NORMA
BRASILEIRA

ABNT NBR ISO 31000

Primeira edição
30.11.2009

Válida a partir de
30.12.2009

Gestão de riscos — Princípios e diretrizes

Risk management – Principles and guidelines

ICS 03.100.01

ISBN 978-85-07-01838-4

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS

Número de referência
ABNT NBR ISO 31000:2009
24 páginas

ABNT
Av.Treze de Maio, 13 - 28º andar
20031-901 - Rio de Janeiro - RJ
Tel.: + 55 21 3974-2300
Fax: + 55 21 3974-2346
abnt@abnt.org.br
www.abnt.org.br

Sumário

Prefácio Nacional

A Associação Brasileira de Normas Técnicas (ABNT) é o Foro Nacional de Normalização. As Normas Brasileiras, cujo conteúdo é de responsabilidade dos Comitês Brasileiros (ABNT/CB), dos Organismos de Normalização Setorial (ABNT/ONS) e das Comissões de Estudo Especiais (ABNT/CEE), são elaboradas por Comissões de Estudo (CE), formadas por representantes dos setores envolvidos, delas fazendo parte: produtores, consumidores e neutros (universidade, laboratório e outros).

Os Documentos Técnicos ABNT são elaborados conforme as regras das Diretivas ABNT, Parte 2.

A Associação Brasileira de Normas Técnicas (ABNT) chama atenção para a possibilidade de que alguns dos elementos deste documento podem ser objeto de direito de patente. A ABNT não deve ser considerada responsável pela identificação de quaisquer direitos de patentes.

A ABNT NBR ISO 31000 foi elaborada pela Comissão de Estudo Especial de Gestão de Riscos (CEE-63). O Projeto circulou em Consulta Nacional conforme Edital nº 08, de 07.08.2009 a 08.09.2009, com o número de Projeto 63:000.01-001.

Esta Norma é uma adoção idêntica, em conteúdo técnico, estrutura e redação, à ISO 31000:2009, que foi elaborada pelo ISO *Technical Management Board Working Group on risk management* (ISO/TMB/WG), conforme ISO/IEC Guide 21-1:2005.

O Escopo desta Norma Brasileira em inglês é o seguinte:

Scope

This Standard provides principles and generic guidelines on risk management.

This Standard can be used by any public, private or community enterprise, association, group or individual. Therefore, this Standard is not specific to any industry or sector.

NOTE For convenience, all the different users of this Standard are referred to by the general term "organization".

This Standard can be applied throughout the life of an organization, and to a wide range of activities, including strategies and decisions, operations, processes, functions, projects, products, services and assets.

This Standard can be applied to any type of risk, whatever its nature, whether having positive or negative consequences.

Although this Standard provides generic guidelines, it is not intended to promote uniformity of risk management across organizations. The design and implementation of risk management plans and frameworks will need to take into account the varying needs of a specific organization, its particular objectives, context, structure, operations, processes, functions, projects, products, services, or assets and specific practices employed.

It is intended that this Standard be utilized to harmonize risk management processes in existing and future standards. It provides a common approach in support of standards dealing with specific risks and/or sectors, and does not replace those standards.

This Standard is not intended for the purpose of certification.

Introdução

Organizações de todos os tipos e tamanhos enfrentam influências e fatores internos e externos que tornam incerto se e quando elas atingirão seus objetivos. O efeito que essa incerteza tem sobre os objetivos da organização é chamado de "risco".

Todas as atividades de uma organização envolvem risco. As organizações gerenciam o risco, identificando-o, analisando-o e, em seguida, avaliando se o risco deve ser modificado pelo tratamento do risco a fim de atender a seus critérios de risco. Ao longo de todo este processo, elas comunicam e consultam as partes interessadas e monitoram e analisam criticamente o risco e os controles que o modificam, a fim de assegurar que nenhum tratamento de risco adicional seja requerido. Esta Norma descreve este processo sistemático e lógico em detalhes.

Embora todas as organizações gerenciem os riscos em algum grau, esta Norma estabelece um número de princípios que precisam ser atendidos para tornar a gestão de riscos eficaz. Esta Norma recomenda que as organizações desenvolvam, implementem e melhorem continuamente uma estrutura[1)] cuja finalidade é integrar o processo para gerenciar riscos na governança, estratégia e planejamento, gestão, processos de reportar dados e resultados, políticas, valores e cultura em toda a organização.

A gestão de riscos pode ser aplicada a toda uma organização, em suas várias áreas e níveis, a qualquer momento, bem como a funções, atividades e projetos específicos.

