnologia e a necessidade de cada vez mais responsabilidades associadas à vigilância e proteção de dados, oportunizando reflexões sobre como o controle interno pode atuar no combate a cenários como esse.

Livros

- Gestão de Riscos com Controles Internos: Ferramentas, Certificações e Métodos para garantir a eficácia empresarial. De autoria de Claudio Dias Lopes, o livro aborda diversos aspectos e aplicações práticas relacionadas à gestão de riscos e controles internos nas organizações, com destaque para os componentes do COSO, mencionados nesse material, e suas aplicações.
- Controles Internos e Cultura Organizacional: Como consolidar a confiança na gestão. De autoria de Sandro Jeger, o livro aborda como os controles internos e a cultura organizacional podem, de forma abrangente e prática,

trabalhar juntos para que os controles sejam implementados de forma eficaz, fortalecendo a confiança na gestão e promovendo a sustentabilidade das empresas.

Referências

ABNT. Associação Brasileira de Normas Técnicas. **ABNT NBR ISO 37301:2021 Sistemas de gestão de** *Compliance* – Requisitos com orientações para uso. Rio de Janeiro: ABNT, 2021.

ABREU, F. C. L. C.; URNIKES, I. C. Antitruste e Anticorrupção: como incentivar a adoção de programas de *Compliance* por empresas privadas? In: LAMACHIA, C.; PETRARCA, C. (org.). *Compliance*: essência e efetividade. Brasília: OAB, Conselho Federal, 2018. p. 89-99.

ANDRADE, R. C. *Compliance* **como realizador do ESG**: construção dos pilares com foco no ambiental. São Paulo: Dialética, 2024.

ABNT. Associação Brasileira de Normas Técnicas. **ABNT NBR ISO 31000:2018** Gestão de Riscos: Princípios e Diretrizes. Rio de Janeiro: ABNT, 2018.

ASSI, M. **Gestão de Riscos com Controles Internos** - Ferramentas, Certificações e Métodos Para Garantir a Eficiência dos Negócios. 2. ed. São Paulo: Saint Paul, 2021.

ASSI, M. *Compliance***, como implementar**. São Paulo: Trevisan Editora, 2018

ATTIE, W. **Auditoria**: conceitos e aplicações. 7. ed. São Paulo: Atlas, 2018.

BERSTEIN, P. L. **Desafio aos deuses**: a fascinante história do risco. 23. ed. Rio de Janeiro: Gulf Professional Publishing, 1997.

BITTENCOURT, S. **Comentários à Lei Anticorrupção**: Lei 12.846/2013. São Paulo: Editora Revista dos Tribunais, 2014. p. 112

BLOK, M. *Compliance* **e Governança Corporativa**. 4ª edição. Rio de Janeiro: Freitas Bastos, 2023.

BOLSONELLO, J.; SILVA; M. T. B.; LARA, A. M. B.; MACUCH, R. S. Uso de brainstorming como ferramenta para aprendizagem. **Conhecimento & Diversidade**, Niterói, v. 15, n. 36, Jan/Mar. 2023.

BRASIL. Ministério da Justiça e Segurança Pública. **Manual de gerenciamento de riscos e controles internos**. Brasília, DF: Ministério da Justiça e Segurança Pública, 2020. Disponível em: https://www.gov.br/mj/pt-br/acesso-a-informacao/governanca/Gestao-de-Riscos/biblioteca/Manual/manual-de-gerenciamento-de-riscos-mjsp-2021.pdf. Acesso em: 11 mar. 2024.

BRASIL. Controladoria-Geral da União. **Metodologia de Gestão de Riscos**. Brasília, DF: CGU, 2018. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/outros-documentos-externos/cgu_metodologia_gestao_riscos.pdf. Acesso em: 28 fev. 2024.

CANDELORO, A. P. P. *Compliance* - inovação estratégica para a sustentabilidade das organizações. **Revista RI - Relações com Investidores**, São Paulo, v. 187, 01 out. 2014.

CANDELORO, A. P. P.; BENEVIDES, M. M. Os 9 passos essenciais para fortalecer o *Compliance* e a Governança Corporativa nas empresas. **Harvard Business Review Brasil**, v. 1, p. 75-80, 2013.

COSO – Committee Of Sponsoring Organizations Of The Treadway Commission. **Internal Control — Integrated Framework**, 2012. Disponível em: https://ce.jalisco.gob.mx/sites/ce.jalisco.gob.mx/files/coso_mejoras_al_control_interno.pdf. Acesso em: 3 abr. 2024.

CRUVINEL, G. A.; RIBEIRO, A. E. S.; OLIVEIRA, A. R. **Controle Interno na Gestão Pública Municipal**. 2022. Disponível em: https://conaci.org.br/noticias/controle-interno-na-gestao-publica-municipal/. Acesso em: 25 mar. 2024.

