



Comissão de
Compliance

Cartilha de Gestão de Riscos

*A importância da Gestão de Riscos como
criação de valor para os negócios*

2023

Ordem dos Advogados do Brasil Seccional de Minas Gerais

Presidente: Sérgio Rodrigues Leonardo

Vice-Presidente: Ângela Parreira de Oliveira Botelho

Secretário Geral: Sanders Alves Augusto

Secretária Geral Adjunta: Cássia Marize Hatem Guimarães

Tesoureiro: Fabrício Souza Cruz Almeida

Tesoureiro Adjunto: Marco Antônio Oliveira Freitas

Diretor Institucional: Rômulo Brasil de Avelar Campos

Diretor de Apoio às Subseções: Alvaro Guilherme Ribeiro Matos

Diretor de Prerrogativas: Ércio Quaresma Firpe

Diretores de Interiorização: Bernardo Carvalho Brant Maia; Márcio Facchini Garcia e Rodrigo Carvalho Fernandes Martins Ribeiro

Diretor de Inclusão: Willian dos Santos

Comissão de Compliance - OAB MG

Presidente: Camila Melo Franco G. Mota

Vice-Presidente: Bárbara Quintão Moreno Campos

Secretário Geral: Luigi Oliveira Ribeiro

Secretária Geral Adjunta: Cynthia Rodrigues

Diretora de Estudos e Pesquisa: Stephanie de Lucca

Idealização e produção

Bernardo Barros
Luana Alves Cândida
Maria Clara Pazzini
Michelle Isaac
Miguel Ribeiro
Pablo Souza Lima
Silvia Bruzzi

SUMÁRIO

INTRODUÇÃO	4
PORQUE DEVO GERIR RISCOS	5
QUAL A IMPORTÂNCIA DA GESTÃO DE RISCOS	7
QUEM DEVE FAZER A GESTÃO DE RISCOS	8
COMO GERIR RISCOS	10
METODOLOGIAS DE AVALIAÇÃO DE RISCOS	12
QUAIS SÃO OS TIPOS DE RISCOS	14
CONCLUSÃO	18
REFERÊNCIA BIBLIOGRÁFICA	19

INTRODUÇÃO

Falar sobre riscos é falar sobre negócios, estratégia, investimento, maturidade, gestão, planejamento empresarial. Quando pensamos em riscos, devemos lembrar que ele **existe em qualquer tipo de negócio e atividade independente da estrutura e porte organizacional.**

Nesse sentido, chegamos a seguinte pergunta: **Se em qualquer negócio e atividade existem riscos, por quê devo geri-los?** A resposta não é simples, como sim ou não. O tema é complexo e se desdobra por toda a estratégia empresarial.

Com o passar dos anos houve um aumento da complexidade do mercado, da concorrência e competitividade, dos avanços tecnológicos e de constantes instabilidades econômicas. **O resultado disso é um cenário cada vez mais imprevisível em relação às incertezas e aos riscos.**

Assim a **gestão de riscos é indispensável** para que você possa entender a quais fatores internos e externos sua organização e você, como executivo, gestor, empresário ou estudante está exposto em razão da sua atividade, e, a partir disso, como você poderá **mitiga-los para garantir a perenidade de seu negócio** e até mesmo rever sua estratégia empresarial, nicho de mercado, capital de investimento e desenvolvimento de novos produtos e serviços.

Além de conhecê-los você precisa saber como **identificá-los** em todos seus processos, fazer sua **gestão, desenvolver planos de ação** para suporte da tomada de decisão da alta administração e para a definição do **apetite ao risco de sua organização.** Assim, o processo de gestão de riscos assume um papel cada vez mais protagonista, sendo algo que deve fazer parte da rotina cotidiana em todas as atividades da organização.

Convido você que se interessa pelo tema Gestão de Riscos a conhecer um pouco mais nessa cartilha, produzida pela **Comissão de Compliance a OAB/MG, gestão 2022/2024**, que irá tratar de pontos importantes no que tange ao tema, além de nortear suas ações iniciais no que se refere aos riscos.

Boa leitura.

I - POR QUE DEVO GERIR RISCOS.