Embora a prática de gestão de riscos tenha sido desenvolvida ao longo do tempo e em muitos setores a fim de atender às necessidades diversas, a adoção de processos consistentes em uma estrutura abrangente pode ajudar a assegurar que o risco seja gerenciado de forma eficaz, eficiente e coerentemente ao longo de uma organização. A abordagem genérica descrita nesta Norma fornece os princípios e diretrizes para gerenciar qualquer forma de risco de uma maneira sistemática, transparente e confiável, dentro de qualquer escopo e contexto.

Cada setor específico ou aplicação da gestão de riscos traz consigo necessidades particulares, vários públicos, percepções e critérios. Portanto, uma característica-chave desta Norma é a inclusão do estabelecimento do contexto como uma atividade no início deste processo genérico de gestão de riscos. O estabelecimento do contexto captura os objetivos da organização, o ambiente em que ela persegue esses objetivos, suas partes interessadas e a diversidade de critérios de risco – o que auxiliará a revelar e avaliar a natureza e a complexidade de seus riscos.

O relacionamento entre os princípios para gerenciar riscos, a estrutura na qual ocorre e o processo de gestão de riscos descritos nesta Norma são mostrados na Figura 1.

Quando implementada e mantida de acordo com esta Norma, a gestão dos riscos possibilita a uma organização, por exemplo:

— aumentar a probabilidade de atingir os objetivos;

— encorajar uma gestão pro-ativa;

— estar atento para a necessidade de identificar e tratar os riscos através de toda a organização;

---

1) **NOTA DA TRADUÇÃO:** Para os efeitos desta Norma Brasileira traduziu-se o termo *framework* por "estrutura".

— melhorar a identificação de oportunidades e ameaças;

— atender às normas internacionais e requisitos legais e regulatórios pertinentes;

— melhorar o reporte das informações financeiras;

— melhorar a governança;

— melhorar a confiança das partes interessadas;

— estabelecer uma base confiável para a tomada de decisão e o planejamento;

— melhorar os controles;

— alocar e utilizar eficazmente os recursos para o tratamento de riscos;

— melhorar a eficácia e a eficiência operacional;

— melhorar o desempenho em saúde e segurança, bem como a proteção do meio ambiente;

— melhorar a prevenção de perdas e a gestão de incidentes;

— minimizar perdas;

— melhorar a aprendizagem organizacional; e

— aumentar a resiliência da organização.

Esta Norma é destinada a atender às necessidades de uma ampla gama de partes interessadas, incluindo:

a) os responsáveis pelo desenvolvimento da política de gestão de riscos no âmbito de suas organizações;

b) os responsáveis por assegurar que os riscos são eficazmente gerenciados na organização como um todo ou em uma área, atividade ou projeto específicos;

c) os que precisam avaliar a eficácia de uma organização em gerenciar riscos; e

d) desenvolvedores de normas, guias, procedimentos e códigos de práticas que, no todo ou em parte, estabelecem como o risco deve ser gerenciado dentro do contexto específico desses documentos.

As atuais práticas e processos de gestão de muitas organizações incluem componentes de gestão de riscos, e muitas organizações já adotaram um processo formal de gestão de riscos para determinados tipos de risco ou circunstâncias. Nesses casos, uma organização pode decidir conduzir uma análise crítica de suas práticas e processos existentes, tomando como base esta Norma.

Nesta Norma, as expressões "gestão de riscos" e "gerenciando riscos" são ambas utilizadas. Em termos gerais, "gestão de riscos" refere-se à arquitetura (princípios, estrutura e processo) para gerenciar riscos eficazmente, enquanto que "gerenciar riscos" refere-se à aplicação dessa arquitetura para riscos específicos.

