19

Instituto Brasileiro de Governança Corporativa

Cadernos de Governança Corporativa

# Gerenciamento de Riscos Corporativos

## Evolução em Governança e Estratégia

IBGC | Instituto Brasileiro de Governança Corporativa

# Gerenciamento de Riscos Corporativos

## Evolução em Governança e Estratégia

IBGC | Instituto Brasileiro de Governança Corporativa

2017

## Instituto Brasileiro de Governança Corporativa

O IBGC é uma organização exclusivamente dedicada à promoção da governança corporativa no Brasil e o principal fomentador das práticas e discussões sobre o tema no país, tendo alcançado reconhecimento nacional e internacional.

Fundado em 27 de novembro de 1995, o IBGC – sociedade civil de âmbito nacional, sem fins lucrativos – tem o propósito de ser referência em governança corporativa, contribuindo para o desempenho sustentável das organizações e influenciando os agentes da nossa sociedade no sentido de maior transparência, justiça e responsabilidade.



Para mais informações sobre o Instituto Brasileiro de Governança Corporativa, visite o *website* <www.ibgc.org.br>.
Para associar-se ao IBGC, ligue: (11) 3185-4200.

I59g Instituto Brasileiro de Governança Corporativa
Gerenciamento de riscos corporativos: evolução em governança e estratégia / Instituto Brasileiro de Governança Corporativa. São Paulo, SP: IBGC, 2017. (Série Cadernos de Governança Corporativa, 19).
64p.

ISBN: 978-85-99645-50-5

1. Governança corporativa. 2. Conselho de administração. 3. Risco. 4. Gestão. I. Título.

CDD – 658.4

Bibliotecária responsável: Mariusa F. M. Loução – CRB-12/330

# Créditos

Esta publicação é resultado de projeto desenvolvido e executado pela Comissão de Gerenciamento de Riscos Corporativos do IBGC. Seu conteúdo não reflete, necessariamente, as opiniões individuais daqueles que participaram de sua elaboração, e sim o entendimento do instituto. Durante sua elaboração, este documento passou por processo intenso de discussões internas e audiência pública, tendo recebido diversas contribuições e sugestões.

## Coordenação geral

Mercedes Marina Stinco.

## Coordenação dos Grupos Redatores e de Revisão

Alex Lelis Buzato Borges, Érico Torres, Luciana Bacci, Ricardo Lemos e Roberto Lamb.

## Membros da Comissão

Alberto Whitaker, Alberto Yamandú Messano Colucci, Alessandra Silva de Jesus Artifon, Alex Lelis Buzato Borges, André Coutinho, André Echeverria, André Vitoria, Antônio Cocurullo, Antonio Edson Maciel dos Santos, Antônio Lemos, Antonio M. F. Ribeiro, Arnaldo Bonoldi Dutra, Carlos Sá, Clara R. F. Biscar, Clovis Corrêa da Costa, Érico Torres, Erlon Lisboa de Jesus, Fábio Coimbra, Fábio Mendes, Fernando Nicolau Freitas Ferreira, Flavio Abrão, Francisco Carlos Fernandes, Frederico de Campos Ventriglia, Ivana Regina Galvão Leite, Ives Pereira Müller, João Francisco Arcoverde Lopez, Leandro Pavão, Leonardo Machado, Lucia Casasanta, Luciana Bacci, Marcelo Lerch Hoffmann, Marco Antonio Bueno, Marcos Lorençani, Marcus Lanzelotti, Maria Paula Aranha, Marilza Benevides, Mario Augusto Filipini, Mercedes Marina Stinco (coord.), Mirian Paula Ferreira Rodrigues, Paulo Baraldi, Pedro Antônio Maziero, Rainer Lutke, Ricardo Aparecido dos Santos, Ricardo Lemos, Ricardo Roschel, Roberto Lamb, Roberto Sobral Hollander, Sandra Cristina Bernardo, Silvio Valdrighi e Tatiana Leite.

## Contribuições e Agradecimentos Especiais


À equipe do IBGC, pelo apoio à comissão e pelas contribuições ao documento.

A Lucas Legnare e Luciana Del Caro, pelo suporte no processo de redação do caderno.

A Carlos Eduardo Lessa Brandão, José Luiz Bichuetti e Sergio Moreno, pelos comentários e pela participação em banca que avaliou a publicação.

A Annibal Ribeiro Lima, Camila Sardenberg, Cida Hess, Clara Regina Ferrão Biscar, Edina Biava, José Martins, José Ricardo De Moraes Pinto, Leila de Oliveira Lopes Rega, Leonardo Viegas, Luiz Alberto de Castro Falleiros, Luiz Athayde, Maurício Loures Rodrigues, Roberta Simonetti, Tatiana de Oliveira Leite e Thomas Brull, pela participação em fórum restrito que debateu o conteúdo do documento.

A Alexandre de Oliveira, Carlos Antonio Vergara Cammas, Diego Silveira Maciel, Felipe A. F. Gomes, Isabella Saboya, Sergio Mastrangelo Ferreira, Vladimir Barcellos Bidniuk e William Borges Lima, pelas contribuições enviadas ao longo do processo de audiência pública.

A Francisco Fernandes, João Francisco Arcoverde Lopez, Maria Paula Aranha, Marilza Benevides e Silvio Valdrighi pelas contribuições geradas na produção dos textos.

A Ricardo Lemos, pela consolidação e revisão das diversas versões geradas pelos grupos redatores.

A Roberto Lamb, pela inestimável e relevante contribuição ao longo de todas as etapas de construção do caderno, tornando o texto o mais rico e atual possível.

# Sumário

# Apresentação

Desde 1999, com o lançamento da primeira edição do *Código das Melhores Práticas de Governança Corporativa*, o IBGC passou a publicar documentos específicos no âmbito das boas práticas de governança corporativa.

A presente publicação, **Gerenciamento de Riscos Corporativos: Evolução em Governança e Estratégia**, integra a série de publicações denominada Cadernos de Governança Corporativa, cujo objetivo é trazer ao mercado informações práticas que contribuam para o processo da governança corporativa.

Os Cadernos de Governança do IBGC são editados, de acordo com seu conteúdo, em três séries: Documentos Legais de Governança, Documentos sobre Estruturas e Processos de Governança e Temas Especiais de Governança. Trazem contribuições, sugestões e recomendações elaboradas pelos associados do IBGC que integram suas diversas comissões de trabalho.

Integrante dos Temas Especiais de Governança, este caderno versa sobre como os administradores, com destaque especial para os conselheiros de administração, podem desenvolver um modelo eficiente de implementação de gerenciamento de riscos a partir dos princípios da boa governança corporativa.

O caderno apresenta de maneira instrutiva os papéis dos principais agentes de governança e algumas das principais práticas recomendadas, trazendo subsídios para a implementação de estrutura de gerenciamento de riscos que dialogue com a estratégia de longo prazo estabelecida pela organização.

Com essa publicação, o IBGC espera contribuir para que as incertezas que acompanham os riscos sejam administradas de forma adequada, garantindo que os administradores estejam mais bem preparados para uma tomada de decisão refletida e equilibrada.

# Prefácio

Esta obra se propõe a trazer reflexões e orientações para executivos e, sobretudo, conselheiros de administração interessados em implantar ou aprimorar o modelo de gerenciamento de riscos corporativos (GRCorp) das organizações em que trabalham. O documento tem o propósito de servir a organizações em diferentes estágios de maturidade de GRCorp.

Se o foco do primeiro caderno do IBGC sobre gerenciamento de riscos[1] era na metodologia do tratamento de riscos, esta publicação dá destaque à governança e à estratégia do GRCorp, ou seja, à estrutura organizacional por meio da qual o gerenciamento de riscos é concebido e operacionalizado. A finalidade do texto, portanto não é ser exaustivo em relação a técnicas de gerenciamento de riscos. Muitos manuais que tratam desse tema podem ser encontrados no mercado, e alguns são citados nas referências bibliográficas no fim deste material. Optou-se, aqui, por apresentar apenas conceitos essenciais para que executivos e conselheiros possam compreender a importância de seu papel na implementação e na coordenação, supervisão e fiscalização de uma estrutura sólida e consistente de gerenciamento de riscos.

A gestão de riscos vem se tornando mais importante no dia a dia das empresas não só como uma forma de reação a fracassos corporativos que poderiam ter sido evitados por um gerenciamento adequado, mas pela sua importância estratégica. As informações levantadas pelo GRCorp são parte integrante do processo de tomada de decisões empresariais, da proteção de ativos e do processo de criação de valor, o que ressalta a importância de que essa estrutura seja dotada de uma governança adequada.

O IBGC acredita que as considerações e sugestões aqui contidas contribuirão para o aperfeiçoamento da governança corporativa, já que o GRCorp é um valioso instrumento de administração e governança e atua em prol do desenvolvimento sustentável das organizações, beneficiando todas as partes interessadas.

Para a concepção deste caderno, foram levadas em conta as discussões e análises feitas pela Comissão de Riscos do IBGC ao longo dos anos, desde a primeira edição do documento (2007),

1. *IBGC,* Guia de Orientação para Gerenciamento de Riscos Corporativos*, 2007. Vale lembrar que a Comissão de Riscos do IBGC já desenvolveu outras publicações sobre o tema com a série Estudos de Caso, a saber:* Visão Evolutiva do Modelo de Gestão de Riscos: Vale e Natura Cosméticos*, 2008;* Gestão Integrada de Riscos: Banco Real e Brasil Telecom*, 2008; e* Gestão de Riscos como Instrumento para a Tomada de Decisão: Votorantim Ceculose e Papel (VCP)*, 2008.*

as experiências de projetos e de implementações de gestão de riscos em empresas de diversos setores e diferentes estágios de maturidade no processo de gestão de riscos. Também foram levadas em conta as boas práticas de GRCorp disseminadas por organizações e institutos independentes, internacionais ou nacionais, associações de indústria ou profissionais, bem como organismos de normatização e entidades reguladoras.

No momento da conclusão desta publicação, encontrava-se em estágio de desenvolvimento a revisão da norma ISO 31.000: *General Guidelines for Principles and Implementation of Risk Management*, bem como o Coso ERM (*Enterprise Risk Management – Aligning Risk with Strategy and Performance*). Este último, especificamente, explora como o GRCorp deve estar integrado ao planejamento estratégico das organizações, uma vez que a estratatégia influencia seu desenvolvimento. Uma empresa que integra GrCorp em seu planejamento estratégico proporciona à administração informações de riscos que precisam ser consideradas nas alterativas estratégicas e nas suas escolhas.

Assim como o IBGC, essas organizações (ISO e Coso) perceberam a complexidade a que as organizações estão sujeitas, as mudanças ocorridas ao longo do tempo e o surgimento de novos riscos. Portanto, torna-se crucial o reforço e a consciência de gerenciamento riscos corporativos nos conselhos de administração.

Na expectativa de que o material seja útil e dê bons frutos, desejamos uma boa leitura.

# Introdução

Na vida cotidiana de indivíduos e organizações, raramente se leva em conta que quase todos os atos e atividades implicam riscos. A palavra risco é proveniente do latim *risicum* ou *riscum*, cuja definição envolve o conceito de ousar – *riscare*. Assim, qualquer ação ou empreendimento traz alguma dose de risco. "Viver é muito perigoso", dizia o personagem Riobaldo na obra *Grande Sertão: Veredas*, de Guimarães Rosa.

As organizações deparam-se cada vez mais com temas como sustentabilidade, corrupção, fraude, abusos nos incentivos de curto prazo para executivos e investidores, ética nos negócios e reputação. Cada um destes temas traz embutidos em si a noção de risco, cujo gerenciamento é parte do que as organizações precisam para obter lucros, realizar objetivos importantes (sociais, ambientais, etc.), criar valor, e, principalmente, ter uma existência longeva.

Costuma-se entender risco como possibilidade de algo não dar certo. Mas seu conceito atual no mundo corporativo vai além: envolve a quantificação e a qualificação da incerteza[2], tanto no que diz respeito às perdas quanto aos ganhos por indivíduos ou organizações. Sendo o risco inerente a qualquer atividade – e impossível de eliminar –, a sua administração é um elemento-chave para a sobrevivência das companhias e demais entidades.

É dessa forma que as atividades de gerenciamento de riscos corporativos (GRCorp) devem ser encaradas. Elas precisam contribuir para a longevidade da organização e para a consecução de seus objetivos estatutários e estratégicos. Para que isso se torne possível, é necessário que as organizações disponham de uma estrutura de gerenciamento de riscos e de governança corporativa, ainda que mínima em organizações menos maduras e de menor capacidade financeira. Esta publicação visa orientar os conselheiros e executivos tanto para a implantação de um modelo de GRCorp quanto para o fortalecimento dos modelos existentes. Dadas as particularidades e os diferentes estágios de desenvolvimento de cada organização, as recomendações e sugestões contidas neste documento devem ser analisadas diante da realidade e do momento de cada uma.

2. *Risco: evento futuro identificado, ao qual é possível associar uma distribuição de probabilidades de ocorrência. Incerteza: evento futuro identificado, ao qual não é possível associar uma distribuição de probabilidades de ocorrência. Ignorância: eventos futuros que, no momento da análise, não poderão sequer ser identificados, muito menos quantificados (exemplo: eventos decorrentes de sistemas complexos como o climático – as consequências do aquecimento global são imprevisíveis). M. Faber, R. Manstetten e J. Proops,* Ecological Economics: Concepts and Methods*, 1996, pp. 209-211.*

De acordo com a 5ª edição do *Código das Melhores Práticas de Governança Corporativa* do IBGC: "Os riscos a que a organização está sujeita devem ser gerenciados para subsidiar a tomada de decisão [...]. Os agentes de governança têm responsabilidade em assegurar que toda a organização esteja em conformidade com os seus princípios e valores, refletidos em políticas, procedimentos e normas internas, e com as leis e os dispositivos regulatórios a que esteja submetida"[3].

O código do IBGC orienta que os conselheiros possuam conhecimento sobre o tema, para que possam efetivamente identificar, priorizar e garantir a gestão eficaz da exposição da organização aos diversos riscos relacionados ao seu negócio. O conselho de administração deve adotar uma atitude proativa, requerendo informações baseadas no modelo de GRCorp. Isto se tornará possível à medida que os conselheiros consigam avaliar os modelos, estruturas, processos, ferramentas e indicadores utilizados.

Este caderno divide-se em três capítulos. No primeiro, são tratados os conceitos básicos sobre GRCorp, sua importância e como a gestão de riscos se alinha às estratégias empresariais. No Capítulo 2, enfocam-se as atribuições dos vários agentes da governança corporativa, com ênfase no papel do conselho de administração a partir da ótica dos processos decisórios, das responsabilidades e dos direcionadores de riscos. Por fim, o Capítulo 3 traz subsídios para a implementação de uma estrutura de GRCorp adequada ao tamanho e à complexidade da organização e que respeite o estágio de maturidade do negócio e a estratégia de longo prazo de sua administração, apresentando as principais práticas recomendadas. O caderno traz, ainda, anexos com informações adicionais.

*3. IBGC,* Código das Melhores Práticas de Governança Corporativa*, 2015, p. 91.*

1

# Definições e Bases

# 1. Definições e Bases

## 1.1 Conceitos de gerenciamento de riscos corporativos

Dado que o risco é inerente a qualquer atividade empresarial, cabe às empresas o gerenciarem com vistas a assumir riscos calculados, reduzir a volatilidade dos seus resultados e aumentar a previsibilidade de suas atividades e se tornar mais resilientes em cenários extremos. A eficácia no seu gerenciamento pode afetar diretamente os objetivos estratégicos e estatutários estabelecidos pela administração – e, em última análise, impacta a longevidade da organização.