O principal objetivo da gestão de riscos é **reduzir a vulnerabilidade** da empresa aos riscos existentes sejam eles internos ou externos.



MAS OS MOTIVOS VÃO MUITO ALÉM:

- ✓ Antecipar ameaças e oportunidades (resposta aos riscos);
- ✓ Minimizar efeitos negativos de uma crise e ocorrências de perdas, fraudes;
- ✓ Melhorar o grau de cumprimento dos objetivos da empresa;
- ✓ Agregar valor à organização pelo tratamento correto dos riscos e dos efeitos negativos da ocorrência;
- ✓ Melhorar o desempenho e relacionamento com os interessados/terceiros.

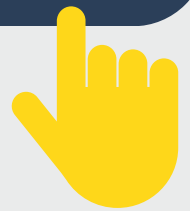
VALE SABER

Uma boa e eficiente **gestão de riscos** auxilia a organização a **administrar, organizar, planejar e controlar** seus recursos humanos e materiais, **minimizando os impactos** ou **aproveitando as oportunidades** que os riscos podem trazer.

Quando a empresa se prepara e estabelece **estratégias e objetivos**, o equilíbrio entre **investimento, crescimento e riscos** é traduzido eficientemente. Uma das formas da empresa se preparar é planejar uma **gestão de riscos**.

II - QUAL A IMPORTÂNCIA DA GESTÃO DE RISCOS?

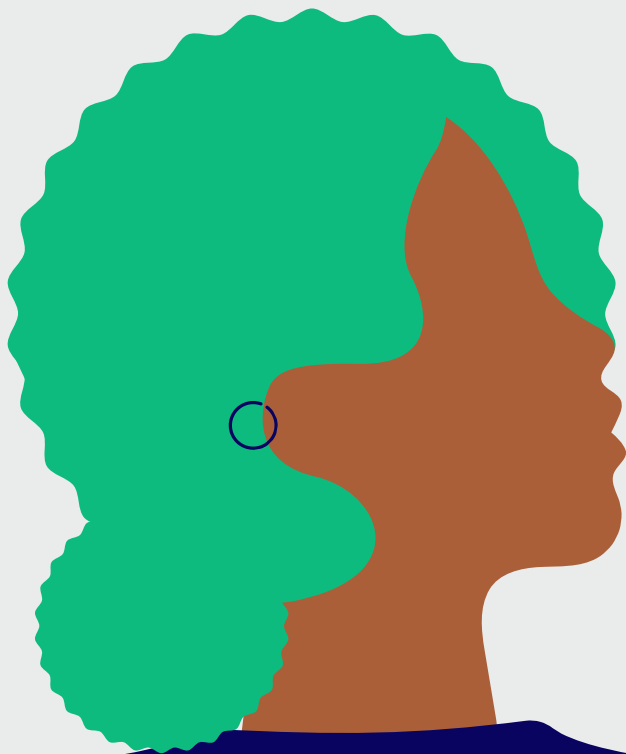
A capacidade de **entender e controlar os riscos** traz maior **segurança e confiança** nas **tomadas de decisão do negócio**, especialmente em **suporte à alta direção**.



Além de **prevenir riscos, proteger e criar valor para as organizações**, o processo de gestão de riscos é benéfico porque:

- ✓ Através da análise, se obtém conhecimento acerca de todos os processos organizacionais;
- ✓ Baseia-se nas informações mais próximas à realidade das organizações;
- ✓ Considera fatores humanos, comportamentais e culturais;
- ✓ É transparente, inclusivo, dinâmico, interativo e proporciona a instituição a possibilidade de se antecipar e/ou reagir às mudanças;
- ✓ Estimula a cultura organizacional com ênfase em padrões éticos, morais e normativos;
- ✓ Melhora e fortalece a imagem da empresa perante terceiros, colaboradores e investidores;
- ✓ Permite, através do monitoramento, a melhoria contínua dos processos da organização.

**III - MAS, QUEM DEVE
FAZER A GESTÃO DE
RISCOS?**





São considerados gestores de riscos, aqueles que são os **titulares responsáveis pelo gerenciamento dos riscos em seus respectivos âmbitos e escopos de atuação.** “Cada especialista é encarregado de prever os riscos em sua determinada área.”