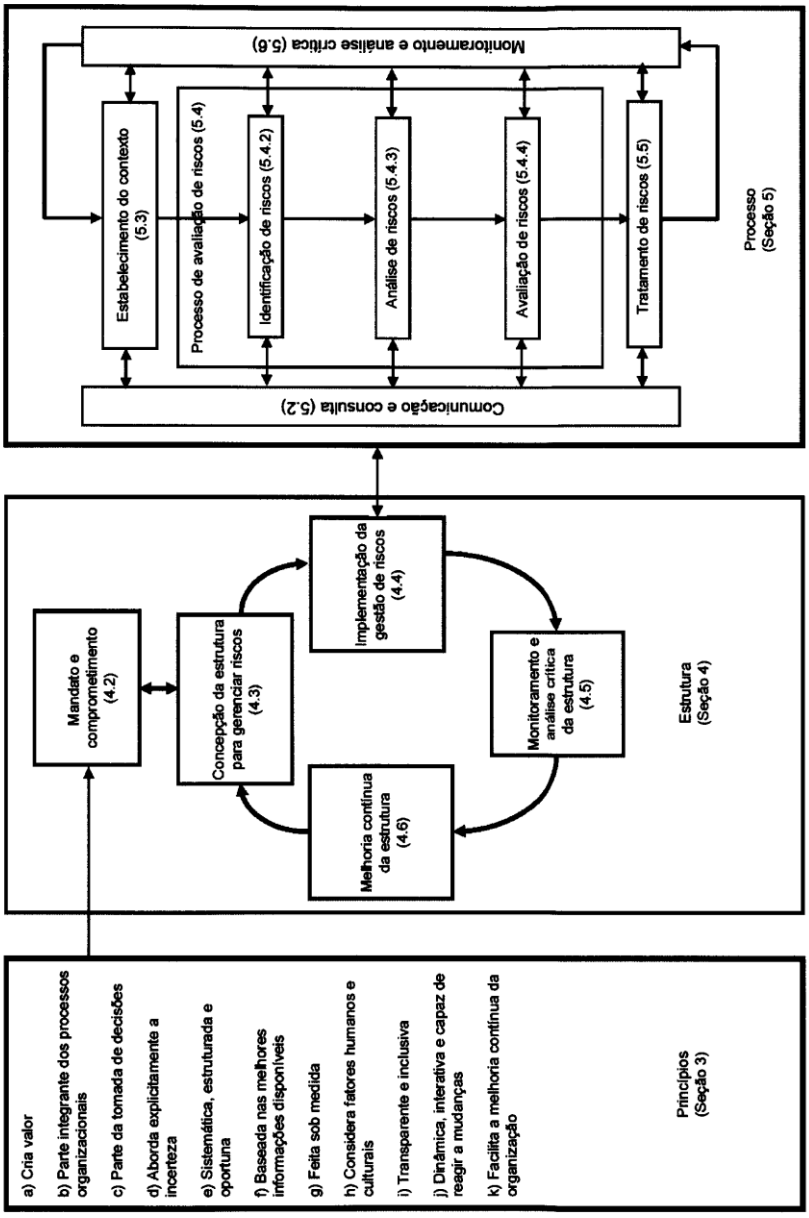

Figura 1 — Relacionamentos entre os princípios da gestão de riscos, estrutura e processo

Gestão de riscos — Princípios e diretrizes

1 Escopo

Esta Norma fornece princípios e diretrizes genéricas para a gestão de riscos.

Esta Norma pode ser utilizada por qualquer empresa pública, privada ou comunitária, associação, grupo ou indivíduo. Portanto, esta Norma não é específica para qualquer indústria ou setor.

NOTA Para conveniência, todos os diferentes usuários desta Norma são referidos pelo termo geral "organização".

Esta Norma pode ser aplicada ao longo da vida de uma organização e a uma ampla gama de atividades, incluindo estratégias, decisões, operações, processos, funções, projetos, produtos, serviços e ativos.

Esta Norma pode ser aplicada a qualquer tipo de risco, independentemente de sua natureza, quer tenha consequências positivas ou negativas.

Embora esta Norma forneça diretrizes genéricas, ela não pretende promover a uniformidade da gestão de riscos entre organizações. A concepção e a implementação de planos e estruturas para gestão de riscos precisarão levar em consideração as necessidades variadas de uma organização específica, seus objetivos, contexto, estrutura, operações, processos, funções, projetos, produtos, serviços ou ativos e práticas específicas empregadas.

Pretende-se que esta Norma seja utilizada para harmonizar os processos de gestão de riscos tanto em normas atuais como em futuras. Esta Norma fornece uma abordagem comum para apoiar Normas que tratem de riscos e/ou setores específicos, e não substituí-las.

Esta Norma não é destinada para fins de certificação.

2 Termos e definições

Para os efeitos deste documento, aplicam-se os seguintes termos e definições.

2.1
risco
efeito da incerteza nos objetivos

NOTA 1 Um efeito é um desvio em relação ao esperado – positivo e/ou negativo.

NOTA 2 Os objetivos podem ter diferentes aspectos (tais como metas financeiras, de saúde e segurança e ambientais) e podem aplicar–se em diferentes níveis (tais como estratégico, em toda a organização, de projeto, de produto e de processo).

NOTA 3 O risco é muitas vezes caracterizado pela referência aos **eventos** (2.17) potenciais e às **consequências** (2.18), ou uma combinação destes.

NOTA 4 O risco é muitas vezes expresso em termos de uma combinação de consequências de um evento (incluindo mudanças nas circunstâncias) e a **probabilidade** (2.19) de ocorrência associada.

NOTA 5 A incerteza é o estado, mesmo que parcial, da deficiência das informações relacionadas a um evento, sua compreensão, seu conhecimento, sua consequência ou sua probabilidade.