O gerenciamento de riscos corporativos (GRCorp) pode ser entendido como um sistema intrínseco ao planejamento estratégico de negócios, composto por processos contínuos e estruturados – desenhados para identificar e responder a eventos que possam afetar os objetivos da organização – e por uma estrutura de governança corporativa – responsável por manter esse sistema vivo e em funcionamento. Por meio desses processos, a organização pode mapear oportunidades de ganhos e reduzir a probabilidade e o impacto de perdas. Trata-se, portanto, de um sistema integrado para conduzir o apetite à tomada de riscos no ambiente de negócios, a fim de alcançar os objetivos definidos.

Há várias estruturas e modelos de GRCorp – como os propostos pelo Committee of Sponsoring Organizations of the Treadway Commission (Coso II) e pela norma ISO 31.000[4]. O processo de GRCorp geralmente se inicia com a *identificação* e *classificação* dos riscos, o que pode ser realizado de acordo com a natureza, origem e conforme o segmento de atuação da empresa, sua cultura, entre outros critérios. Uma metodologia adotada estabelece, por exemplo, que há riscos internos (surgidos na organização), externos (alheios à empresa) e estratégicos (relacionados às informações utilizadas pela administração para a tomada de decisões). Uma das ferramentas geralmente aceitas para classificar ou categorizar os riscos é a *matriz de riscos*, que considera a origem dos eventos (interna, externa ou estratégica) e os divide em diversas classes. Os tipos de riscos serão apresentados de forma mais detalhada no Anexo 2 deste caderno.

As etapas posteriores do processo de GRCorp são a *avaliação*, que busca determinar o grau de exposição da empresa ao risco (dado pela *probabilidade de ocorrência* e *impacto* do evento), a mensuração (quantificação das estimativas de perdas) e o tratamento dado aos riscos. Este implica a tomada de uma decisão básica por parte da companhia: a de *evitar* ou *aceitar* o risco. A opção por aceitá-los leva a algumas alternativas, tais como reter, reduzir, compartilhar ou explorar o risco. Quando decide reter o risco, a empresa o assume no nível atual de severidade (impacto e probabilidade). Quando decide reduzir o grau de severidade, toma medidas para minimizar ou mitigar sua probabilidade de ocorrência e o seu impacto. Já o compartilhamento refere-se aos casos em que

4. *Podendo-se aqui integrarmos também, de forma auxiliar, as normas ISO 22.301, família ISO 27.000 e NIST, ISO 38.500 e Cobit 5, e o* draft *de norma BS 65.000 do British Standard Institute (BSI), que tratam de gestão de riscos em relação aos sistemas de informações, governança de TI, continuidade de negócios e da resiliência organizacional.*

o risco é repassado parcialmente ou dividido com terceiros. A exploração significa, por fim, o uso das competências da organização para obter resultados com a exposição no nível atual, ou com aumento da exposição, para aproveitar vantagens competitivas.

Outras etapas do processo de GRCorp são o monitoramento e a comunicação dos riscos. O primeiro envolve o constante acompanhamento, por parte do conselho e da diretoria, da eficácia e adequação do processo. Já a comunicação contribui para que o ambiente corporativo reflita os valores e a cultura de riscos desejada pela organização.

Um dos objetivos do GRCorp é encontrar um equilíbrio dos níveis de retenção, redução, exploração e transferência de riscos, e que ele seja adequado ao apetite a riscos da organização.

O apetite ao risco está associado ao nível de risco que a organização está disposta a aceitar na busca e na realização de sua missão. Ele deve ser estabelecido pelo conselho de administração (CA) (ou pelos sócios, caso a organização não possua conselho), levando em conta o melhor interesse da organização, e serve como ponto de referência para a fixação de estratégias e para a escolha dos objetivos relacionados a essas estratégias. A partir desse apetite, configura-se o perfil de riscos da empresa. Fazendo uma analogia com os investidores do mercado financeiro, há desde as companhias mais conservadoras até as mais arrojadas quando se trata da propensão a correr riscos e a aceitar possíveis perdas ou ganhos."A tolerância ao risco pode ser vista como a variação aceitável em torno dos limites estabelecidos. Dentro dos riscos e exposições aceitáveis, os limites de tolerância são 'gatilhos' para atuação do conselho de administração. Indicadores de riscos e indicadores da efetividade dos hedges devem ser acompanhados pelo conselho de administração"[5].

Outro conceito importante é a estratégia de GRCorp. Ela deve incluir questões de expectativas, objetivos, metas, investimentos e desempenho em relação às práticas de GRCorp da companhia. Tanto a definição da estratégia de GRCorp quanto a determinação do perfil de riscos são atribuições do CA, como será detalhado no Capítulo 2 deste caderno.

A gestão eficaz de riscos é dada pela qualidade da estrutura de governança, dos recursos humanos, das estratégias, da cultura, pela percepção dos riscos trazidos pela qualidade do ambiente de negócios, dos processos, dos controles e da tecnologia empregados. Ela é um diferencial das empresas nas quais relações risco-retorno embasam a tomada de decisões por parte dos administradores, visando alcançar os objetivos da organização. A relação risco-retorno sugere que quanto maior o retorno esperado dos investimentos, maiores serão os riscos a ser assumidos, o que exige a avaliação da competência para geri-los e controlá-los. Portanto, a reflexão sobre a capacidade de gerir os riscos assumidos é fundamental para escolhas bem embasadas e conscientes.

A implantação do GRCorp traz vários benefícios para as companhias gerirem seus riscos, sejam eles operacionais ou relacionados ao ambiente de negócios como um todo. Uma vez que a organização passa a contar com processos claros para identificar, mensurar, reportar, monitorar

5. *S. A. Ross, R. W. Westerfield, J. Jaffe e R. Lamb,* Administração Financeira*, 2015. p. 924. Enquanto "apetite ao risco" está associado ao nível de risco que a organização pode aceitar na busca e realização de sua missão/visão (análise* ex ante*), "tolerância ao risco" diz respeito ao nível aceitável de variabilidade na realização das metas e objetivos definidos (atividade mais associada ao monitoramento,* ex post*).*

e mitigar os riscos há um aprimoramento dos controles internos, trazendo ganhos operacionais, reduzindo a possibilidade de perdas e maximizando a eficiência e a eficácia empresarial.

Outro benefício da gestão de riscos é o aprofundamento das discussões sobre aspectos-chave do negócio, bem como a identificação de novas oportunidades. As informações levantadas propiciam melhor embasamento da tomada de decisões, facilitando os processos de escolha de alocação de recursos.

O GRCorp promove a transparência, ao explicitar os principais riscos do negócio e a forma como eles são tratados. Os investidores passam a contar com mais subsídios para avaliar se vale a pena empregar o capital naquela empresa (ou qual o retorno esperado para tanto). Outras partes interessadas, como a comunidade, o governo e os funcionários, também se beneficiam direta ou indiretamente de um sistema de GRCorp robusto e bem estruturado, na medida em que a empresa gera valor pela assunção de riscos, seus resultados são menos voláteis, e o sistema contribui para a viabilidade da organização, levando em conta as dimensões econômico-financeira, ambiental, social, reputacional e de conformidade.

Além disso, há uma melhoria na governança corporativa em decorrência dos processos inerentes ao gerenciamento de riscos, como o aumento da prestação de contas, da responsabilidade corporativa e do envolvimento dos diversos níveis de decisão da organização, como o CA. Tudo isso converge, por fim, para a longevidade da companhia e para a sua valorização.

## 1.2 História

O gerenciamento de riscos é uma prática que faz parte da rotina de qualquer empresário desde tempos muito remotos[6]. No entanto, o tema vem ganhando relevância crescente desde o fim do século XX, dado o aumento da complexidade das companhias, instituições financeiras e organizações do terceiro setor, além da maior interligação entre os mercados (globalização). O início da vasta literatura sobre o tema foi dedicado à área de seguros[7]. Mais recentemente, o assunto tem se desenvolvido como uma metodologia estruturada a partir de várias vertentes, entre as quais se destacam as de finanças, auditoria, estratégia e tecnologia da informação.

Na indústria financeira, o incentivo para implementar o gerenciamento de riscos surgiu na década de 1980, com a preocupação crescente do Bank of England e do Federal Reserve Board (EUA) com a exposição dos bancos a operações não registradas em balanço, conjugadas com problemas de empréstimos para os países então categorizados como do terceiro mundo.

O Bank of International Settlements (BIS) deu prosseguimento à iniciativa das duas instituições, por meio do envio de propostas para os bancos e de pedidos para que estes fizessem comentários e sugestões. Os primeiros resultados desse processo vieram em 1988, com o primeiro Acordo da Basileia (Basileia I) e suas emendas subsequentes a partir de 1996. O primeiro acordo, de 1988, tinha como foco a alocação de capital para fazer frente a riscos de crédito.

6. *Ver P. Bernstein,* Desafio aos Deuses: A Fascinante História do Risco*, 1996.*
7. *Ver, por exemplo, E. J. Vaughan e C. M. Elliot,* Fundamentals of Risk and Insurance*, 2003.*

A partir de 1993, introduziram-se regras para o risco de mercado, que tem como grande referência a publicação pelo JP Morgan do RiskMetrics[8] em outubro de 1994. O documento veio em resposta aos grandes desastres financeiros do início dos anos 1990 (casos conhecidos como os da Procter & Gamble, Orange County, Barings, etc.) e introduziu o conceito de *Value-at-Risk* (VaR). O VaR mede a perda potencial máxima do valor de uma carteira com determinado nível de confiança num dado intervalo de tempo e em condições normais de funcionamento do mercado.

Entretanto, o processo de identificação e tratamento de riscos não financeiros se mostra mais complexo. Enquanto os riscos financeiros são mais facilmente quantificáveis por meio de ferramentas como o VaR, a mensuração de outros riscos – como o operacional, o ambiental ou o reputacional – envolve maior grau de subjetividade. Desde a publicação do RiskMetrics, observou-se um intenso debate sobre como adaptar o conceito de VaR para os riscos não financeiros. No entanto, o único consenso atingido foi o de que o VaR não seria suficiente, sendo necessário combinar uma série de técnicas quantitativas e qualitativas para a mensuração dos riscos não financeiros. Adicionalmente, é preciso lembrar que na definição de VaR inclui-se o conceito de "ambiente normal de negócios", o que faz com que, de antemão, modelos de VaR não funcionem em situação de crise (para esses casos existem os modelos de "*stress-test*").

Em junho de 1999, o Basel Committee on Banking Supervision do BIS, ou Comitê da Basileia, propôs uma nova estrutura para a adequação do capital, o Basileia II, cuja publicação substituiu o acordo de 1988. O Comitê da Basileia propôs uma estrutura apoiada em três pilares: o primeiro tratava da adequação do capital regulatório mínimo com base nos riscos de mercado, de crédito e operacionais; o segundo reforçava a capacidade dos supervisores bancários em avaliar e adaptar o capital regulatório às condições de cada instituição financeira; e o terceiro atribuía à transparência e à divulgação de informações um papel importante e relevante no fomento à disciplina de mercado.

Como resultado da crise financeira de 2007-2008, que revelou graves deficiências regulatórias no sistema financeiro mundial, em 2010 o BIS voltou a propor um novo acordo, o Basileia III, que passou a promover o aumento de reserva de capital por parte dos bancos em busca de proteção a eventuais crises e suas decorrentes "corridas aos bancos".

Na mesma linha do BIS, a Comissão Europeia de Supervisão dos Seguros e Previdência (Ceiops – Commission for European Insurance and Occupational Pension Supervisors) elaborou em 2007 a diretiva de abordagem para a Solvência II[9]. Aplicada à indústria de seguros e de previdência, o regime de Solvência II tem uma estrutura de três pilares, em que cada um possui sua abordagem e governa um aspecto diferente: i) cálculo dos requisitos de capital de solvência e capital mínimo requerido, com base no modelo padrão ou interno; ii) princípios gerais que regem a regulação de riscos e controles internos; e iii) diretrizes sobre divulgação e transparência de informação a respeito da solvência e situação financeira.

8. *Ver <https://www.msci.com/documents/10199/5915b101-4206-4ba0-aee2-3449d5c7e95a>.*
9. *Solvency II ou Solvência II, em resumo, é a supervisão baseada em risco. É o regime criado pelo Parlamento europeu (Directive 2009/138/EC of the European Parliament and of the Council of 25 November 2009 on the taking-up and pursuit of the business of Insurance and Reinsurance [Solvency II]) para seguradoras melhorarem suas práticas de controle e gestão de riscos envolvendo práticas de governança.*

Paralelamente ao desenvolvimento pelo ramo financeiro, auditores, contadores e legisladores têm devotado atenção crescente aos controles internos. Nas companhias não financeiras, as diretrizes mais utilizadas a respeito de gestão de riscos têm origem nas recomendações do Committe of Sponsoring Organizations of the Treadway Commission (Coso). Este comitê emitiu recomendações e estabeleceu uma metodologia integrada para ajudar as organizações a analisar e a melhorar seus sistemas de controles internos e seus processos de gestão do risco empresarial (*ERM – Enterprise Risk Management*). Essa metodologia, altamente difundida desde então, tem sido incorporada às políticas, regras e regulamentos por várias empresas para melhor controlar suas atividades, de forma a atingir os objetivos estabelecidos.

O Financial Accounting Standards Board (Fasb) publicou guias encorajando a divulgação de demonstrações financeiras mais completas, demonstrando o que tem sido feito para mitigar e gerenciar os riscos a partir do modelo de governança instaurado, entre outras iniciativas. Um grupo de reguladores e profissionais tem publicado guias importantes relativos aos controles internos e ao gerenciamento de riscos. Entre os esforços notáveis incluem-se, além do Relatório Coso (1992), o Relatório Cadbury (1992) e o Turnbull (1999).

Mas o século XXI se iniciaria com uma nova onda de escândalos corporativos (Enron, WorldCom, Adelphia, entre outros), que demandaria ainda maior regulamentação. Como resposta, foi criada em 2002 nos Estados Unidos a Lei Sarbanes-Oxley (SOX), que enfatizou o papel fundamental dos controles internos e transformou em exigência legal nos EUA as boas práticas de governança corporativa. A SOX afetou todas as empresas americanas e estrangeiras com títulos e ações negociados em bolsas americanas, além de suas subsidiárias. E ainda serviu de base para regulamentações locais ao redor do mundo, colocando em voga toda a metodologia que vinha sendo desenvolvida para aprimorar os controles internos. A SOX veio a exigir que diretores-presidentes e diretores financeiros de empresas de capital aberto explicitamente certifiquem a acuracidade dos demonstrativos financeiros publicados por meio da estruturação de controles internos e da gestão de riscos corporativos, além de procedimentos de prevenção e detecção de fraudes. A lei estabeleceu também punições mais rígidas (criminais) para diretores-presidentes e diretores financeiros e alterou a forma como as empresas são auditadas. Na mesma linha da SOX e em resposta à crise do mercado financeiro de 2007-2008, foi aprovada nos EUA a Lei Dodd-Frank, que aumentou a regulamentação e definiu restrições relevantes sobre a atividade financeira do país.