VALE SABER

É recomendável que o gestor de riscos possua algumas habilidades e competências, tais como:

- ✓ Visão sistêmica;
- ✓ Saber executar, pensar, agir e tomar decisões de forma estratégica, mesmo em momentos de incerteza;
- ✓ Proatividade e viés preventivo, além de uma comunicação eficaz;
- ✓ Familiaridade com as tendências tecnológicas;
- ✓ Capacidade de traduzir complexidades e incertezas em informações claras, relevantes e oportunas para tomada de decisão;
- ✓ Saber liderar e ter ética profissional.

IV - COMO GERIR RISCOS?



A ISO 31000 é a norma que estabelece as **diretrizes para o processo de gestão de riscos** em uma organização, buscando definir as **boas práticas** que regem o setor e norteiam o **modo ideal** de realizar o gerenciamento de ameaças.

1 - Planejamento

É a decisão de como o gerenciamento de risco será feito. Isso abrange qual metodologia será utilizada, as ferramentas disponíveis e como esse gerenciamento de riscos será executado.

2 - Identificação

A identificação dos riscos pode ser definida como o processo de reconhecimento e descrição dos riscos para determinar o que, onde, quando, porque e como algo poderia ocorrer. Seu objetivo é, ao final do mapeamento de identificação, obter uma lista de riscos, incluindo as causas e os eventos que possam gerar algum impacto para a organização. É considerada parte fundamental e ferramenta estratégica para conhecimento claro do negócio.

3 - Análise Qualitativa

Compreender a importância do risco através de escalas médias de impacto e probabilidade. Deve-se avaliar quais são seus efeitos sobre a empresa e classificar quais são os mais prioritários e merecem maior atenção.

4 - Análise Quantitativa

Investigar o impacto e efeitos do risco com precisão numérica. Deve-se trabalhar os dados existentes, para investigar a probabilidade dos riscos e estimar os impactos na empresa.

5 - Planejamento de Respostas

É nesta parte do gerenciamento de riscos que são construídas as estratégias de respostas para os riscos e os planos de ações para cada um. As soluções para a atuação sobre os riscos devem ser específicas e factíveis.

6- Monitoramento

Acompanhar o comportamento dos riscos no tempo e a adequação do nível de exposição existente. Para isso, deve-se utilizar de sistemas, relatórios e indicadores.



V - METODOLOGIAS DE AVALIAÇÃO DE RISCOS

Existem inúmeras técnicas de identificação, análise e avaliação de riscos. Todas possuem vantagens e desvantagens.



NBR IEC 31010:2021 - Gestão de Riscos - Técnicas para o processo de avaliação de riscos, diretamente ligada a norma ISO 31000 - Gestão de Riscos – Diretrizes, apresenta um repertório de 42 técnicas de avaliação de riscos.



IEC 31010 - Apresenta pontos fortes e limitações das diferentes técnicas de gestão de riscos, levando em consideração quais são mais adequadas para cada etapa do processo.



A norma ainda traz diferentes **opções de técnicas para cada processo**, dentre elas destacam-se:

- **Técnicas para obter pontos de vista das partes interessadas e especialistas**

Ex.: Brainstorming, Delphi, Pesquisas, Técnica de Grupo Nominal.

- **Técnicas para identificar riscos**

Ex.: Lista de verificação e classificação, Análise de modos e efeitos de Falha (FMEA), Estudo de perigo e operabilidade (HAZOP), Análise de cenários.

- **Técnicas para determinar fontes, causas e fatores de riscos**

Ex.: Método de análise Ishkawa (espinha de peixe);