[ABNT ISO GUIA 73:2009, definição 1.1]

2.2
gestão de riscos
atividades coordenadas para dirigir e controlar uma organização no que se refere a **riscos** (2.1)

[ABNT ISO GUIA 73:2009, definição 2.1]

2.3
estrutura da gestão de riscos
conjunto de componentes que fornecem os fundamentos e os arranjos organizacionais para a concepção, implementação, **monitoramento** (2.28), análise crítica e melhoria contínua da **gestão de riscos** (2.2) através de toda a organização

NOTA 1 Os fundamentos incluem a política, objetivos, mandatos e comprometimento para gerenciar **riscos** (2.1).

NOTA 2 Os arranjos organizacionais incluem planos, relacionamentos, responsabilidades, recursos, processos e atividades.

NOTA 3 A estrutura da gestão de riscos está incorporada no âmbito das políticas e práticas estratégicas e operacionais de toda a organização.

[ABNT ISO GUIA 73:2009, definição 2.1.1]

2.4
política de gestão de riscos
declaração das intenções e diretrizes gerais de uma organização relacionadas à **gestão de riscos** (2.2)

[ABNT ISO GUIA 73:2009, definição 2.1.2]

2.5
atitude perante o risco
abordagem da organização para avaliar e eventualmente buscar, reter, assumir ou afastar-se do **risco** (2.1)

[ABNT ISO GUIA 73:2009, definição 3.7.1.1]

2.6
plano de gestão de riscos
esquema dentro da **estrutura da gestão de riscos** (2.3), que especifica a abordagem, os componentes de gestão e os recursos a serem aplicados para gerenciar **riscos** (2.1)

NOTA 1 Os componentes de gestão tipicamente incluem procedimentos, práticas, atribuição de responsabilidades, seqüência e cronologia das atividades.

NOTA 2 O plano de gestão de riscos pode ser aplicado a um determinado produto, processo e projeto, em parte ou em toda a organização.

[ABNT ISO GUIA 73:2009, definição 2.1.3]

2.7
proprietário do risco
pessoa ou entidade com a responsabilidade e a autoridade para gerenciar um **risco** (2.1)

[ABNT ISO GUIA 73:2009, definição 3.5.1.5]

2.8
processo de gestão de riscos
aplicação sistemática de políticas, procedimentos e práticas de gestão para as atividades de comunicação, consulta, estabelecimento do contexto, e na identificação, análise, avaliação, tratamento, **monitoramento** (2.28) e análise crítica dos **riscos** (2.1)

[ABNT ISO GUIA 73:2009, definição 3.1]

2.9
estabelecimento do contexto
definição dos parâmetros externos e internos a serem levados em consideração ao gerenciar riscos, e estabelecimento do escopo e dos **critérios de risco** (2.22) para a **política de gestão de riscos** (2.4)

[ABNT ISO GUIA 73:2009, definição 3.3.1]

2.10
contexto externo
ambiente externo no qual a organização busca atingir seus objetivos

NOTA O contexto externo pode incluir:

— o ambiente cultural, social, político, legal, regulatório, financeiro, tecnológico, econômico, natural e competitivo, seja internacional, nacional, regional ou local;

— os fatores–chave e as tendências que tenham impacto sobre os objetivos da organização; e

— as relações com **partes interessadas** (2.13) externas e suas percepções e valores.

[ABNT ISO GUIA 73:2009, definição 3.3.1.1]

2.11
contexto interno
ambiente interno no qual a organização busca atingir seus objetivos

NOTA O contexto interno pode incluir:

— governança, estrutura organizacional, funções e responsabilidades;

— políticas, objetivos e estratégias implementadas para atingi-los;

— capacidades compreendidas em termos de recursos e conhecimento (por exemplo, capital, tempo, pessoas, processos, sistemas e tecnologias);

— sistemas de informação, fluxos de informação e processos de tomada de decisão (tanto formais como informais);

— relações com partes interessadas internas, e suas percepções e valores;

— cultura da organização;

— normas, diretrizes e modelos adotados pela organização; e

— forma e extensão das relações contratuais.

[ABNT ISO GUIA 73:2009, definição 3.3.1.2]

2.12
comunicação e consulta
processos contínuos e iterativos que uma organização conduz para fornecer, compartilhar ou obter informações e se envolver no diálogo com as **partes interessadas** (2.13) e outros, com relação a gerenciar **riscos** (2.1)

NOTA 1 As informações podem referir-se à existência, natureza, forma, **probabilidade** (2.19), significância, avaliação, aceitabilidade, tratamento ou outros aspectos da gestão de riscos.

NOTA 2 A consulta é um processo bidirecional de comunicação sistematizada entre uma organização e suas partes interessadas ou outros, antes de tomar uma decisão ou direcionar uma questão específica. A consulta é:

— um processo que impacta uma decisão através da influência ao invés do poder; e

— uma entrada para o processo de tomada de decisão, e não uma tomada de decisão em conjunto.