DELOITTE. **Integridade Corporativa no Brasil**: evolução do *Compliance* e das boas práticas empresariais nos últimos anos. 2022.Disponível em: https://pesquisas.lp.deloittecomunicacao.com.br/Integridade-corporativa-2022. Acesso em: 28 mar. 2024.

DAMODARAN, A. **Gestão estratégica do risco**: uma referência para a tomada de riscos empresariais. Porto Alegre: Bookman, 2009.

EXAME. **Wells Fargo pagará US$ 185 mi de multa por contas falsas.** 2016. Disponível em: https://exame.com/negocios/wells-fargo-pagara-us-185-mi-de-multa-por-contas-falsas/. Acesso em: 28 mar. 2024.

FAÇANHA, M. C.; LIMA, F. A. P.; Luca, M. M. M.; VASCONCELOS, A. C. Gerenciamento de riscos e gestão de controles internos em empresas brasileiras envolvidas em crimes de corrupção e lavagem de dinheiro. **Revista Contemporânea de Contabilidade**, v. 17, n. 43, p. 34–50, 2020.

FARIAS, T. A.; Salim, P. H.; Santos, R. R. S. Aversão ao risco e resposta comportamental: uma exploração histórico-econômica. **Revista de Estudos Sociais**, v. 22, n. 45, 2021.

GITMAN, L. J. **Princípios de Administração Financeira**. 12. ed. São Paulo: Pearson, 2010.

IBGC – Instituto Brasileiro de Governança Corporativa. **Guia de orientação para o gerenciamento de riscos corporativos**. São Paulo, SP: IBGC, 2007.

IBGC – Instituto Brasileiro de Governança Corporativa. **Gerenciamento de riscos corporativos**: evolução em governança e estratégia. São Paulo, SP: IBGC, 2017.

ITI – Instituto Nacional de Tecnologia da Informação. **Programa de Integridade e** *Compliance*. Brasília: ITI, 2018. Disponível em: https://www.gov.br/iti/pt-br/acesso-a-informacao/institucional/Programa_de_Integridade_e_*Compliance*___Assinado_1.pdf. Acesso em: 15 mar. 2024.

MENDONÇA, G. M. F. A relação entre segurança jurídica e *Compliance* para a retomada do crescimento econômico. In: Lamachia, C.; Petrarca, C. (org.). *Compliance*: essência e efetividade. Brasília: OAB, Conselho Federal, 2018. p. 23-28.

ROCHA, C. O. L. Programa de *Compliance* nas Empresas Estatais. In: Lamachia, C.; Petrarca, C. (org.). *Compliance*: essência e efetividade. Brasília: OAB, Conselho Federal, 2018. p. 117-125.

SOUZA, F. N. C. L. Implementação de um programa de *Compliance*. In: Lamachia, C.; Petrarca, C. (org.). *Compliance*: essência e efetividade. Brasília: OAB, Conselho Federal, 2018. p. 209-214.

VIEIRA, J. B.; BARRETO, R. T. S. **Governança, gestão de riscos e integridade**. Brasília: Enap, 2019. 240 p.

Sobre a autora

Ana Raquel Silva Rocha Sudério: possui graduação em Administração pela Universidade Estadual do Ceará (2018), especialização em Administração Financeira pela Universidade Estadual do Ceará (2020), mestrado em Administração pelo Programa de Pós-Graduação em Administração da Universidade Estadual do Ceará (2022) e atualmente é doutoranda em Administração no mesmo programa. Membro do grupo de pesquisas Integra Saberes sobre trabalho, organizações e gestão, desde 2016, onde orienta e desenvolve pesquisas na área de Gestão e Estudos Organizacionais, com ênfase nos seguintes temas: Startups, Psicodinâmica do Trabalho e Gestão Financeira. Atualmente mantém vínculo temporário como docente na Universidade Estadual do Ceará, onde orienta trabalhos acadêmicos dos alunos do curso de Administração, especialmente situados no setor de estudos quantitativos, que abrange as áreas de gestão financeira, contabilidade e economia.

Especialização em
Auditoria e Controle interno

Fiel a sua missão de interiorizar o ensino superior no estado Ceará, a Uece, como uma instituição que participa do Sistema Universidade Aberta do Brasil, vem ampliando a oferta de cursos de graduação e pós-graduação na modalidade de educação a distância e gerando experiências e possibilidades inovadoras com uso das novas plataformas tecnológicas decorrentes da popularização da internet, do funcionamento do cinturão digital e da massificação dos computadores pessoais.

Comprometida com a formação de professores em todos os níveis e a qualificação dos servidores públicos para bem servir ao Estado, os cursos da UAB/Uece atendem aos padrões de qualidade estabelecidos pelos normativos legais do Governo Federal e se articulam com as demandas de desenvolvimento das regiões do Ceará.

UECE

UAB UNIVERSIDADE ABERTA DO BRASIL

CAPES