- **Técnicas para analisar controles**

Ex.: Análise Bow Tie; Análise de Camadas de Proteção

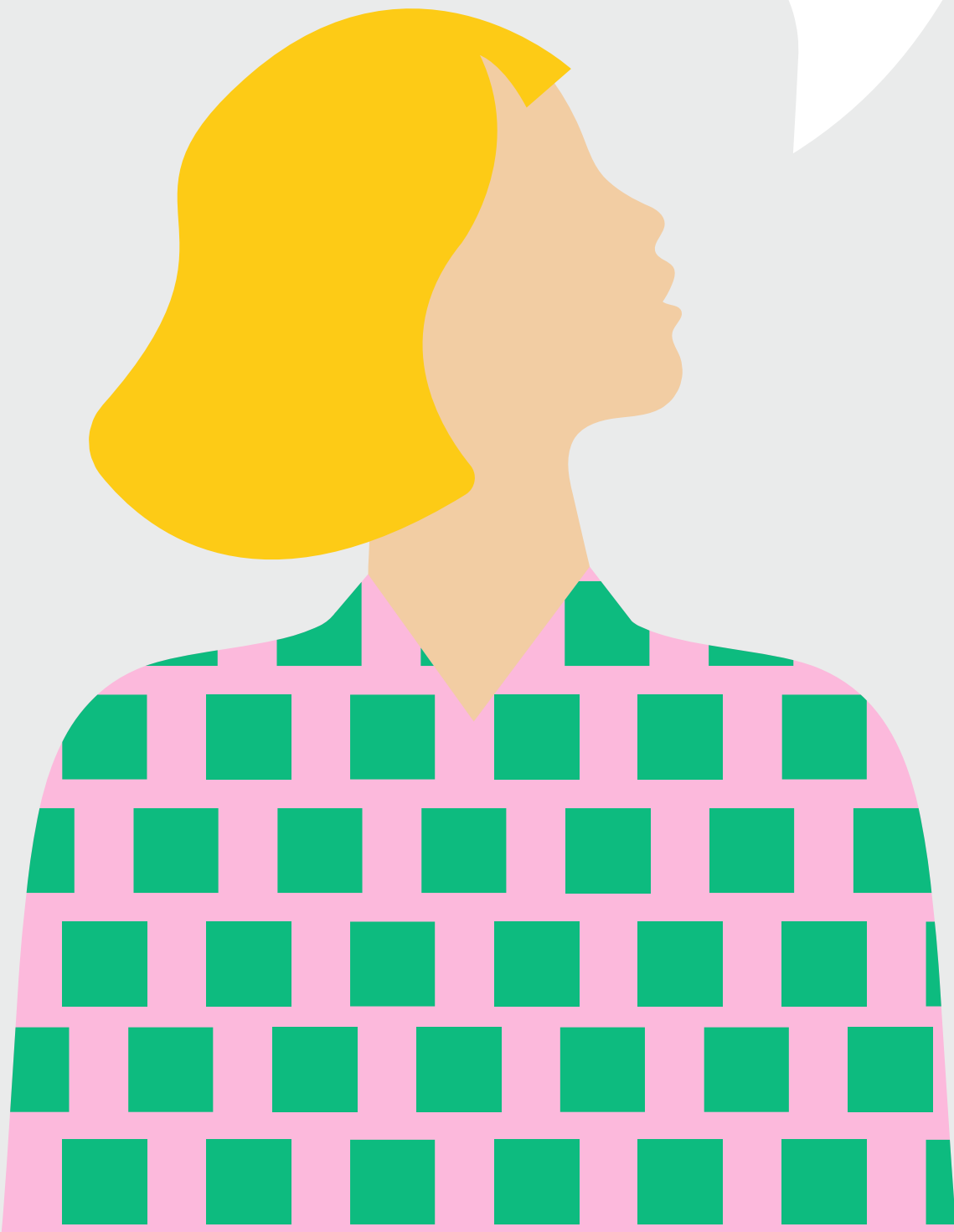
- **Técnicas para entender consequências e probabilidade**

Ex.: Matriz de probabilidade e consequência (mapa de calor); Análise da árvore de Falha.

- **Técnicas para avaliar significância do risco**

Ex.: Tão baixo quanto razoavelmente praticável (ALARP) e na medida do praticável (SFAIRP), Gráfico de Pareto.

**VI - QUAIS SÃO OS
TIPOS DE RISCOS?**



Riscos Operacionais: Ligados à operação da empresa e podem variar a depender do segmento de cada organização. Por exemplo: Mineradoras possuem como riscos operacionais os ambientais, de saúde e segurança do trabalho, riscos ligados à qualidade do produto. Empresas do setor financeiro possuem riscos ligados às operações de crédito classificados como riscos operacionais.