[ABNT ISO GUIA 73:2009, definição 3.2.1]

2.13
parte interessada
pessoa ou organização que pode afetar, ser afetada, ou perceber-se afetada por uma decisão ou atividade

NOTA Um tomador de decisão pode ser uma parte interessada.

[ABNT ISO GUIA 73:2009, definição 3.2.1.1]

2.14
processo de avaliação de riscos[2)]
processo global de **identificação de riscos** (2.15), **análise de riscos** (2.21) e **avaliação de riscos** (2.24)

[ABNT ISO GUIA 73:2009, definição 3.4.1]

2.15
identificação de riscos
processo de busca, reconhecimento e descrição de **riscos** (2.1)

NOTA 1 A identificação de riscos envolve a identificação das **fontes de risco** (2.16), **eventos** (2.17), suas causas e suas **consequências** (2.18) potenciais.

NOTA 2 A identificação de riscos pode envolver dados históricos, análises teóricas, opiniões de pessoas informadas e especialistas, e as necessidades das **partes interessadas** (2.13).

[ABNT ISO GUIA 73:2009, definição 3.5.1]

2.16
fonte de risco
elemento que, individualmente ou combinado, tem o potencial intrínseco para dar origem ao **risco** (2.1)

NOTA Uma fonte de risco pode ser tangível ou intangível.

[ABNT ISO GUIA 73:2009, definição 3.5.1.2]

2.17
evento
ocorrência ou mudança em um conjunto específico de circunstâncias

NOTA 1 Um evento pode consistir em uma ou mais ocorrências e pode ter várias causas.

NOTA 2 Um evento pode consistir em alguma coisa não acontecer.

NOTA 3 Um evento pode algumas vezes ser referido como um "incidente" ou um "acidente".

NOTA 4 Um evento sem **consequências** (2.18) também pode ser referido como um "quase acidente", ou um "incidente" ou "por um triz".

[ABNT ISO GUIA 73:2009, definição 3.5.1.3]

---

2) **NOTA DA TRADUÇÃO**: Para os efeitos desta Norma Brasileira, o termo *risk assessment* foi traduzido como "processo de avaliação de riscos" (2.14) para evitar conflito com o termo *risk evaluation,* que foi traduzido como "avaliação de riscos" (2.24).

2.18
consequência
resultado de um **evento** (2.17) que afeta os objetivos

NOTA 1 Um evento pode levar a uma série de consequências.

NOTA 2 Uma consequência pode ser certa ou incerta e pode ter efeitos positivos ou negativos sobre os objetivos.

NOTA 3 As consequências podem ser expressas qualitativa ou quantitativamente.

NOTA 4 As consequências iniciais podem desencadear reações em cadeia

[ABNT ISO GUIA 73:2009, definição 3.6.1.3]

2.19
probabilidade (*likelihood*)
chance de algo acontecer

NOTA 1 Na terminologia de gestão de riscos, a palavra "probabilidade" é utilizada para referir-se à chance de algo acontecer, não importando se definida, medida ou determinada objetiva ou subjetivamente, qualitativa ou quantitativamente, ou se descrita utilizando-se termos gerais ou matemáticos (tal como probabilidade ou frequência durante um determinado período de tempo).

NOTA 2 O termo em Inglês "*likelihood*" não tem um equivalente direto em algumas línguas; em vez disso, o equivalente do termo "*probability*" é freqüentemente utilizado. Entretanto, em Inglês, "*probability*" é muitas vezes interpretado estritamente como uma expressão matemática. Portanto, na terminologia de gestão de riscos, "*likelihood*" é utilizado com a mesma ampla interpretação de que o termo "*probability*" tem em muitos outros idiomas além do inglês.

[ABNT ISO GUIA 73:2009, definição 3.6.1.1]

2.20
perfil de risco
descrição de um conjunto qualquer de **riscos** (2.1)

NOTA O conjunto de riscos pode conter riscos que dizem respeito a toda a organização, parte da organização, ou referente ao qual tiver sido definido.

[ABNT ISO GUIA 73:2009, definição 3.8.2.5]

2.21
análise de riscos
processo de compreender a natureza do **risco** (2.1) e determinar o **nível de risco** (2.23)

NOTA 1 A análise de riscos fornece a base para a **avaliação de riscos** (2.24) e para as decisões sobre o **tratamento de riscos** (2.25).

NOTA 2 A análise de riscos inclui a estimativa de riscos.

[ABNT ISO GUIA 73:2009, definição 3.6.1]

2.22
critérios de risco
termos de referência contra os quais a significância de um **risco** (2.1) é avaliada

NOTA 1 Os critérios de risco são baseados nos objetivos organizacionais e no **contexto externo** (2.10) e **contexto interno** (2.11).