A UK Bribery Act de 2010 veio reforçar e melhorar a lei anticorrupção americana (FCPA) estabelecida em 1977. O Brasil formulou também a sua lei anticorrupção (Lei 12.846/2013), que entrou em vigor em 2014. Na sequência dessa lei, uma série de decretos e portarias contribuiu para a regulamentação anticorrupção no Brasil. A lei busca responsabilizar empresas, seus controladores, controladas, consorciadas ou coligadas por práticas lesivas à administração pública. As companhias passaram a responder nas esferas administrativa e civil por atos de corrupção e fraude em licitações e contratos com o poder público.

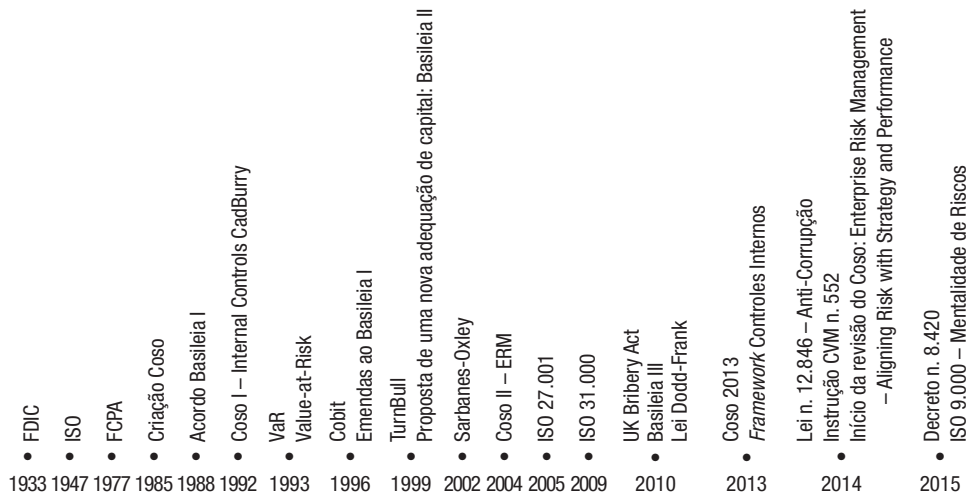
A regulamentação da Lei n. 12.846, dada por meio do Decreto Federal n. 8.420/2015, estabeleceu os critérios para cálculo de multas, os parâmetros para a avaliação de programas de

conformidade (*compliance*)[10], as regras para celebração dos acordos de leniência e disposições sobre o cadastro nacional de empresas punidas.

Especificamente sobre o programa de integridade (*compliance*), o decreto estabeleceu os mecanismos e procedimentos de integridade, auditoria, aplicação de códigos de ética ou conduta e incentivos de denúncia de irregularidades que devem ser adotados pela empresa e monitorados pelo Ministério da Transparência, Fiscalização e Controle, antiga Controladoria Geral da União. O programa de integridade deve ser estruturado, aplicado e atualizado de acordo com as características de riscos atuais das atividades de cada pessoa jurídica, que, por sua vez, é responsável pelo constante aprimoramento e adaptação do programa.

Apesar de todo esse desenvolvimento recente, a busca por padrões de GRCorp ainda continua bastante ativa no Brasil e no mundo. Modelos alinhados às boas práticas vêm sendo desenvolvidos (alguns em resposta às crises) com o objetivo de incorporar novos conceitos de avaliação de riscos e de controles, além de atender às exigências do mercado e de órgãos reguladores. A figura a seguir traz os principais eventos que contribuíram para a evolução das práticas de GRCorp:

**Figura 1. Evolução do gerenciamento de riscos**




Legenda:
FDIC – Federal Deposit Insurance Corporation
ISO – International Organization for Standardization
FCPA – Forreign Corrupt Practices Act
Coso – Committee of Sponsoring Organizations of the Treadway Commission
Basileia – Basel Committee on Banking Supervision
Cadbury – Committee on the Financial Aspects of Corporate Governance
Cobit – Control Objectives for Information and related Technology
Sarbanes-Oxley – Lei norte-americana formulada por Paul Sarbanes e Michael Oxley em 2002

10. *Programas de conformidade, ou* compliance*, têm por objetivo assegurar o cumprimento das normas legais e regulamentares. Além disso, buscam garantir a adequação, o fortalecimento e o funcionamento dos controles internos da organização.*

2

# Governança e Maturidade de GRCorp

# 2. Governança e Maturidade de GRCorp

## 2.1 Governança corporativa e gerenciamento de riscos

O IBGC, em seu *Código das Melhores Práticas de Governança Corporativa*, define governança corporativa como "o sistema pelo qual as empresas e demais organizações são dirigidas, monitoradas e incentivadas, envolvendo os relacionamentos entre sócios, conselho de administração, diretoria, órgãos de fiscalização e controle e demais partes interessadas"[11].

A gestão de riscos existe para ser associada ao processo decisório e ao processo de estabelecimento da estratégia, ou seja, a gestão de riscos é processo que deve ser integrado ao processo de decisão. Do ponto de vista operacional, podemos dizer que o gerenciamento de riscos integra a governança de uma empresa, pois o risco precisa ser identificado, medido, tratado e monitorado – e essas informações alimentam o processo de tomada de decisão por parte de diferentes agentes, sejam os sócios, o conselho de administração (CA), a diretoria, assim como as demais partes interessadas (por exemplo clientes, fornecedores, comunidade, reguladores, o governo, entre outros). Dessa forma, o GRCorp traz vantagens na estrutura de governança das organizações, como o aumento da transparência e da prestação de contas, o fortalecimento dos controles internos e maior comprometimento com a responsabilidade corporativa.

Para funcionar adequadamente, o GRCorp necessita ter estabelecido e formalizado uma estrutura de governança clara. Essa estrutura definirá atribuições e reponsabilidades de cada agente nos diferentes níveis e práticas de GRCorp no que diz respeito aos riscos, indicando, por exemplo, quem identificará e avaliará os riscos, quem tomará as decisões sobre o tratamento dos riscos, quem monitorará os riscos, e quem fiscalizará o processo como um todo.

As principais reflexões a serem discutidas pelo CA e pela diretoria para a construção do modelo de governança de GRCorp incluem:

- 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? Existe diferença entre percepção e exposição desses riscos?
- Como a organização responde aos riscos?

11. *IBGC,* Código das Melhores Práticas de Governança Corporativa*,* op. cit.*, p. 20.*

- Existem informações confiáveis para tomada de decisões?
- 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?

Este caderno não se aprofundará nos temas relacionados a cada uma dessas questões, e elas devem ser entendidas como um instrumento não exaustivo para reflexão do CA. As respostas a elas servirão de base para a avaliação do modelo atual ou para a criação do modelo de GRCorp mais apropriado para a organização.

### 2.1.1 Governança e cultura de GRCorp

A governança e a cultura de GRCorp são a base dos demais componentes de gerenciamento de riscos. A governança define o tom, reforça a importância e estabele as responsabilidades pelo GRCorp. A cultura, por sua vez, refere-se aos valores éticos, aos comportamentos desejados e ao entendimento de risco na organização. A cultura está refletida no processo de tomada de decisão e ampara o cumprimento da missão e da visão da organização. Uma cultura de consciência dos riscos enfatiza a importância do GRCorp e incentiva o fluxo transparente das informações de riscos com uma atitude de conhecimento, prestação de contas e melhoria contínua.

A cultura de riscos deve permear toda a organização, e cabe ao CA engajar-se para promover um amplo entendimento da importância do tema para a longevidade dos negócios. A cultura de riscos de uma organização decorre de sua identidade e diz respeito ao conjunto de seus padrões éticos, valores, atitudes e comportamentos aceitos e praticados, e à disseminação da gestão de riscos como parte do processo de tomada de decisão em todos os níveis. Ela é estabelecida pelo discurso e pelo comportamento do CA, da diretoria e do apetite a riscos da organização. A cultura de riscos de uma organização influencia a forma como ela identifica, aceita e faz o gerenciamento de riscos.

## 2.2 Papéis e atribuições do modelo de governança de GRCorp nas três linhas de defesa

O modelo de governança de GRCorp, representado pelas funções distribuídas na estrutura organizacional, auxilia o gerenciamento dos riscos em diferentes níveis da organização.

Esse modelo visa assegurar que a informação proveniente do processo de gestão de riscos seja adequadamente comunicada e utilizada como base para a tomada de decisões e a responsabilização em todos os níveis organizacionais aplicáveis. O modelo é mais efetivo quando

os objetivos de gestão de riscos são integrados às metas para premiação de desempenho com o acompanhamento de indicadores-chave que ponderam desempenho e riscos assumidos.

Conforme o tópico anterior, a gestão e a consideração dos riscos no processo decisório devem ser integradas à cultura da organização, e vários agentes desempenham papéis e responsabilidade no GRCorp. Ele não pode ser atribuição de apenas uma área ou pessoa, mas deve ser executada por todas as unidades e pessoas dentro da organização que tenham responsabilidade de integrar e orientar os vários esforços de gestão de riscos, interagindo com a administração.

Os processos envolvidos no GRCorp devem ser definidos e incorporados como parte integrante da cultura e da estrutura organizacional, resultando em um sistema por meio do qual a responsabilidade de gestão de riscos é claramente distribuída, as atividades são formalmente especificadas, e a comunicação é delineada para que todos os envolvidos atinjam os objetivos organizacionais.

As funções de GRCorp devem ser descritas, formalizadas, aprovadas e divulgadas na política de GRCorp de abrangência corporativa. Esta deve representar o conjunto de princípios, ações, papéis e responsabilidades necessários a identificação, avaliação, resposta e monitoramento dos riscos aos quais a empresa está exposta.

Três documentos podem constituir o arcabouço para a comunicação das práticas de GRCorp:

1) *Política de gestão de riscos*, divulgada para o mercado (a exemplo das divulgações da política de negociação de títulos mobiliários, ou da política de transações com partes relacionadas);
2) *Norma de gestão de riscos* (ou documento equivalente), de divulgação interna e que estabelece procedimentos na tomada de riscos, responsabilidades, inclusive de relato, prestação de contas, segregação de funções, fronteiras de atuação, e o sistema geral de governança da gestão de riscos; e
3) *Código de conduta*, de divulgação interna e externa, cujo objetivo é promover princípios éticos e refletir a identidade e a cultura da organização, complementando as obrigações legais e regulamentares[12].

Os processos e atividades que envolvem o GRCorp, bem como o seu monitoramento, devem ser exercidos:

i. Pelos diversos agentes dos órgãos de governança, incluindo o CA, o comitê de auditoria e demais e comitês de assessoramento (como o comitê de gerenciamento de riscos ou outros que discutam temas técnicos específicos), a diretoria e o conselho fiscal, quando aplicável. Caso a organização não possua um CA, essa atribuição será exercida pelo(s) sócio(s).
ii. Pelas três linhas de defesa[13], conforme a seguir detalhado.

12. *O Anexo 3 deste caderno traz um modelo de política e outro de norma de GRCorp para referência. O IBGC disponibiliza em seu* website *seu próprio código de conduta (ver referências bibliográficas), para que ele possa servir de inspiração para empresas, agentes de mercado e outros tipos de organização.*
13. *Três linhas de defesa ou 3LOD é uma estrutura para a governança da exposição ao risco, também implícita no quadro*

1ª Linha de defesa – realizada pelos gestores das unidades e responsáveis diretos pelos processos: contempla as funções que gerenciam e têm a responsabilidade sobre os riscos;

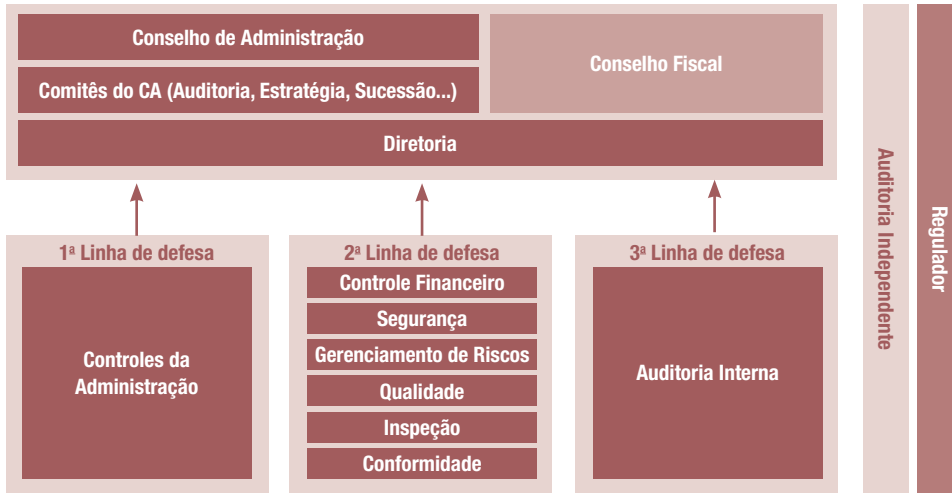
2ª Linha de defesa – realizada pelos gestores corporativos de GRCorp, de conformidade ou de outras práticas de controle, por exemplo, e que contempla as funções que monitoram a visão integrada dos riscos;

3ª Linha de defesa – realizada pela auditoria interna: fornece avaliações independentes por meio do acompanhamento dos controles internos.

O modelo da governança de GRCorp pressupõe a existência de interação entre todos os níveis da organização, incluindo o CA e seus comitês, o conselho fiscal, a diretoria e os agentes da primeira, segunda e terceira linhas de defesa.

Nesse modelo, cada uma dessas três linhas desempenha um papel distinto dentro da estrutura mais ampla de governança da organização.

**Figura 2. Linhas de defesa da função GRCorp**




Fonte: Adaptado de IIA, *Declaração de Posicionamento do IIA: As Três Linhas de Defesa no Gerenciamento Eficaz de Riscos e Controles*, 2013.

*de referência do ERM do Coso, ampla e internacionalmente usada por instituições financeiras, mas igualmente aplicável a qualquer organização. Reúne diversas funções e equipes corporativas, incluindo estruturas e agentes de governança, permitindo controlar riscos-chave identificados. Existem abordagens orientadas para cinco linhas de defesa ou 5LOD, em que a inclusão de mais duas linhas determinando as responsabilidades relativas à governança de riscos e aos cumprimentos regulatórios parte do topo da organização para a base envolvida (*tone at the top*), permite que as três linhas de defesa funcionem adequadamente de forma sistêmica, sendo possibilitada então com a inclusão da quarta linha de defesa, conhecida como "provedores de garantia interna", e da quinta linha de defesa, conhecida como "conselho de supervisão de riscos e gestão executiva".*

A diretoria inclui o diretor-presidente e os demais membros que respondem pela operação e pelo desempenho das diferentes unidades de negócio e de suporte. Os diretores podem ter diferentes responsabilidades e formas de prestação de contas no modelo das três linhas de defesa, dependendo da organização em que atuam. Por exemplo, um diretor de tecnologia pode exercer o papel de segunda linha de defesa em uma empresa do setor financeiro, mas talvez atue na primeira linha de defesa em uma companhia de tecnologia.

Existem várias alternativas para a construção da governança de GRCorp. Cada organização deverá adotar aquela mais adequada ao seu perfil e nível de maturidade. Dessa forma, as organizações em estágios mais iniciais devem refletir a partir dos direcionadores acima mencionados, para que definam o melhor modelo a ser adotado.