Riscos Estratégicos: São riscos ligados ao conjunto de ações e diretrizes de uma organização. Levam em consideração o posicionamento da empresa frente aos diversos cenários internos, como por exemplo político, econômico, avanço tecnológico e possíveis mudanças regulatórias.

Riscos Financeiros: inerente à gestão financeira da empresa. A exemplo, podem ocorrer riscos cambiais, risco de liquidez no que tange ao cumprimento de obrigações a curto prazo.

Riscos de Conformidade: São os chamados riscos de compliance. Se relacionam ao não cumprimento dos requisitos legais oriundos de leis propriamente ditas, ou, por exemplo, de resoluções como no sistema regulatório.

Riscos Cibernéticos: os riscos cibernéticos advêm de tentativas, criminosas ou não, que possam danificar, roubar ou destruir dados, comprometendo sites, servidores ou interrompendo infraestruturas inteiras de tecnologia. Os mais conhecidos são Malware, Phishing, Ransomware, Reutilização de credenciais e Ataque de senha.

Riscos Reputacionais: se caracterizam pela possibilidade de exposição negativa da organização. A reputação de uma organização consiste na forma como terceiros diretos e indiretos, sejam colaboradores, parceiros comerciais, fornecedores, investidores, e a sociedade de forma geral a enxergam. Por exemplo: é uma empresa confiável, inovadora, ética.

A reputação é construída ao longo da história da organização, dessa forma os riscos reputacionais podem gerar danos extremos e irreversíveis à organização gerando por vezes dificuldade de continuidade dos negócios.

Riscos Regulatórios: “Toda empresa está sujeita a uma série de legislações e normas regulamentadoras, seja na questão trabalhista, fiscal, tributária, ambiental ou qualquer outra. Estar em conformidade com essas regras é uma obrigação e também representa uma ameaça, através dos chamados riscos regulatórios.

Entende-se como risco regulatório a possibilidade e o impacto causado por uma eventual mudança na legislação vigente ou normas regulamentadoras sob as quais uma empresa é regida.

Isso significa que, alterações no sistema regulatório podem gerar efeitos negativos para uma organização.”

CONCLUSÃO

A solução de gestão de riscos, permite a **redução e mitigação dos riscos e melhora a performance corporativa**. As empresas podem, inclusive, utilizar o nível de maturidade da sua política e exercer a gestão de riscos para controlar os riscos globais e estabelecer prioridades na agenda do plano estratégico.

Implementar uma política de conformidade e gerenciar riscos ajudará a empresa a **entender melhor seus riscos globais e cumprir os regulamentos locais**. Pode também ajudá-lo a **acompanhar seus programas internos, gerenciar o desempenho geral** e atuar como uma **ferramenta de gerenciamento corporativo**.

Gerir riscos é gerir conhecimento.

Não há dúvidas que a gestão de riscos é essencial para qualquer organização, nos diversos tipos de estrutura desde que bem executada, como apresentamos brevemente ao longo deste material, **pode diminuir os riscos de uma instituição, fortalecer a marca empresarial, auxiliar na identificação de ameaças e oportunidades**. Também pode ser utilizada como ferramenta de gestão estratégica obrigatória para o crescimento e perenidade de uma organização.

REFERÊNCIAS BIBLIOGRÁFICAS

A.C.E. Consultoria. Gerenciamento de Riscos. Livro eletrônico. Disponível em >www.aceconsultoria.com.br

ABNT NBR ISO 31000:2018 - Gestão de Riscos - Diretrizes

CAVALCANTI, Leo. Risco regulatório: o que é, como funciona e como prevenir. Linkana, 2021. Disponível em: <<https://www.linkana.com/blog/risco-regulatorio/>>

NBR IEC 31010:2021 - Gestão de Riscos - Técnicas para o processo de avaliação de riscos

Regulatory Support & Strategic Risk. Deloitte. Disponível em: <<https://www2.deloitte.com/br/pt/pages/risk/solutions/regulatorio-estrategico.html>>

Risco de negócio: o que é, os principais e como reconhecê-los. FIA BUSINESS SCHOOL, 2021. Disponível em: <<https://fia.com.br/blog/risco-de-negocio/>>