NOTA 2 Os critérios de risco podem ser derivados de normas, leis, políticas e outros requisitos.

[ABNT ISO GUIA 73:2009, definição 3.3.1.3]

2.23
nível de risco
magnitude de um **risco** (2.1) ou combinação de riscos, expressa em termos da combinação das **consequências** (2.18) e de suas **probabilidades** (2.19)

[ABNT ISO GUIA 73:2009, definição 3.6.1.8]

2.24
avaliação de riscos
processo de comparar os resultados da **análise de riscos** (2.21) com os **critérios de risco** (2.22) para determinar se o **risco** (2.1) e/ou sua magnitude é aceitável ou tolerável

NOTA A avaliação de riscos auxilia na decisão sobre o **tratamento de riscos** (2.25).

[ABNT ISO GUIA 73:2009, definição 3.7.1]

2.25
tratamento de riscos
processo para modificar o **risco** (2.1)

NOTA 1 O tratamento de risco pode envolver:

— a ação de evitar o risco pela decisão de não iniciar ou descontinuar a atividade que dá origem ao risco;

— assumir ou aumentar o risco, a fim de buscar uma oportunidade;

— a remoção da **fonte de risco** (2.16);

— a alteração da **probabilidade** (2.19);

— a alteração das **consequências** (2.18);

— o compartilhamento do risco com outra parte ou partes (incluindo contratos e financiamento do risco); e

— a retenção do risco por uma escolha consciente.

NOTA 2 Os tratamentos de riscos relativos às consequências negativas são muitas vezes referidos como "mitigação de riscos", "eliminação de riscos", "prevenção de riscos" e "redução de riscos".

NOTA 3 O tratamento de riscos pode criar novos riscos ou modificar riscos existentes.

[ABNT ISO GUIA 73:2009, definição 3.8.1]

2.26
controle
medida que está modificando o **risco** (2.1)

NOTA 1 Os controles incluem qualquer processo, política, dispositivo, prática ou outras ações que modificam o risco.

NOTA 2 Os controles nem sempre conseguem exercer o efeito de modificação pretendido ou presumido.

[ABNT ISO GUIA 73:2009, definição 3.8.1.1]

2.27
risco residual
risco (2.1) remanescente após o **tratamento do risco** (2.25)

NOTA 1 O risco residual pode conter riscos não identificados.

NOTA 2 O risco residual também pode ser conhecido como "risco retido".

[ABNT ISO GUIA 73:2009, definição 3.8.1.6]

2.28
monitoramento
verificação, supervisão, observação crítica ou identificação da situação, executadas de forma contínua, a fim de identificar mudanças no nível de desempenho requerido ou esperado

NOTA O monitoramento pode ser aplicado à **estrutura da gestão de riscos** (2.3), ao **processo de gestão de riscos** (2.8), ao **risco** (2.1) ou ao **controle** (2.26).

[ABNT ISO GUIA 73:2009, definição 3.8.2.1]

2.29
análise crítica
atividade realizada para determinar a adequação, suficiência e eficácia do assunto em questão para atingir os objetivos estabelecidos

NOTA A análise crítica pode ser aplicada à **estrutura da gestão de riscos** (2.3), ao **processo de gestão de riscos** (2.8), ao **risco** (2.1) ou ao **controle** (2.26).

[ABNT ISO GUIA 73:2009, definição 3.8.2.2]

3 Princípios

Para a gestão de riscos ser eficaz, convém que uma organização, em todos os níveis, atenda aos princípios abaixo descritos.

a) **A gestão de riscos cria e protege valor.**

A gestão de riscos contribui para a realização demonstrável dos objetivos e para a melhoria do desempenho referente, por exemplo, à segurança e saúde das pessoas, à segurança, à conformidade legal e regulatória, à aceitação pública, à proteção do meio ambiente, à qualidade do produto, ao gerenciamento de projetos, à eficiência nas operações, à governança e à reputação.

b) **A gestão de riscos é parte integrante de todos os processos organizacionais.**

A gestão de riscos não é uma atividade autônoma separada das principais atividades e processos da organização. A gestão de riscos faz parte das responsabilidades da administração e é parte integrante de todos os processos organizacionais, incluindo o planejamento estratégico e todos os processos de gestão de projetos e gestão de mudanças.

c) **A gestão de riscos é parte da tomada de decisões.**

A gestão de riscos auxilia os tomadores de decisão a fazer escolhas conscientes, priorizar ações e distinguir entre formas alternativas de ação.

d) **A gestão de riscos aborda explicitamente a incerteza.**

A gestão de riscos explicitamente leva em consideração a incerteza, a natureza dessa incerteza, e como ela pode ser tratada.