## 2.3 Agentes do modelo de governança de GRCorp

### 2.3.1 Órgãos de governança

#### 2.3.1.1 Conselho de administração

O CA deve ser o responsável por determinar os objetivos estratégicos, os direcionamentos e o perfil de riscos da organização adequado ao apetite a riscos desta, relacionados a sua cultura e identidade. Tais responsabilidades advêm da ideia do "*tone at the top*", ou seja, os princípios éticos da organização devem emanar justamente desse órgão.

Com relação a seu papel no GRCorp, o CA deve monitorar o funcionamento do processo de gestão de riscos e acompanhar o perfil de riscos da organização e os planos de ação definidos em resposta aos riscos.

Cabe ao CA avaliar se o desempenho da organização está de acordo com o apetite e a tolerância a riscos estabelecidos. Também é sua tarefa monitorar a eficiência e a efetividade do sistema de controles internos o qual deve sistemicamente evoluir em capacidade conforme o avanço das modalidades de riscos, inerentes à evolução do desempenho corporativo e modelos de negócios, incluídos os cibernéticos.

Durante suas reuniões, o CA deve dedicar tempo para tratar da análise da matriz de riscos e do sistema de controles internos, da definição de níveis adequados de exposição e do acompanhamento periódico das exposições a risco e dos respectivos planos de ação e mitigação.

O CA tem como missão proteger e valorizar o patrimônio da organização. Deve ter pleno conhecimento dos valores da empresa, propósitos e crenças dos acionistas, zelando pelo seu aprimoramento.

O CA deve[14]:

- Procurar compreender os elementos-chave do sucesso da organização;
- Avaliar os riscos estratégicos da empresa;
- Definir e revisar periodicamente o apetite a riscos da organização;

*14. Adaptado de NACD,* Report of the NACD Blue Ribbon Commission on Risk Governance: Balancing Risk and Reward*, 2009.*

- Definir seu papel e o dos comitês de assessoramento na supervisão dos riscos;
- Avaliar se o GRCorp da empresa (incluindo pessoas e processos) é adequado e tem recursos suficientes;
- Discutir com a diretoria executiva o nível de efetividade do sistema de controles internos da organização, assim como fornecer orientações para o seu aprimoramento constante;
- Assegurar que a administração implemente controles efetivos para mitigar os riscos de interrupções de negócios (continuidade dos negócios) e controles para mitigar os riscos de perdas das informações ou de acessos não autorizados (segurança da informação);
- Definir, com os executivos, os tipos, os formatos e a periodicidade da informação sobre riscos e controles internos que necessita para acompanhamento;
- Estimular o diálogo dinâmico e construtivo sobre riscos e controles entre a gestão e o CA, incluindo a disposição e a vontade dos conselheiros de questionar pressupostos;
- Monitorar de forma contínua os riscos que podem impactar os objetivos da organização;
- Monitorar os alinhamentos críticos: estratégia, riscos, controles, conformidade (*compliance*), incentivos e pessoas;
- Avaliar periodicamente se os processos de GRCorp permitem ao CA atingir seus objetivos de supervisão dos riscos;
- Ser o responsável formal pela orientação estratégica e pelo monitoramento das atividades de gestão de riscos e do sistema de controles internos da organização.

Além disso, cabe ao CA refletir sobre o estágio de maturidade de GRCorp em que a companhia se encontra, em cada dimensão demonstrada, e desenvolver, com a diretoria, uma visão de futuro sobre o estágio em que a organização deverá estar, e um plano de ações necessárias para tanto. A avaliação do estágio de maturidade será analisada à frente, no item 2.4.

#### 2.3.1.2 Conselho fiscal

Na qualidade de agente de governança, o conselho fiscal tem a responsabilidade de verificar se a organização está em conformidade com os seus princípios e valores, refletidos em políticas, procedimentos e normas internas, e com as leis e os dispositivos regulatórios.

No seu trabalho de fiscalização, os conselheiros fiscais devem abster-se de orientar ou direcionar qualquer atividade da organização. Eles podem contribuir sobre temas de gestão de riscos, fazendo constar de suas atas ou seu parecer, conforme o caso, as informações complementares que julgarem necessárias ou úteis ao processo de gestão de riscos ou à informação da assembleia geral. O entendimento da estratégia e dos riscos ao longo do exercício é parte fundamental do processo de formação da opinião do conselho fiscal sobre os resultados e o relatório da administração, a ser oferecido à assembleia geral.

Algumas das principais atividades relacionadas à gestão de riscos pelo conselho fiscal são:

- Conhecer os processos, o mapa de riscos, os indicadores-chave de riscos e os responsáveis pelo processo de GRCorp e seu alinhamento com os objetivos do negócio,

bem como a estrutura de controles internos, os riscos monitorados, os controles-chave, o sistema de monitoramento, e a adequação de pessoal e orçamento;

- Dialogar com os agentes com papel na definição, supervisão e monitoramento da gestão de riscos: comitê de auditoria, comitê de gestão de riscos, auditoria interna, áreas contábil, jurídica, de conformidade, de ética e conduta, buscando reunir informações sobre a gestão de riscos para subsidiar a formação de sua opinião sobre os atos de gestão;
- Definir, junto com os executivos, tipos, formatos e periodicidade da informação sobre riscos que o conselho fiscal necessita para seu dever de fiscalização.

#### 2.3.1.3 Comitê de auditoria

As organizações têm tratado esse comitê de diversas formas. Trata-se de "órgão relevante de assessoramento ao CA, para auxiliá-lo no controle sobre a qualidade de demonstrações financeiras e controles internos, visando a confiabilidade e integridade das informações para proteger a organização e todos as partes interessadas"[15].

O comitê de auditoria tem como objetivo:

- Supervisionar a qualidade e a integridade dos relatórios financeiros;
- Supervisionar a aderência às normas legais, estatutárias e regulatórias;
- Supervisionar a adequação dos processos relativos ao gerenciamento de riscos e ao sistema de controles internos, em linha com as diretrizes estabelecidas pelo CA;
- Supervisionar as atividades dos auditores internos e independentes.

O comitê de auditoria deve desenvolver papéis de supervisão da gestão de riscos conforme definidos pelo CA. A supervisão da execução das políticas, o cumprimento das normas de gestão de riscos, bem como o acompanhamento dos indicadores-chave de riscos devem ser objeto de relatos e relatórios para o conselho. Estes, por sua vez, devem incluir alertas e pontos de discussão de temas relativos a riscos para deliberação do CA. Isso deve incluir avaliações periódicas da cultura de riscos que permeia a organização.

#### 2.3.1.4 Comitê executivo de gestão de riscos corporativos[16]

Sobre a existência de um comitê executivo específico de GRCorp, vale destacar que não se trata de exigência regulatória[17], mas está alinhada às melhores práticas de gestão de riscos e controles internos. A existência desse comitê está associada ao nível de maturidade

15. *IBGC,* Código das Melhores Práticas de Governança Corporativa, op. cit., *p. 79.*
16. *O IBGC entende que comitês devem ser órgãos de assessoramento ao CA formados por conselheiros. Porém, no caso do comitê executivo de gestão de riscos corporativos, foi adotada a nomenclatura comumente utilizada no mercado. Trata-se, portanto, de um órgão subordinado à diretoria, com atividade diária na organização.*
17. *Os órgãos e entidades do Poder Executivo Federal devem instituir um comitê de governança, riscos e controles. As empresas estatais federais devem implementar políticas de conformidade e gerenciamento de riscos adequadas ao seu porte e consistentes com a natureza, complexidade e risco das operações por elas realizadas. Art. 23 da Instrução Normativa Conjunta CGU/MP n. 001, de 10 de maio de 2016.*

da organização em relação às práticas de governança corporativa e também à sua maturidade de GRCorp. O comitê executivo de gestão de riscos é órgão de avaliação colegiada da diretoria, formado pelos responsáveis diretos pelos riscos e demais executivos e profissionais que possam contribuir para o processo decisório de riscos na organização. Esse comitê pode ser instituído no processo de aprendizado organizacional para a gestão de riscos ou naquelas organizações que lidam diariamente com assunção de riscos e/ou com operações de *hedge*. O órgão pode recomendar de forma colegiada matérias de riscos a serem decididas pela diretoria e propor, juntamente com outros órgãos de governança, linhas de ação e diretrizes a serem deliberadas e aprovadas pelo CA. O comitê pode monitorar a execução das políticas e o cumprimento das normas de gestão de riscos e fazer o acompanhamento dos indicadores-chave de riscos, orientando decisões quando os indicadores apresentam a necessidade de tomada de decisão. O comitê pode também elaborar relatos e relatórios de acompanhamento para o CA. Quando o processo de gestão de riscos da organização estiver maduro, as atividades do comitê podem ser assumidas como parte da agenda das reuniões de diretoria.

Sugere-se que o comitê executivo de riscos seja coordenado pelo diretor-presidente da organização e tenha como membros o diretor financeiro, os diretores operacionais, a auditoria interna, assessores e outros responsáveis pelas áreas envolvidas com riscos. Essa composição depende do nível de complexidade das operações da organização, assim como da maturidade de seu processo de gestão de riscos, mas deve sempre contar com pessoas que possuam competências e qualidades adequadas e que sejam capazes de proporcionar supervisão independente e objetiva, a todo o tempo. O comitê pode, ainda, contratar profissionais qualificados para atuarem como especialistas.

As principais responsabilidades desse comitê executivo são:

- Aplicar e executar as ações relativas a riscos segundo os princípios, políticas e estratégias de GRCorp da organização;
- Avaliar no âmbito da gestão, e sugerir alterações, quando necessário, a estratégia de GRCorp, para deliberação do CA;
- Monitorar e desenvolver ações relativas a:
    a. Principais riscos a que a organização está exposta (por tipo de risco e/ou negócio) e o impacto deles no perfil de riscos da organização;
    b. Desenvolver e aperfeiçoar indicadores-chave de riscos e controles internos para monitoria e gestão de riscos;
    c. Discutir e escolher estratégias de mitigação de riscos avaliando alternativas recomendadas;
    d. Calcular impactos e probabilidades;
    e. Auxiliar o processo decisório da diretoria, sobretudo nos casos mais difíceis e complexos, integrando o processo de análise e cálculo de riscos nas decisões colegiadas ou das unidades.

#### 2.3.1.5 Diretoria

A diretoria é diretamente responsável por todas as atividades de uma organização, inclusive pelo GRCorp e pelas atividades de controle.

Em qualquer empresa, o diretor-presidente é o depositário final da responsabilidade pelo modelo de GRCorp e pelo sistema de controles internos. Um dos aspectos mais importantes dessa responsabilidade é prover os recursos necessários para assegurar a efetividade do modelo de GRCorp. Mais do que qualquer outro indivíduo ou função, é o diretor-presidente que deve colocar em prática o tom e o nível de maturidade esperados pelo CA em relação ao modelo de GRCorp, assim como a efetividade do sistema de controles internos. Naturalmente, os diretores de diferentes áreas terão diferentes responsabilidades no GRCorp e no sistema de controles internos. Essas responsabilidades podem variar consideravelmente, dependendo das características da organização.

As responsabilidades do diretor-presidente incluem certificar-se de que todos os componentes do GRCorp estejam implementados. O diretor-presidente geralmente cumpre com as suas atribuições:

- Fornecendo liderança e direcionamento aos altos executivos. Em conjunto com eles, o diretor-presidente estabelece os valores, os princípios e as principais políticas (aprovadas pelo CA) que constituem o alicerce do modelo de GRCorp e do sistema de controles internos que integra tal modelo;
- Reunindo-se periodicamente com os diretores responsáveis pelas principais áreas funcionais – vendas, *marketing*, produção, finanças, recursos humanos – para revisar suas responsabilidades quanto à forma como administram riscos. O diretor--presidente adquire conhecimento dos riscos inerentes às operações, às respostas a risco e às melhorias de controles necessárias, bem como à condição das iniciativas em andamento. Para efetivamente poder desenvolver seu papel de liderança, o diretor--presidente deverá definir claramente as informações de que necessita, especialmente na tomada de riscos estratégicos.

De posse dessas informações, o diretor-presidente estará em condições de tomar decisões com base em riscos calculados e de monitorar as atividades e os riscos em relação ao apetite a riscos da empresa. No caso de alteração das circunstâncias, surgimento de novos riscos, implementação de estratégias ou ações antecipadas indicarem desalinhamento potencial em relação ao perfil e ao apetite a riscos da empresa, o diretor--presidente adotará as medidas necessárias para restabelecer o alinhamento e discutirá com o CA as medidas a serem adotadas, ou, ainda, se o perfil de riscos da empresa deve ser ajustado.

### 2.3.2 Agentes de defesa

#### 2.3.2.1 Primeira linha de defesa – gestores das unidades e responsáveis diretos pelos processos

Os gestores das unidades e os responsáveis diretos pelos processos são encarregados da gestão dos riscos relativos aos objetivos de suas unidades e/ou dos processos, assim

como pelas atividades de controles neles inseridos (ver Figura 2). Essas pessoas entendem os objetivos estratégicos e alinham os objetivos operacionais aos objetivos estratégicos. Além disso, orientam a aplicação dos componentes do GRCorp e das atividades de controles, em suas esferas de responsabilidade, certificando-se de que a sua aplicação esteja consistente com o perfil e o apetite a riscos. Nesse sentido, a responsabilidade flui em cascata, e cada executivo efetivamente preside sua área de atuação. É importante destacar, portanto, que a responsabilidade pelo GRCorp deve ser atribuída a todos os níveis da empresa, evitando que se torne apenas responsabilidade do CA.

#### 2.3.2.2 Segunda linha de defesa – GRCorp

Esse grupo é responsável por fixar as políticas e metodologias – além de ter um papel importante de monitoramento do desempenho – do modelo de GRCorp. Os papéis e responsabilidades desse agente incluem, entre outros:

- Ser o defensor "apoiador" do GRCorp na empresa (desde os níveis estratégicos aos operacionais);
- Prover política, estrutura e metodologia às unidades de negócio para identificar, analisar e efetivamente gerenciar seus riscos visando ao cumprimento dos objetivos;
- Facilitar o desafio e direcionar as atividades de GRCorp, sem que isso implique a posição de responsável pelo gerenciamento corporativo de riscos;
- Garantir que a política e a estratégia de GRCorp definidas pelo conselho estejam operando efetivamente para atingir os objetivos da empresa;
- Identificar questões atuais e emergentes;
- Identificar mudanças no apetite ao risco implícito da organização;
- Auxiliar a gerência a desenvolver processos e controles para gerenciar riscos;
- Direcionar os problemas identificados aos responsáveis por saná-los;
- Prestar contas ao CA ou aos comitês de assessoramento que tratam dos temas de riscos, se houver.

Em algumas empresas, a responsabilidade de colocar em operação as práticas do sistema de controles internos é compartilhada também por esse gestor.

#### 2.3.2.3 Terceira linha de defesa – auditoria interna[18]

A auditoria interna desempenha papel fundamental na avaliação da efetividade e determinação de melhorias do GRCorp e do sistema de controles internos. Aliás, ela é parte dos sistemas de monitoramento do GRCorp e de controles internos. A auditoria interna não tem a responsabilidade primária de estabelecer e manter a estrutura de GRCorp – essa tarefa é de responsabilidade do

18. *Definições extraídas do IIA, que realizou estudos, discutiu com especialistas e definiu o papel dos auditores internos em relação aos riscos.*

diretor-presidente e dos profissionais que ele designar –, mas é fundamental para verificar a efetividade das políticas e normas estabelecidas.