e) **A gestão de riscos é sistemática, estruturada e oportuna.**

Uma abordagem sistemática, oportuna e estruturada para a gestão de riscos contribui para a eficiência e para os resultados consistentes, comparáveis e confiáveis.

f) **A gestão de riscos baseia-se nas melhores informações disponíveis.**

As entradas para o processo de gerenciar riscos são baseadas em fontes de informação, tais como dados históricos, experiências, retroalimentação das partes interessadas, observações, previsões, e opiniões de especialistas. Entretanto, convém que os tomadores de decisão se informem e levem em consideração quaisquer limitações dos dados ou modelagem utilizados, ou a possibilidade de divergências entre especialistas.

g) **A gestão de riscos é feita sob medida.**

A gestão de riscos está alinhada com o contexto interno e externo da organização e com o perfil do risco.

h) **A gestão de riscos considera fatores humanos e culturais.**

A gestão de riscos reconhece as capacidades, percepções e intenções do pessoal interno e externo que podem facilitar ou dificultar a realização dos objetivos da organização.

i) **A gestão de riscos é transparente e inclusiva.**

O envolvimento apropriado e oportuno de partes interessadas e, em particular, dos tomadores de decisão em todos os níveis da organização assegura que a gestão de riscos permaneça pertinente e atualizada. O envolvimento também permite que as partes interessadas sejam devidamente representadas e terem suas opiniões levadas em consideração na determinação dos critérios de risco.

j) **A gestão de riscos é dinâmica, iterativa e capaz de reagir a mudanças.**

A gestão de riscos continuamente percebe e reage às mudanças. Na medida em que acontecem eventos externos e internos, o contexto e o conhecimento modificam-se, o monitoramento e a análise crítica de riscos são realizados, novos riscos surgem, alguns se modificam e outros desaparecem.

k) **A gestão de riscos facilita a melhoria contínua da organização.**

Convém que as organizações desenvolvam e implementem estratégias para melhorar a sua maturidade na gestão de riscos juntamente com todos os demais aspectos da sua organização.

O Anexo A fornece informações adicionais para as organizações que desejam gerenciar riscos de forma mais eficaz.

4 Estrutura

4.1 Generalidades

O sucesso da gestão de riscos irá depender da eficácia da estrutura de gestão que fornece os fundamentos e os arranjos que irão incorporá-la através de toda a organização, em todos os níveis. A estrutura auxilia a gerenciar riscos eficazmente através da aplicação do processo de gestão de riscos (ver Seção 5) em diferentes níveis e dentro de contextos específicos da organização. A estrutura assegura que a informação sobre riscos proveniente desse processo seja adequadamente reportada e utilizada como base para a tomada de decisões e a responsabilização em todos os níveis organizacionais aplicáveis.

Esta seção descreve os componentes necessários da estrutura para gerenciar riscos e a forma como eles se inter-relacionam de maneira iterativa, conforme mostrado na Figura 2.

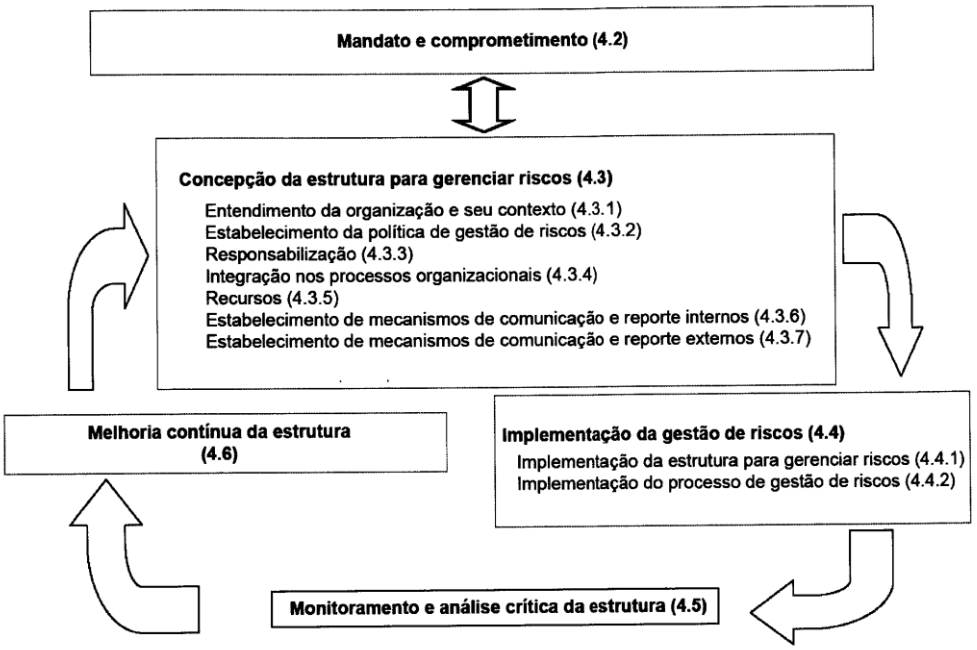

Figura 2 — Relacionamento entre os componentes da estrutura para gerenciar riscos

Esta estrutura não pretende prescrever um sistema de gestão, mas antes auxiliar a organização a integrar a gestão de riscos em seu sistema de gestão global. Portanto, convém que as organizações adaptem os componentes da estrutura a suas necessidades específicas.