Todas as atividades dentro de uma empresa – e não apenas os controles internos e o sistema de GRCorp – estão potencialmente dentro da extensão da responsabilidade dos auditores internos.

Cabe à auditoria interna:

- Avaliar a confiança das informações, revisar a efetividade e a eficiência das operações, salvaguardar os ativos assegurando o cumprimento das leis, regulamentos e contratos;
- Examinar o sistema de controles internos provendo à alta direção uma avaliação sobre a sua efetividade;
- Assessorar o diretor-presidente e o CA, por meio do comitê de auditoria, monitorando, examinando, avaliando, informando e recomendando melhorias de adequação no ambiente interno e efetividade no processo de GRCorp.

Os auditores internos devem ser objetivos com respeito às atividades que examinam. Esta objetividade está embasada pela posição que ocupam dentro da empresa, respondendo diretamente ao conselho, reportando-se ao comitê de auditoria e apresentando relatos ao conselho fiscal. O principal executivo de auditoria só deve ser selecionado e demitido com o consentimento do CA ou do comitê de auditoria. O auditor interno conta com acesso à diretoria, ao comitê de auditoria e ao conselho fiscal. Os auditores internos também têm papel fundamental em auxiliar as áreas operacionais a compreender os controles, as normas e as políticas estabelecidas.

### 2.3.3 Agentes externos

#### 2.3.3.1 Auditoria independente

Os auditores externos possibilitam à diretoria e ao CA uma visão singular, independente e objetiva, que pode contribuir para que a organização realize os seus objetivos de comunicação externa de informações financeiras.

São responsáveis por formar uma opinião sobre as demonstrações contábeis com base na avaliação de conclusões obtidas de evidências de auditoria e expressar essa opinião por meio de relatório escrito de acordo com as Normas Brasileiras de Contabilidade (ver NBC TA 700). Contribuem para o cumprimento dos objetivos de comunicação de informações financeiras da empresa e para a gestão de riscos, com informações úteis para a administração cumprir com as suas responsabilidades relativas ao GRCorp e ao sistema de controles internos.

#### 2.3.3.2 Órgãos reguladores

Os órgãos reguladores influenciam diretamente a liberdade econômica e a esfera de atuação da organização pela imposição de normas e condutas e por sanções pelo descumprimento de tais normas, ou seja, regulam o ambiente de negócio com o qual a empresa está envolvida.

## 2.4 Nível de maturidade

Esta publicação propõe os seguintes níveis de maturidade em relação ao estágio de GRCorp de uma organização: i) inicial, ii) fragmentado, iii) definido, iv) consolidado e v) otimizado. Existem distintas alternativas para a construção da governança de GRCorp e para chegar ao nível de maturidade desejado. Cada organização deverá desenhar aquela mais adequada ao seu perfil de negócio, cultura organizacional, modelo de gestão e nível desejado de maturidade em relação às suas práticas de GRCorp.

Dessa forma, podemos destacar que o nível de maturidade em GRCorp em uma organização é definido pelos seguintes aspectos:

- As ações adotadas para alcançar suas metas e objetivos em relação ao GRCorp e ao sistema de controles internos;
- O nível de esforço (tempo e investimento) empreendido para alcançar essas metas e objetivos;
- Os resultados obtidos, assim como a eficácia e a eficiência das práticas implementadas;
- O nível de envolvimento dos profissionais em relação a essas práticas;
- O nível de entendimento da maturidade da organização, assim como das oportunidades de melhorias.

Em última instância, a maturidade representa a compreensão da posição atual da empresa e deve determinar seus objetivos, além dos métodos e meios empregados para alcançá-los.

### 2.4.1 Mensurando a maturidade

A mensuração do estágio de maturidade do GRCorp é uma importante ferramenta para que a organização possa se planejar, indicando onde está, onde deseja chegar e quais ações precisará tomar para alcançar o estágio almejado de GRCorp.

Para essa mensuração, é necessário que as organizações avaliem a atual capacidade em relação às práticas de GRCorp e que compreendam como e por que devem aperfeiçoá-las. Essa avaliação permitirá que as organizações possam documentar, comunicar e programar melhorias no seu modelo.

A Figura 3 apresenta uma visão geral dos componentes de GRCorp integrados ao processo de governança corporativa da organização, considerando os principais elementos que devem existir para garantir a implementação de GRCorp.

**Figura 3 – Componentes de GRCorp**

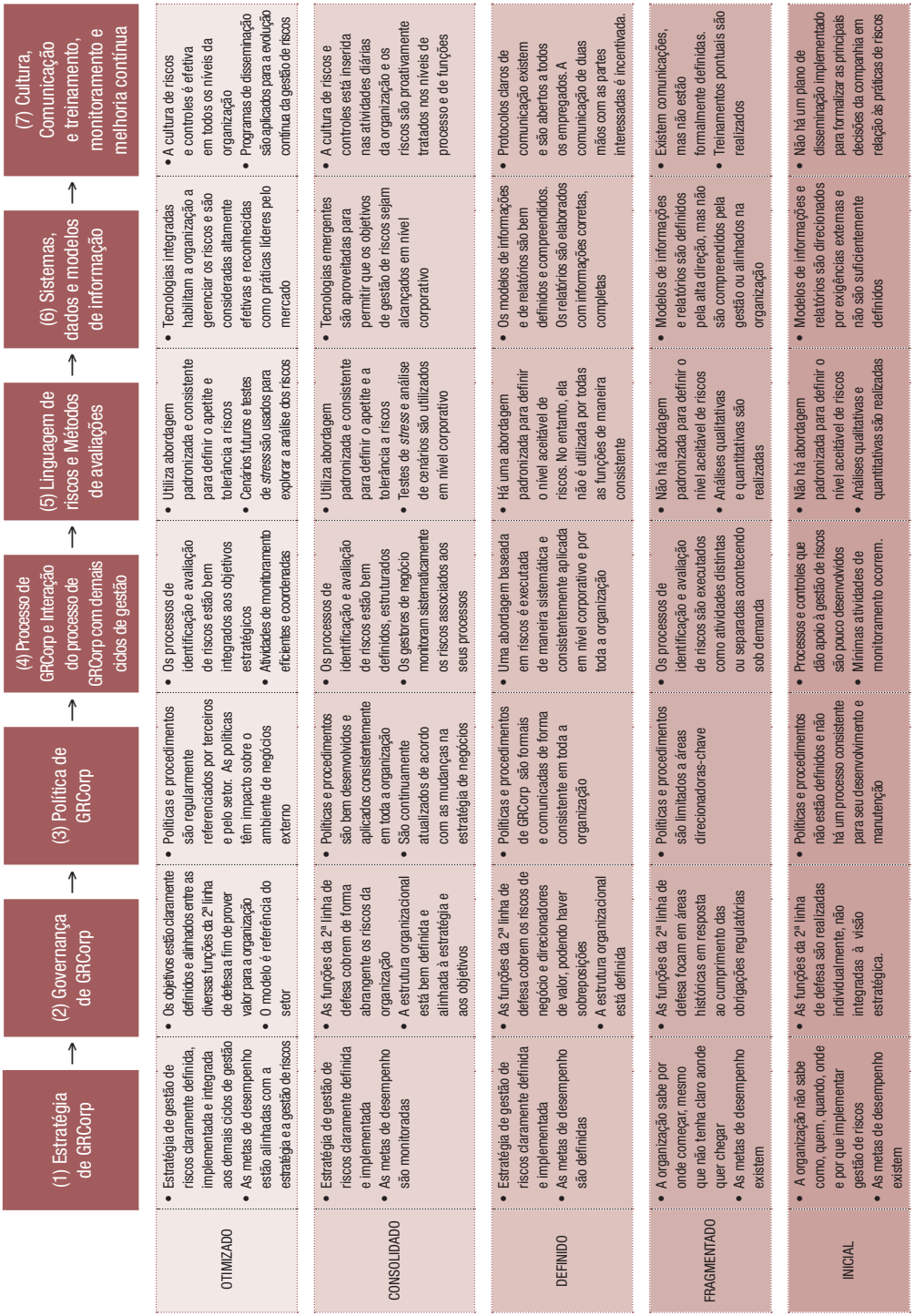
Sendo assim, o atual nível de maturidade de uma organização pode ser mensurado por meio das respostas encontradas para as seguintes reflexões, relacionadas aos componentes de GRCcorp:

| | COMPONENTE DO GRCORP | REFLEXÕES |
|---|---|---|
| (1) | Estratégia de GRCorp | • Existem estratégias, objetivos e metas de GRCorp estabelecidos? |
| (2) | Governança de GRCorp* | • Existe estrutura organizacional com papéis e responsabilidades claramente definidos nas práticas de GRCorp?<br>• A estrutura considera papel do CA e da diretoria e de todas as três linhas de defesas detalhadas no modelo de governança de GRCorp? |
| (3) | Política de GRCorp | • As questões acima mencionadas estão regimentadas, aprovadas e divulgadas por meio de uma política de GRCorp? |
| (4) | Processo de GRCorp e interação desse processo com os demais ciclos de gestão | • Existe processo de GRCorp definido e implementado com atividades de identificação de riscos, avaliação de riscos (incluindo cenários), avaliação das atividades de controle, resposta, monitoramento e comunicação?<br>• Existe norma de gestão de riscos (ou documento equivalente), de divulgação interna, que estabelece procedimentos, responsabilidades – inclusive de relato –, segregação de funções, fronteiras de atuação e o sistema geral de governança da gestão de riscos?<br>• As práticas de GRCorp estão alinhadas às demais práticas de controle?<br>• Existe um modelo definido para a incorporação do GRCorp nos processos decisórios e nos ciclos de gestão? |
| (5) | Linguagem de riscos e métodos de avaliação | • Existe taxonomia de riscos (categorias) e métodos de avaliações definidos?<br>• A organização utiliza-se de técnicas de mensuração? |
| (6) | Sistemas, dados e modelos de informação | • As informações sobre a exposição de riscos da organização são compartilhadas com os diferentes níveis da organização e capturadas de forma consistente? |
| (7) | Cultura de GRCorp, comunicação e treinamento e Monitoramento (interno e externo) e melhoria contínua | • O GRCorp esta incorporado no processo decisório, na cultura da organização e no dia a dia da gestão do negócio?<br>• A organização avalia o entendimento dos empregados em relação à cultura, às práticas de GRCorp e ao sistema de controles internos?<br>• As ações de comunicação e treinamento da cultura de GRCorp são realizadas com os diferentes públicos da organização?<br>• Os órgãos de governança e as três linhas de defesa monitoram permanentemente as práticas de GRCorp?<br>• O GRCorp é realizado de forma contínua? |

* Aqui a governança de GRCorp diz respeito a como o processo geral de gestão de riscos, definido na estratégia de GRCorp, é incorporado no processo geral de governança da organização, visando garantir que a estratégia de GRCorp seja efetiva e alinhada com os objetivos estratégicos da organização.

Ao responder a cada uma dessas reflexões, a organização poderá se autoavaliar e identificar o nível de maturidade e o estágio em que se encontra em relação às práticas de GRCorp, levando em conta as sete dimensões dos componentes de GRCorp. A Figura 4 indica as características dos estágios de maturidades propostos nesta obra:

## Figura 4. Mensurando a maturidade em relação aos componentes de GRCorp



Nesse contexto, o modelo de maturidade de GRCorp proposto aqui é derivado da função do modelo de governança corporativa da organização.

Esta publicação propõe a definição e a implementação de todos os componentes escritos, considerando as particularidades das organizações, com a participação decisiva do CA e da diretoria na definição e no monitoramento da estratégia de GRCorp, da governança de GRCorp e da política de GRCorp.

Os agentes da segunda linha de defesa desempenham o papel de operacionalizar e também de monitorar o funcionamento desses componentes que serão executados por toda a organização, incluindo a diretoria e a primeira linha de defesa, representada pelos gestores das unidades e responsáveis diretos pelos processos.

Considerando que cada organização está inserida em um contexto externo e interno determinado pelo seu setor, nível de atuação e regulamentação, além de suas partes interessadas e modelo de negócio, para que possa se posicionar e obter o resultado da mensuração de sua maturidade é recomendado que avalie seu estágio em cada dimensão e, então, realize a autoclassificação nos níveis de maturidades propostos.

Vale destacar que, em geral, as organizações apresentam maturidades distintas para cada dimensão analisada. Este fato é parte do processo. Cabe à própria entidade avaliar seu nível de maturidade em cada dimensão/estágio à luz de sua realidade e expectativas futuras em relação às práticas de GRCorp.

### 2.4.2 Consolidando os resultados da avaliação de maturidade

Uma vez que a organização tenha realizado a avaliação do nível de maturidade de GRCorp em cada dimensão demonstrada, o CA deve refletir em qual estágio a organização deve estar e, na sequência, a diretoria deve desenvolver as ações necessárias e definir os prazos esperados para atingir os próximos estágios.

É importante observar que o objetivo da utilização do modelo de maturidade é fornecer para a organização um guia estruturado e detalhado para facilitar a melhoria incremental na capacidade de gestão, permitindo a definição de uma abordagem realista de curto, médio e longo prazos para a estratégia de GRCorp. A avaliação do modelo de maturidade permite que a organização possa documentar, comunicar e programar melhorias no seu modelo de GRCorp.

O produto final dessa avaliação deverá compreender a análise da situação atual em cada dimensão, a definição do estágio desejado e as ações requeridas para se alcançar o estágio desejado, que devem ser objeto de planos de ação. Também é recomendável realizar uma pesquisa de padrões na indústria e comparar a organização com as empresas líderes nas práticas de GRCorp. A Figura 5 apresenta um exemplo de consolidação dos resultados de maturidade de GRCorp.

**Figura 5. Exemplo de consolidação dos resultados de maturidade de GRCorp**


## 2.4.3 Transformando os resultados da avaliação de maturidade em planos ou projetos

Uma vez analisado o nível de maturidade atual e definido o nível almejado, a organização precisa estabelecer as ações necessárias para a evolução das práticas de GRCorp, devendo designar um grupo de trabalho para atuar em cada uma das frentes descritas, conforme previsto no modelo de maturidade. Uma vez que as ações tenham sido implementadas, os planos de melhoria devem ser estruturados e novas avaliações devem ser realizadas.

No processo de evolução das organizações, as seguintes perguntas devem ser feitas:

- Existe uma pessoa ou equipe responsável para a melhoria do GRCorp?
- Existe um plano de melhoria preparado para a progressão das práticas de GRCorp a partir do nível atual de maturidade para o próximo nível no modelo?
- Antes da implementação do plano de melhorias, foram mensurados os benefícios que podem ser obtidos a partir do alcance do próximo nível de maturidade?

O plano de melhoria é gerenciado em termos de projeto com objetivos e recursos claros. Esse processo de melhoria contínua deve ser revisado periodicamente à luz das expectativas e da estratégia de GRCorp, do tom que vem do topo, da identidade e da cultura estabelecidas pela organização. Toda organização deve avaliar a relação de custo/benefício para determinar o nível ideal a ser atingido. Em alguns casos, por exemplo, pode não se justificar a busca do nível de maturidade otimizado.

3

# Modelo Conceitual de Implementação de GRCorp

# 3. Modelo Conceitual de Implementação de GRCorp

Apesar da tendência de as organizações indicarem um modelo específico de gestão de riscos adotado (como a ISO 31.000 e o Modelo ERM [Coso]), não existe uma única forma de implementar o GRCorp, nem uma única estrutura adequada para tal. O modelo escolhido depende da cultura da empresa e da complexidade e da natureza do negócio.

Desta forma, é importante que as organizações, ao considerarem a adoção ou construção de um modelo de GRCorp, analisem o ambiente e o mercado em que atuam, assim como seu entendimento sobre gestão de riscos e a sua cultura organizacional. Elas podem se debruçar sobre os seguintes assuntos:

- Percepção da proposta de valor: A organização, por meio do conselho de administração (CA), sobretudo, precisa se certificar de que há compreensão da importância das práticas de GRCorp para o fortalecimento da governança corporativa e para o atingimento dos objetivos estratégicos;
- Disseminação de cultura uniforme: O CA, os diretores e outros executivos devem exercer sua liderança e autoridade para disseminar o GRCorp em todos os níveis da empresa, estabelecer expectativas, definir responsabilidades, engajar o público interno, provocar a mudança e estabelecer uma cultura de identificação e gerenciamento de riscos de forma coordenada e integrada;
- Análise do contexto: A organização deve avaliar o contexto externo, nos aspectos culturais, socioeconômicos, políticos, legais, regulamentares, financeiros e tecnológicos. Deve avaliar também o contexto interno, considerando suas capacidades em recursos e conhecimentos e as possibilidades de aplicação prática dos recursos e do conhecimento da organização para a implantação de um modelo de GRCorp.

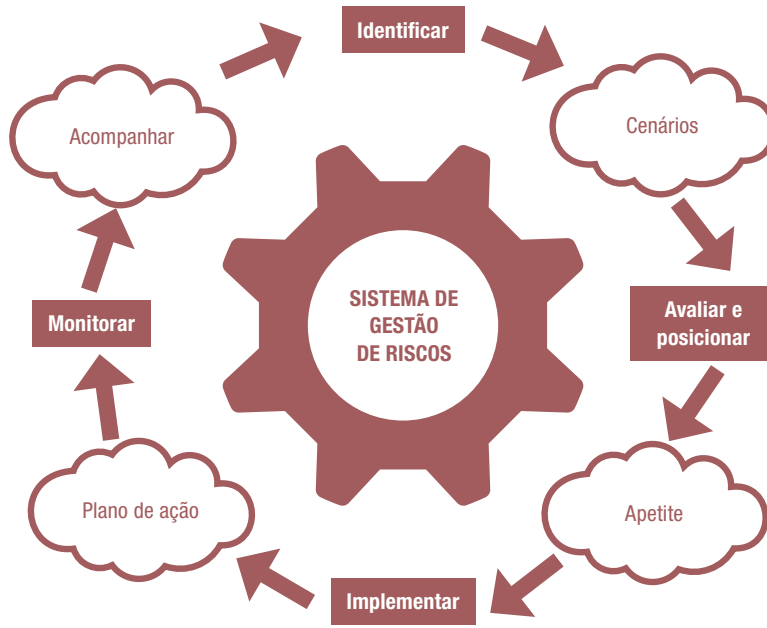
As organizações possuem diferentes propósitos, valores, princípios e estratégias, além de diversas estruturas organizacionais, filosofias operacionais diversificadas e capacidades específicas de gerenciar riscos a partir de seus perfis. Mas, a despeito dessas singularidades, há algo em comum quando se trata de GRCorp: o importante é introduzir na organização a prática de considerar os riscos de forma estruturada no processo de decisão, bem como de tratar os riscos, identificando, avaliando e respondendo de forma consistente com o modelo adotado. A implantação do modelo de GRCorp é um processo que deve ser continuamente aprimorado e alinhado ao planejamento estratégico e à identidade da organização.

A governança de GRCorp é constituída pelos processos de tomada de decisão, de supervisão, de monitoramento e de asseguração de funcionamento efetivo da estrutura de gestão de riscos. Esses processos, agregados aos conhecimentos dos gestores e diretores sobre o negócio, viabilizam o desenvolvimento de mecanismos de tomada de decisão e de controle da exposição a

riscos. Nas empresas inovadoras, a assunção de riscos é incentivada. A criatividade, a flexibilidade e principalmente a rapidez de respostas criativas trazem a necessidade de uma cultura de gestão de riscos inovadora e uma governança de GRCorp diferenciada e condizente com um ambiente altamente moderno. Esta pode ser uma forma de tratamento dos riscos disruptivos – aqueles que ameaçam tecnologias, produtos ou processos existentes, pela destruição de processos incrementais – por apresentar soluções de forma completamente revolucionária.

Para a implantação do modelo proposto neste caderno, apresentamos a seguir os principais passos que uma organização deve percorrer.

**Figura 6. Passos para a implantação do GRCorp**




## 3.1 Passo 1 – Identificar e classificar os riscos

Trata-se da definição do conjunto de eventos, externos ou internos, que podem impactar (positiva ou negativamente) os objetivos estratégicos da organização, inclusive os relacionados aos ativos intangíveis. O processo de identificação e análise geral de riscos deve ser monitorado e continuamente aprimorado para identificar os riscos eventualmente não conhecidos, seja por ignorância, seja pela falta de atribuição de probabilidade (incerteza), vulnerabilidade ou velocidade. Este processo deve ampliar o conhecimento da exposição a riscos.

Os objetivos estratégicos orientam como a organização deverá trabalhar para preservar e criar valor, o que depende crucialmente do perfil de riscos corporativos. A definição do perfil de riscos é atribuição do corpo executivo, devendo o CA discutir e avaliar (papel de supervisão).

Não há um tipo de classificação de riscos que seja consensual, exaustivo ou definitivo e aplicável a todas as organizações; a classificação deve ser desenvolvida de acordo com as características de cada organização, contemplando as particularidades da sua indústria, mercado e setor de atuação. Por exemplo: os estoques de materiais de consumo são menos relevantes para um banco do que para uma indústria, para a qual pode representar um dos principais fatores de risco. Analogamente, as variáveis relacionadas ao "risco de mercado" são cruciais para um banco e podem não ser tão relevantes para determinada organização manufatureira. Além disso, o apetite e a disposição para aceitar riscos têm componentes subjetivos, o que faz com que organizações atuando no mesmo setor e no mesmo negócio possam ter perfis e apetites ao risco diferentes. Embora a análise de probabilidades e impactos dos riscos que afetam um determinado ramo de negócio possa ser geral, o apetite e a disposição para aceitar riscos têm componentes subjetivos, o que faz com que organizações atuando no mesmo setor e no mesmo negócio apresentem perfis e apetites ao risco diferentes.

Uma das formas de categorização dos riscos consiste em desenhar uma matriz que considere a origem dos eventos internos e externos à organização e a natureza dos riscos e sua tipificação. Mais detalhes sobre diversas categorias de riscos podem ser consultados no Anexo 2 deste documento (Exemplos de categorização de riscos).

## 3.2 Passo 2 – Avaliar os riscos

Para se definir qual tratamento será dado a determinado risco, o primeiro passo consiste em determinar o seu efeito potencial, ou seja, o grau de exposição da organização àquele risco e a capacidade e o preparo para administrá-lo. Esse grau considera pelo menos três aspectos: a probabilidade de ocorrência, a vulnerabilidade e o seu impacto (em geral medido pelo impacto no desempenho econômico-financeiro na imagem da organização e em fatores sociais, ambientais, de conformidade e estratégicos). Deve-se incorporar também à análise o impacto intangível.

A quantificação do grau de exposição nem sempre é simples, podendo haver interdependência entre os riscos em dois níveis: i) os eventos podem não ser independentes; ii) um determinado evento pode gerar "impactos múltiplos", ou seja, efeitos sobre diferentes tipos de riscos, em diversas áreas. Nesse caso, o grau de exposição irá depender do impacto financeiro consolidado, da probabilidade, da velocidade ou da vulnerabilidade conjunta de todos os eventos e deve ser medido quantitativamente de acordo com a metodologia de cada empresa. Para o caso de eventos independentes que tenham efeito sobre uma única área – como a maior parte dos riscos operacionais –, o grau de exposição financeira será calculado com base técnica estudada de forma a se adequar aos objetivos e apetites a risco de cada organização.

A maneira mais usual de se documentar o impacto, a probabilidade ou a vulnerabilidade em relação aos riscos identificados é por meio do mapa de riscos. A Figura 7 é um exemplo de mapa (ou matriz) de riscos. Respostas aos riscos devem ser desenvolvidas começando com os riscos encontrados no quadrante superior direito (os riscos-chave), que concentra eventos de grande probabilidade e grande impacto, ou seja, de alta severidade. À medida que o seu grau de severidade diminui de intensidade, os riscos podem ser monitorados e tratados em periodicidades mais espaçadas, conforme ilustrado. Mas,

de forma nenhuma, os chamados riscos de severidade média (os de baixa probabilidade e alto impacto, ou alta probabilidade e baixo impacto) ou baixa devem ser ignorados, especialmente os primeiros. Respeitando as características de cada organização, os riscos-chave devem ser monitorados pela administração, e os riscos secundários devem ser monitorados pelos gestores das camadas inferiores da organização. É preciso levar em consideração, ainda, a quantidade de riscos em questão, de tal forma que seu gerenciamento não se torne demasiadamente custoso ou difícil para a organização, com a devida atenção aos efeitos da agregação de grande número de riscos de baixo impacto ou baixa probabilidade. A organização precisa, com base em sua área de atuação e perfil, fazer uma avaliação criteriosa de como gerenciar esses riscos, levando em conta seu impacto para a organização e para a sociedade, estando permanentemente atenta às externalidades[19] geradas por sua atuação.

**Figura 7. Matriz de riscos**


19. *Efeitos de uma transação que incidem sobre terceiros que não consentiram ou dela não participaram não completamente refletidos nos preços. Externalidades podem ser positivas ou negativas.*

## 3.3 Passo 3 – Implementar a função de gestão de riscos e estrutura de controles internos

Para implantar o modelo e promover a cultura de GRCorp, deve-se elaborar uma arquitetura para facilitar a implementação da governança de GRCorp.

O gerenciamento dos riscos de um determinado processo é uma atividade a ser atribuída aos gestores desse processo, inclusive com a aplicação de modelos de mercado. Cabe à gestão de GRCorp integrar e orientar os vários esforços, em consonância com os objetivos estabelecidos pela administração, e avaliar a necessidade de estabelecer um comitê executivo de gestão de riscos.

## 3.4 Passo 4 – Monitorar

### 3.4.1 Definir medidas de desempenho

O processo de definição de medidas de desempenho deve incluir a gestão de riscos e a análise permanente da efetividade das medidas definidas na medição de desempenho ajustado ao risco e na tomada de riscos ajustados ao apetite.

O principal objetivo da definição de medidas de desempenho e risco deve ser o de avaliar se os planos de ação e os respectivos controles implementados são efetivos para a avaliação do desempenho com atenção para os riscos assumidos.

Caso se chegue à conclusão de que os planos de ação e controles adotados não são suficientes para o controle dos riscos assumidos na busca de desempenho ou da mitigação dos riscos da empresa, a própria gestão de riscos deve ser revisada. Da mesma forma, é possível que a assunção de riscos esteja aquém do necessário para os objetivos esperados, conforme o apetite a riscos difinido na estratégia, o que também indica a necessidade da revisão da gestão de riscos associada ao processo decisório.

As questões que devem ser consideradas neste passo são:

- Como é feita a definição e gerenciamento dos objetivos estratégicos e das metas de desempenho;
- Como é feita a gestão dos objetivos e das metas estratégicas, norteando a identificação dos riscos, seus respectivos controles e dos demais componentes da arquitetura de riscos;
- Como é feito o gerenciamento antecipado de mudanças no ambiente de negócios, em termos de objetivos, metas, riscos e controles.

### 3.4.2 Preparar relatórios periódicos de riscos e controle

Deve ser enfatizada a importância de se combinar objetivos estratégicos com medidas de desempenho, fatores críticos de sucesso, riscos e controles. É importante também atentar-se para que o número de indicadores seja limitado aos necessários para a tomada de decisão informada, de modo a não prejudicar o seu monitoramento.

É de vital importância a preparação de relatórios periódicos de riscos, assegurando que os resultados reportados cheguem até a diretoria e o CA. Sua frequência depende do tipo de organização e do tipo de risco que está sendo reportado. Para uma empresa financeira, pode ser fundamental que o relatório seja diário e reportado à administração. Para outra organização, na qual o risco relevante é o contencioso ou o estratégico de longo prazo, o relatório periódico pode ser necessário apenas quando surgirem informações novas que justifiquem a sua elaboração.

Os relatórios periódicos de riscos e controles são peças importantes no modelo de GRCorp e podem ser usados de diversas formas e finalidades, aqui listadas de forma não exaustiva:

- Medir o progresso e monitorar metas-chave relativas à contribuição das áreas para a realização da estratégia organizacional;
- Emitir alertas quando ações corretivas se fizerem necessárias;
- Sinalizar para que a diretoria e o CA avaliem o progresso referente ao atingimento das metas corporativas como um todo;
- Alertar a diretoria e o CA das áreas de risco que precisam de atenção;
- Compartilhar melhores práticas;
- Alertar o departamento de auditoria interna a respeito de áreas de risco, que podem precisar de uma revisão nos controles internos.

Cabe à administração a avaliação contínua da adequação e da eficácia de seu modelo de GRCorp. Este deve ser constantemente monitorado, com o objetivo de assegurar a presença e o funcionamento de todos os seus componentes ao longo do tempo. O monitoramento regular ocorre no curso normal das atividades de gestão. Já o escopo e a frequência de avaliações ou revisões específicas dependem, normalmente, de uma avaliação do perfil de riscos e da eficácia dos procedimentos regulares de monitoramento.

O monitoramento contínuo realizado pelo GRCorp deve incluir:

- A documentação formal relativa aos riscos, os resultados de avaliações, análises e testes realizados;
- O relato, a documentação interna e externa (quando aplicável) de deficiências encontradas, assim como o respectivo nível de ameaça ou exposição percebida, potencial ou real, e oportunidades identificadas para exploração ou reforço e revisão dos controles utilizados;
- O conteúdo dos relatórios relativos aos riscos e os níveis de informação estratégica: significância de problemas ou fatos anormais, princípios da cultura, implicações práticas e comportamentais, informação aos níveis superiores, laterais, diretoria, CA, comitê de auditoria, auditores e outras entidades externas.

Opcionalmente, a empresa poderá adotar indicadores-chave de riscos construídos a partir de intervalos de tolerância à perda. Toda vez que o indicador estiver fora do intervalo, uma luz de alerta aparecerá no painel de controle das áreas de monitoramento responsáveis na segunda linha de defesa e/ou auditoria interna, indicando a necessidade de algum tipo de intervenção.

### 3.4.3 Registrar e quantificar as perdas ocasionadas pela materialização dos eventos de riscos

A gestão de GRCorp deve elaborar uma base de conhecimento de perdas relacionadas aos negócios de forma a auxiliar no direcionamento das decisões relacionadas aos riscos. O processo de constituição do banco de dados de perdas operacionais abrange desde a implementação de controles de captura até a categorização e armazenamento das perdas, a modelagem e o posterior reporte das perdas operacionais.

As questões que devem ser consideradas nesta etapa são:

- Como é feita a definição dos controles de captura e a classificação dos dados?
- Como é feita a implementação da base de dados?
- Como é realizado o processo de validação contínua?
- Como é feita a conciliação financeira/contábil?
- Como a base de dados deve ser estruturada de forma a proporcionar informação sistematizada, inclusive para suportar o tratamento de eventos futuros ainda não identificados?

# Considerações Finais

O conselho de administração (CA) deve ser o responsável por determinar os objetivos estratégicos e o perfil de riscos da organização. Definir seu perfil consiste em identificar o grau de apetite a riscos da organização, bem como as faixas de tolerância a desvios em relação aos níveis de riscos determinados como aceitáveis. O CA deve estabelecer também a política de responsabilidade da diretoria em: i) avaliar a quais riscos a organização pode ficar exposta; ii) desenvolver procedimentos para administrá-los; e iii) avaliar, discutir e aprovar a política de riscos proposta pelo comitê executivo de riscos.

É recomendável que os integrantes do CA tenham conhecimentos sobre indicadores de desempenho para opinar sobre o assunto em pauta, pois sem este conhecimento básico envolvendo finanças corporativas, o gerenciamento de riscos corporativos não alcançará os objetivos propostos. É recomendável também que a empresa tenha um programa para trazer a cultura de gestão de riscos para novos conselheiros.

O papel fundamental de implementar uma estrutura sólida de gerenciamento de riscos e controle é delegado aos gestores, com o comitê de auditoria (ou instância que desempenha sua função) exercendo a atividade de supervisão, auxiliado, quando necessário, pelas demais linhas de defesa.

Como ponto de partida para análise do modelo de GRCorp praticado pela organização, ou para instituí-lo, sugere-se que o CA discuta o tema com a diretoria, definindo:

- Os riscos que afetam o negócio e como eles estão integrados ao planejamento estratégico;
- Como os riscos estratégicos são considerados e controlados nos processos de decisão;
- Como os elementos de gestão de riscos estão atrelados às metas e à remuneração dos executivos;

- Como o GRCorp integra a agenda do conselho, dos comitês e dos gestores;
- Quem são os gestores de riscos de cada processo e a quem se reportam;
- Como é disseminada a cultura de gerenciamento de riscos;
- Quais os relatórios relativos ao GRCorp, quem os produz e quem os recebe;
- Quais os controles existentes para a identificação, o acompanhamento e a mitigação dos riscos.

Os membros do CA, por sua vez, devem fazer uma reflexão conjunta sobre o processo relativo ao GRCorp mais adequado à organização, respondendo às seguintes questões:

- Quais riscos devem ser levados ao CA e ao comitê de auditoria?
- Quais temas merecem uma discussão aprofundada?
- É avaliada a relação entre risco e oportunidade?
- Qual deve ser o apetite a riscos da organização?
- Quais as faixas de tolerância para cada risco assumido e como a agregação de riscos afeta as tolerâncias?
- O CA reflete explicitamente sobre riscos em seus processos decisórios?
- O CA reflete periodicamente e cobra testes sobre a efetividade do ambiente e a cultura de integridade e conformidade em todos os níveis na organização?

Essas reflexões são necessárias para que os membros do CA atentem para os riscos que devem ser analisados pelo órgão e para o seu papel dentro da estrutura de GRCorp da organização. As reflexões ajudam a evitar penalidades e consequências danosas à organização e aos seus próprios membros. A preocupação com riscos é fundamental para que o CA cumpra "o papel de guardião dos princípios, valores, objeto social e sistema de governança da organização, sendo seu principal componente, além de decidir os rumos estratégicos do negócio", de acordo com a 5ª edição do *Código das Melhores Práticas de Governança Corporativa* do IBGC em seu item 2.1.

# Referências


ABNT (Associação Brasileira de Normas Técnicas). NBR ISO 31.000: 2009, Gestão de Riscos – Princípios e Diretrizes.

Anbima (Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais). *Perspectivas: A Reforma Financeira Norte-Americana – A Lei Dodd/Frank*. Disponível em: <http://www.anbima.com.br/data/files/B2/24/B5/51/742D7510E7FCF875262C16A8/Perspectivas_20ANBIMA_20Reforma_20Americana_1_.pdf>. Acesso em: 15 dez. 2016.

Baraldi, Paulo A. "Apetite e Tolerância aos Riscos". 2013. Disponível em: <www.riskatrisk.com.br/APETITE_E_TOLERANCIA_AOS_RISCOS1.pdf>. Acesso em: 9 dez. 2016.

_____. "Como Alinhar Estratégias a Objetivos e Metas e ao Processo de Decisão". 2013. Disponível em: <www.riskatrisk.com.br/imagens-para-site/Alinhar.Estratégias.Metas.pdf>. Acesso em: 9 dez. 2016.

_____. *Gerenciamento de Riscos Empresariais*. 2. ed. revista e ampliada. Rio de Janeiro, Elsevier (Editora Campus), 2005.

Bernstein, P. *Desafio aos Deuses: A Fascinante História do Risco*. 3. ed. Campus, Rio de Janeiro, 1996.

BIS (Bank for International Settlements). *International Convergence of Capital Measurement and Capital Standards: A Revised Framework (Basel II [Basileia II])*. 2005. Disponível em: <http://www.bis.org>.

Brealey, R. & Myers, S. *Financiamento e Gestão de Risco*. Porto Alegre, Bookman, 2005.

Brigham, E. F.; Gapenski, L. C. & Ehrardt, M. C. *Administração Financeira: Teoria e Prática*. São Paulo, Atlas, 2001.

Burnaby, Priscilla & Hass, Susan. "Ten Steps to Enterprise-wide Risk Management". *Corporate Governance*, vol 9, n. 5, 2009.

Coso. *Gerenciamento de Riscos Corporativos – Estrutura Integrada – Sumário Executivo Estrutura*. PriceWaterhouse-Coopers, São Paulo, 2007.

Coso Report. *Internal Control: Integrated Framework*. 1997. Disponível em: <http://www.coso.org>.

Coso II. *ERM – Enterprise Risk Management*, 2004. Disponível em: <erm.coso.org>.

Crouhy M.; Galai, D. & Mark, R. *Gerenciamento de Risco: Abordagem Conceitual e Prática – Uma Visão Integrada dos Riscos de Crédito e de Mercado*. Rio de Janeiro/São Paulo, Qualitymark/Serasa, 2004.

Doherty, Neil A. *Integrated Risk Management: Techniques and Strategies for Managing Corporate Risk*. Nova York, McGraw-Hill, 2000.

Faber, M.; Manstetten, R. & Proops, J. *Ecological Economics: Concepts and Methods*. Cheltenham, Edward Elgar Publishing Ltd., 1996.

Galesne, A; Fensterseifer, J. E. & Lamb, R. *Decisões de Investimentos da Empresa*. São Paulo, Atlas, 1999.

Grinblat, M. & Titman, S. *Mercados Financeiros e Estratégia Corporativa*. Porto Alegre, Bookman, 2005.

IBGC (Instituto Brasileiro de Governança Corporativa). *Código das Melhores Práticas de Governança Corporativa*. 5. ed. São Paulo, 2015. Disponível em: <http://www.ibgc.org.br/index.php/publicacoes/codigo-das-melhores-praticas>. Acesso em: 9 dez. 2016.

_____. *Guia de Orientação para Gerenciamento de Riscos Corporativos*. São Paulo, IBGC, 2007 (Série Cadernos de Governança Corporativa, n. 3). Disponível em: <http://www.ibgc.org.br/index.php/publicacoescadernos-de-governanca>. Acesso em: 9 dez. 2016.

_____. *Visão Evolutiva do Modelo de Gestão de Riscos: Vale e Natura Cosméticos*. São Paulo, IBGC, 2008 (Série Estudos de Caso, n. 1). Disponível em: <http://www.ibgc.org.br/index.php/publicacoes/estudos-de-casos>. Acesso em: 9 dez. 2016.

_____. *Gestão Integrada de Riscos: Banco Real e Brasil Telecom*. São Paulo, IBGC, 2008 (Série Estudos de Caso, n. 2). Disponível em: <http://www.ibgc.org.br/index.php/publicacoes/estudos-de-casos>. Acesso em: 9 dez. 2016.

_____. *Gestão de Riscos como Instrumento para a Tomada de Decisão: Votorantim Ceculose e Papel (VCP)*. São Paulo, IBGC, 2008 (Série Estudos de Caso, n. 3). Disponível em: <http://www.ibgc.org.br/index.php/publicacoes/estudos-de-casos>. Acesso em: 9 dez. 2016.

_____. *Código de Conduta do IBGC*. São Paulo, IBGC, 2013. Disponível em: <http://www.ibgc.org.br/index.php/publicacoescodigo-de-conduta>. Acesso em: 9 dez. 2016.

IIA (The Institute of Internal Auditors). *Declaração de Posicionamento do IIA: As Três Linhas de Defesa no Gerenciamento Eficaz de Riscos e Controles*. Jan. 2013. Disponível em: <http://www.iiabrasil.org.br/new/2013/downs/As_tres_linhas_de_defesa_Declaracao_de_Posicionamento2_opt.pdf>. Acesso em: 12 set. 2016.

Jorion, P. *Value-at-Risk: A Nova Fonte de Referência para a Gestão do Risco Financeiro*. São Paulo, BM&F, 2003.

Kaplan, Robert S. & Mikes, A. "Gestão de Riscos: Um Novo Modelo". *Harvard Business Review*, jun. 2012.

NACD (National Association of Corporate Directors). *Report of the NACD Blue Ribbon Commission on Risk Governance: Balancing Risk and Reward*. Washington (DC), NACD, 2009.

Ross, S. A.; Westerfield, R. W.; Jaffe, J. & Lamb, R. *Administração Financeira*. Porto Alegre, Grupo AMGH, 2015.

Sarbanes-Oxley Act. Public Company Accounting Reform and Investor Protection Act of 2002, EUA, 2002.

Scott, H. *Risk Management and Insurance*. 2. ed. Boston, Mc Graw Hill, 2010.

Vaughan, E. J. & Elliot, C. M. *Fundamentals of Risk and Insurance*. 9. ed. Nova York, Wiley, 2003.

World Bank. *Governance and Development*. 1992.

# Anexos

## ANEXO 1 – Normas e regulamentações envolvendo gestão de riscos

Pelo fato de sofrerem contínua evolução, as normas aqui citadas devem ser consultadas diretamente em suas fontes. Também não devem ser consideradas a única fonte para a tomada de decisão.

ISO 9.000:2015 – Institui a mentalidade de riscos nas empresas buscando a certificação da ISO, que devem garantir que possuam um processo de GRCorp.

ISO 31.000:2009 – Esta ISO apresenta princípios, diretrizes, modelos e processos para o gerenciamento de riscos.

ISO Guia 73:2009 – Complemento da ISO 31.000, apresenta uma coleção de termos e definições relacionados ao gerenciamento de riscos.

Ver ambos (31.000:2009 e Guia 73:2009) em <http://www.iso.org/iso/iso31000>.

Decreto Federal n. 8.420/2015 – regulamenta diversos aspectos da Lei Anticorrupção, tais como critérios para o cálculo da multa, parâmetros para avaliação de programas de *compliance*, regras para a celebração dos acordos de leniência e disposições sobre os cadastros nacionais de empresas punidas. Procedimentos que estão sob a responsabilidade da antiga Controladoria-Geral da União (CGU) agora Ministério da Transparência, Fiscalização e Controle.

Alguns outros instrumentos regulatórios são:

- Portaria n. 909 CGU (avaliação de programas de integridade)
- Portaria n. 910 CGU (procedimento para processo administrativo e acordo de leniência)
- Instruções Normativas CGU n. 01/2015 e 02/2015 (regulamenta o registro de informações no Cadastro Nacional de Empresas Inidôneas e Suspensas [Ceis] e no Cadastro Nacional de Empresas Punidas [CNEP])
- Portaria Conjunta n. 2.279/2015 CGU e Secretaria da Micro- e Pequena Empresa (regras anticorrupção para micro- e pequenas empresas)
- Resolução CGPAR n. 18 de 10 de maio de 2016
- Instrução Normativa Conjunta MP/CGU n. 1 de 10 de maio de 2016
- Lei n. 13.303 (Lei das Estatais), de 30 de junho de 2016

# ANEXO 2 – Exemplos de categorização de riscos

Em geral, quase todos os riscos são oriundos de[20]:

- Fontes externas (fatos alheios à empresa)
- Fontes internas (surgidos na organização)
- Estratégia ou informação para tomada de decisão (na busca pela sua longevidade)

## Fontes externas

Risco externo ou de ambiente surge quando há forças externas que poderiam alterar significativamente os pilares que sustentam os objetivos e estratégias de uma organização e, num extremo, colocá-la fora dos negócios.

Pode derivar de falha na compreensão das necessidades do cliente, do fracasso em se antecipar ou reagir a ações de competidores, do excesso de dependência de fornecedores ou clientes, etc. Como a vantagem competitiva e a habilidade para sustentá-la ficam cada vez mais temporárias, as premissas da administração sobre o ambiente empresarial proveem um ponto de partida crítico para formular e avaliar estratégias empresariais. Essas premissas incluem o perfil estratégico dos principais competidores, tendências demográficas e sociais, novas tecnologias que trazem oportunidades para vantagem competitiva, desenvolvimentos políticos, econômicos e de regulamentações. Se a administração de uma companhia não possuir uma compreensão uniforme dos riscos do ambiente, os seus objetivos estratégicos não terão foco. As consequências podem ser severas: perda de fatia de mercado e de vantagem competitiva. Diante das graves consequências oriundas de erros estratégicos, a administração tem de se assegurar de que as premissas do ambiente de negócios nas quais sua estratégia é baseada têm consistência com a realidade.

Exemplos:

- Risco de concorrência
- Risco de sustentação
- Risco de relações com acionistas
- Risco de disponibilidade de capital

20. *Cabe também salientar outro tipo de risco que podemos entender ter naturezas interna e externa, de crescimento em escala mundial, muito ligado à disruptividade trazida pela nova era da informação massiva de poder coletivo gerado, que vem mudando radicalmente os modelos de negócios e empresas. O risco está no chamado advento e crescimento pelo mundo das organizações exponenciais, detentoras de um propósito transformador massivo provocando mudanças profundas, transformando e impactando indústrias e economias, bem como no fato de as organizações tradicionais e lineares, suas culturas, pessoas e decisores apresentarem visões e capacidades de entender e adotar as práticas dessa tendência.*

- Risco de desatre natural
- Risco político ou de soberania
- Risco legal e regulatório
- Risco do mercado financeiro
- Risco de recursos naturais
- Risco cibernético
- Risco disruptivo

## Fontes internas

O risco com origem em fontes internas normalmente decorre do risco de que os processos de negócio empresariais:

- Não sejam claramente definidos;
- Não estejam adequadamente alinhados com estratégias empresariais;
- Não sejam executados efetiva e eficazmente para satisfazer as necessidades dos clientes;
- Não agreguem valor à organização;
- Exponham recursos financeiros, físicos e intelectuais significativos a perdas inaceitáveis, apropriação indébita ou mau uso.

Riscos de processo incluem:

- Risco operacional
- Risco fluxo de caixa
- Risco de autoridade
- Risco de processamento de informação/tecnologia
- Risco de integridade
- Risco de satisfação do cliente
- Risco de recursos humanos
- Risco de desenvolvimento de produto
- Risco de eficiência e eficácia
- Risco de capacidade produtiva
- Risco de defasagem de desempenho
- Risco de ciclos
- Risco de fontes de matérias-primas e suprimentos
- Risco de obsolescência
- Risco de aderência
- Risco de interrupção empresarial
- Risco de falha de produto/serviço
- Risco socioambiental
- Risco de resíduos – efluentes e emissões atmosféricas
- Risco de segurança e saúde

- Risco de erosão de marca/patente

Dentro dos processos organizacionais podemos detalhar os riscos financeiros:

- Risco de preço
- Risco de derivativos
- Risco de modelagem
- Risco de taxa de juros
- Risco de câmbio
- Risco de *commodities*
- Risco de instrumentos financeiros
- Risco de liquidez
- Risco de crédito
- Risco de concentração
- Risco de compensação
- Risco de garantia

O foco que tem sido considerado com maior frequência está relacionado aos *riscos de comportamento* inesperado e indesejável dos funcionários, bem como às falhas de *conformidade* que levam a consequências adversas de suborno, relatórios financeiros fraudulentos e outros comportamentos ilegais e antiéticos.

Outro tema diz respeito ao gerenciamento dos *riscos de eventos externos incontroláveis ou em sistemas interligados e complexos*, com identificação de riscos que a empresa deve assegurar ou proteger com uma estimativa da probabilidade e consequências de eventos súbitos e análise de cenários para antecipar e planejar riscos externos como os riscos associados a *fatores macroeconômicos ou políticos globais*.

## Estratégia ou informação para tomada de decisão

Risco de estratégia ou risco de informação para tomada de decisão é o risco de que informação utilizada no apoio a decisões estratégicas, operacionais e financeiras não seja pertinente ou fidedigna.

Muitas das decisões são tomadas com base em medidas de desempenho ou em resultados de análises da indústria, de processos empresariais ou financeiros. Se os indicadores de tais medidas não estiverem alinhados com estratégias empresariais ou não foram realistas, compreensíveis e factíveis, eles não permitirão foco adequado e poderão incentivar decisões que não sejam compatíveis com as estratégias. Nesse contexto, procedimentos e tecnologias que permitam preservar as características conhecidas como Cida (confidencialidade, integridade, disponibilidade e autenticidade de informações e sistemas de informações) são importantes.

Exemplos:

- Risco de avaliação situacional

- Risco de atividades empresariais
- Risco de avaliação
- Risco de estrutura de organização
- Risco de alocação de recursos
- Risco de planejamento
- Risco de ciclo de vida
- Risco de planejamento e orçamento
- Risco de informações contábeis
- Risco de avaliação de relatórios financeiros
- Risco de avaliação de investimento
- Risco de relatórios regulamentados
- Risco de precificação
- Risco de compromisso contratual
- Risco de alinhamento
- Risco de informações regulamentadas

# ANEXO 3 – Modelos de política e de norma interna de gestão de riscos

## 3.1 Modelo de política de GRCorp

Itens que podem constituir uma política de GRCorp:

### Objetivo

### Escopo e diretrizes gerais da política de riscos

### Apetite a riscos e limites aceitáveis para riscos

Considerações sobre o alinhamento do perfil e do apetite a riscos com as estratégias da organização;
Considerações sobre os limites para riscos e os responsáveis por seu estabelecimento e acompanhamento.

### Riscos e eventos objeto da política de riscos

Considerações sobre tipologia dos riscos que afetam a organização, de fontes internas e externas;
Considerações sobre avaliação e tratamento de riscos realizados pela organização;
Comentários sobre riscos priorizados pela organização.

### Estrutura organizacional para a gestão de riscos e instâncias de governança

Descrição sucinta da estrutura organizacional de gestão de riscos;
Descrição sucinta dos papéis atribuídos às instâncias de governança:

- Conselho de administração
- Conselho fiscal
- Comitê executivo de gestão de riscos
- Diretor designado com responsável geral pela gestão de riscos
- Diretorias
- Responsável pela gestão de riscos
- Gestão de riscos nas áreas
- Auditoria interna

### Estrutura de Monitoramento

Considerações sobre indicadores de riscos, seu acompanhamento e avaliação;
Considerações sobre periodicidade de acompanhamentos pelo comitê executivo de gestão de riscos, conselhos de administração e conselho fiscal.

### Comunicação

Considerações sobre os processos de comunicação e as diretrizes de comunicação e compartilhamento de informações sobre riscos no âmbito da organização.

## 3.2 Modelo de norma interna de GRCorp

### OBJETIVOS DA NORMA INTERNA DE GESTÃO DE RISCOS

1. Objetivos
2. Abrangência
3. Aprovações
4. Responsáveis pela atualização
5. Responsáveis pela divulgação e distribuição
6. Periodicidade de atualização
7. Público-alvo e responsabilidades
8. Cumprimento e sanções
9. Vigência

### ABORDAGEM E OBJETIVOS DO GERENCIAMENTO DE RISCOS CORPORATIVOS

1. Abordagem do gerenciamento de riscos corporativos
2. Objetivos do gerenciamento de riscos corporativos
3. Ciclo de vida do gerenciamento de riscos corporativos

### PRINCÍPIOS DO GERENCIAMENTO DE RISCOS

1. Apetite a risco da organização
2. Filosofias, princípios, política, orientação e procedimentos
3. Modelo organizacional da função de gerenciamento de riscos corporativos
4. Metodologia de mensuração de riscos
5. Perfil de riscos
6. Ambiente de controle
7. Limites e *compliance*
8. Medida de desempenho do risco corporativo
9. Estrutura de reporte
10. Sistema e infraestrutura

## MODELO DE GERENCIAMENTO DE RISCOS CORPORATIVO

1. Definição de gerenciamento de riscos corporativos
2. Estabelecendo a governança de gerenciamento de riscos corporativos
3. Modelo organizacional da função de gerenciamento de riscos corporativos
4. Linguagem comum de riscos
5. Processo e procedimentos de gerenciamento de riscos corporativos
6. Critérios de priorização
7. Ciclo de revisão periódica

## FERRAMENTAS UTILIZADAS NO GERENCIAMENTO DE RISCOS CORPORATIVOS

1. *Software*
2. Documentos complementares

## FORTALECIMENTO DA CULTURA DE RISCOS E CONTROLES

1. Cultura de riscos e controles
2. Plano de treinamento

## GLOSSÁRIO DE TERMOS UTILIZADOS

1. Glossário de termos utilizados
2. Bibliografia

# ANEXO 4 – Glossário

*Agregação de riscos:* Processo em que se consideram os efeitos conjuntos resultantes de diferentes riscos ou dos efeitos do mesmo risco em vários sistemas, várias áreas de negócios ou diferentes processos da organização.

*Apetite a riscos:* Representa o nível de risco que a organização pode aceitar, conforme estabelecido por sua visão e missão, indicando o grau de exposição aceitável na sua busca de valor.

*Capacidade para o risco:* É definida pelo impacto máximo de um risco que a organização pode suportar sem ameaçar sua continuidade.

*Cultura de riscos:* A cultura de riscos de uma organização diz respeito ao conjunto de seus padrões éticos, valores, atitudes e comportamentos aceitos e praticados, e à disseminação da gestão de riscos como parte do processo de tomada de decisão em todos os níveis. Ela é estabelecida pelo discurso e pelo comportamento do conselho de administração (CA) e da diretoria e do apetite a riscos da organização.

*Dono do risco:* É designado pela diretoria como o responsável pela identificação e efetiva gestão de riscos de sua área de atuação. Deve ter papéis e responsabilidades definidos para escolher e aplicar respostas a esses riscos e autoridade suficiente para priorizar ações relativas à gestão de riscos de sua área e estar integrado ao processo geral de governança de riscos da organização.

*Estratégia de GRCorp:* A definição de expectativas, objetivos, metas, investimentos e desempenho em relação às práticas de GRCorp da companhia. Ela define em que ponto a companhia quer chegar quando se trata de GRCorp e que meios serão usados para atingir os objetivos.

*Exposição ao risco:* Diz respeito à possibilidade de a organização ser afetada por um determinado risco. Examinar se há exposição a determinado risco é importante porque pode ocorrer que uma organização que atue em determinado setor não tenha exposição a determinados riscos que afetam outras empresas desse setor.

*Governança de GRCorp:* Diz respeito aos papéis e responsabilidades de cada um dos agentes de governança corporativa da empresa, desde os funcionários envolvidos na gestão, que devem ser responsáveis por controlar riscos diretos de suas atividades, até os membros do CA e da diretoria. O fluxo de informações relativas ao controle de riscos e à transparência desses dados também é parte da governança de GRCorp da companhia, que trata de quais são os fóruns de decisão, quais as alçadas desses fóruns, quais são os seus papéis e responsabilidades e como são compostos. Orienta e deve estar inserida na política de riscos e na norma interna de gestão de riscos.

*Indicadores-chave de riscos:* São os indicadores discutidos e definidos pelo conselho de administração e pela diretoria para acompanhamento das metas de desempenho associadas ao perfil de riscos aceito pela organização. Os indicadores-chave mostram níveis de alerta para atuação do conselho na revisão da estratégia.

*Mapa (matriz) de riscos:* Ferramenta que indica, graficamente, quais são os riscos de baixas probabilidade e impacto, de baixa probabilidade e alto impacto, de alta probabilidade e baixo impacto e, por fim, de alta probabilidade e alto impacto. Veja um exemplo de mapa de riscos no item 3.2 desta obra.

*Maturidade do modelo de gestão de riscos:* Espelha a compreensão do estágio em que se encontram os processos de gestão e governança de riscos da organização. Para a avaliação da maturidade devem ser consideradas as ações adotadas para alcance de metas e objetivos de GRCorp, o esforço em tempo e investimento, a medição da eficácia e eficiência das práticas adotadas, o envolvimento dos profissionais, o entendimento do processo de gestão de riscos como parte da cultura, as estruturas organizacionais envolvidas com GRCorp, a consideração de como os riscos são integrados no processo decisório em todos os níveis e a governança do processo no seu todo.

*Norma interna de gestão de riscos:* É um documento de circulação interna da organização que traz as orientações da organziação com relação ao GRCorp, e que deve ser conhecido por todos os seus funcionários envolvidos em processos decisórios. A norma interna detalha a visão da companhia sobre o apetite e o perfil de riscos da organização e estabelece as tolerâncias para cada risco, com base em parâmetros de indicadores-chave de riscos. Deve tratar dos objetivos do GRCorp, trazer orientações, o modelo organizacional da função de GRCorp com a designação dos responsáveis diretos pelos riscos, as suas estruturas de reporte, e a integração do sistema de controles internos com a governança de GRCorp. A norma estabelece procedimentos, responsabilidades, segregação de funções, fronteiras de atuação, e operacionalização do sistema geral de governança da gestão de riscos. O Anexo 3 deste caderno traz um modelo de norma interna de GRCorp.

*Perfil de riscos:* Mostra o nível de riscos para um determinado desempenho e sua tendência de comportamento quando a organização avança na exploração de oportunidades ou na minimização de eventuais impactos.

*Política de riscos:* Uma declaração formal da organização que descreve ao mercado os seus principais entendimentos e sua visão sobre riscos, descrevendo em linhas gerais como ela faz o gerenciamento de riscos, com os objetivos e estratégias da política de gerenciamento de riscos. Traz considerações sobre o apetite e o perfil de riscos da organização, incluindo, quando for o caso, considerações gerais sobre os riscos para os quais busca proteção, os instrumentos utilizados para proteção, a estrutura organizacional de gerenciamento de riscos, a estrutura organizacional de controles internos para verificação da efetividade da política de gerenciamento de riscos e o processo geral de governança de riscos. A política de riscos é divulgada para o mercado, assim como as demais políticas declaradas pela organização e deve ser objeto de discussão para conhecimento de todos os colaboradores da organização. O Anexo 3 desta obra traz um modelo de política de GRCorp.

*Risco:* A possibilidade de ocorrência de eventos que afetem a capacidade de uma organização atingir seus objetivos.

*Sensibilidade ao risco:* Diz respeito a como a organização é afetada por um determinado risco. É determinada em função do tamanho do risco ou da relevância de seu impacto, da possibilidade de sua ocorrência e da capacidade e preparo da organização para reagir e responder a esse risco.

*Tolerância ao risco:* Estabelece as variações aceitáveis em torno dos limites estabelecidos para os riscos aceitos por uma organização.

*Tolerância máxima ao risco:* É estabelecida pelo ponto em que o perfil de riscos encontra a exposição aceitável determinada pelo apetite a riscos.

Patrocínio Master

Deloitte.

A Deloitte oferece serviços nas áreas de Auditoria, Consultoria Empresarial, Consultoria Tributária, Consultoria em Gestão de Riscos, Financial Advisory e Outsourcing para clientes dos mais diversos setores. Com uma rede global de firmas-membro em mais de 150 países, a Deloitte reúne habilidades excepcionais e um profundo conhecimento local para ajudar seus clientes a alcançar o melhor desempenho, qualquer que seja o seu segmento ou região de atuação.

No Brasil, onde atua desde 1911, a Deloitte é uma das líderes de mercado e seus mais de 5.500 profissionais são reconhecidos pela integridade, competência e habilidade em transformar seus conhecimentos em soluções para os clientes. Suas operações cobrem todo o território nacional, com escritórios em São Paulo, Belo Horizonte, Brasília, Campinas, Curitiba, Fortaleza, Joinville, Porto Alegre, Rio de Janeiro, Recife, Ribeirão Preto e Salvador.

Na área de gestão de riscos corporativos, a Deloitte conta com a maior estrutura de profissionais dedicados exclusivamente a essa função no Brasil, apoiando os clientes a endereçar todos os desafios do gênero. Nossa visão multidisciplinar tem proporcionado também uma posição diferenciada para contribuir com o aprimoramento da governança corporativa nas empresas. Acesse em nosso *website* uma diversidade de conteúdos e soluções sobre gerenciamento de riscos e governança corporativa, entre tantos outros temas de negócios.

www.deloitte.com.br

## Copatrocínio

Parker Randall Brasil

sabesp

## Apoio

- Carlos Sá
- CIP – Câmara Interbancária de Pagamentos
- Erlon Lisboa de Jesus
- Fernando Nicolau Freitas Ferreira
- Mario Filipini
- Mercedes Stinco
- Muller & Sinergy Consulting
- PFM Consultoria e Sistemas

# Gerenciamento de Riscos Corporativos

## Cadernos de Governança Corporativa

O IBGC é uma organização exclusivamente dedicada à promoção da governança corporativa no Brasil e o principal fomentador das práticas e discussões sobre o tema no país, tendo alcançado reconhecimento nacional e internacional.

Fundado em 27 de novembro de 1995, o IBGC – sociedade civil de âmbito nacional, sem fins lucrativos – tem o propósito de ser referência em governança corporativa, contribuindo para o desempenho sustentável das organizações e influenciando os agentes da nossa sociedade no sentido de maior transparência, justiça e responsabilidade.


Patrocínio Master:

Deloitte.

Copatrocínio:

Parker Randall Brasil

sabesp



IBGC | Instituto Brasileiro de Governança Corporativa

Av. das Nações Unidas, 12.551
21º andar - Brooklin Novo
World Trade Center - SP
04578-903 - São Paulo - SP
Tel.: 55 11 3185.4200
Fax.: 55 11 3043.7005
Email: ibgc@ibgc.org.br

www.ibgc.org.br