Se as práticas e processos de gestão existentes em uma organização incluirem componentes de gestão de riscos ou se a organização tiver já adotado um processo formal de gestão de riscos para determinados tipos ou situações de risco, então convém que estes sejam criticamente analisados e avaliados em relação a esta Norma, incluindo os atributos contidos no Anexo A, a fim de determinar sua suficiência e eficácia.

4.2 Mandato e comprometimento

A introdução da gestão de riscos, e a garantia de sua contínua eficácia requerem comprometimento forte e sustentado a ser assumido pela administração da organização, bem como um planejamento rigoroso e estratégico para obter-se esse comprometimento em todos os níveis. Convém que a administração:

— defina e aprove a política de gestão de riscos;

— assegure que a cultura da organização e a política de gestão de riscos estejam alinhadas;

— defina indicadores de desempenho para a gestão de riscos que estejam alinhados com os indicadores de desempenho da organização;

— alinhe os objetivos da gestão de riscos com os objetivos e estratégias da organização;

— assegure a conformidade legal e regulatória;

— atribua responsabilidades nos níveis apropriados dentro da organização;

— assegure que os recursos necessários sejam alocados para a gestão de riscos;

— comunique os benefícios da gestão de riscos a todas as partes interessadas; e

— assegure que a estrutura para gerenciar riscos continue a ser apropriada.

4.3 Concepção da estrutura para gerenciar riscos

4.3.1 Entendimento da organização e seu contexto

Antes de iniciar a concepção e a implementação da estrutura para gerenciar riscos, é importante avaliar e compreender os contextos externo e interno da organização, uma vez que estes podem influenciar significativamente a concepção da estrutura.

A avaliação do contexto externo da organização pode incluir, mas não está limitada a:

a) ambientes cultural, social, político, legal, regulatório, financeiro, tecnológico, econômico, natural e competitivo, quer seja internacional, nacional, regional ou local;

b) fatores–chave e tendências que tenham impacto sobre os objetivos da organização; e

c) relações com partes interessadas externas e suas percepções e valores.

A avaliação do contexto interno da organização pode incluir, mas não está limitada a:

— governança, estrutura organizacional, funções e responsabilidades;

— políticas, objetivos e estratégias implementadas para atingi-los;

— capacidades, entendidas em termos de recursos e conhecimento (por exemplo, capital, tempo, pessoas, processos, sistemas e tecnologias);

— sistemas de informação, fluxos de informação e processos de tomada de decisão (formais e informais);

— relações com partes interessadas internas e suas percepções e valores;

— cultura da organização;

— normas, diretrizes e modelos adotados pela organização; e

— forma e extensão das relações contratuais.

4.3.2 Estabelecimento da política de gestão de riscos

Convém que a política de gestão de riscos estabeleça claramente os objetivos e o comprometimento da organização em relação à gestão de riscos e, tipicamente, aborde:

— a justificativa da organização para gerenciar riscos;

— as ligações entre os objetivos e políticas da organização com a política de gestão de riscos;

— as responsabilidades para gerenciar riscos;

— a forma com que são tratados conflitos de interesses;

— o comprometimento de tornar disponíveis os recursos necessários para auxiliar os responsáveis pelo gerenciamento dos riscos;

— a forma com que o desempenho da gestão de riscos será medido e reportado; e

— o comprometimento de analisar criticamente e melhorar periodicamente a política e a estrutura da gestão de riscos em resposta a um evento ou mudança nas circunstâncias.

Convém que a política de gestão de riscos seja comunicada apropriadamente.

4.3.3 Responsabilização

Convém que a organização assegure que haja responsabilização, autoridade e competência apropriadas para gerenciar riscos, incluindo implementar e manter o processo de gestão de riscos, e assegurar a suficiência, a eficácia e a eficiência de quaisquer controles. Isto pode ser facilitado por:

— identificar os proprietários dos riscos que têm a responsabilidade e a autoridade para gerenciar riscos;

— identificar os responsáveis pelo desenvolvimento, implementação e manutenção da estrutura para gerenciar riscos;

— identificar outras responsabilidades das pessoas, em todos os níveis da organização no processo de gestão de riscos;

— estabelecer medição de desempenho e processos de reporte internos ou externos e relação com os devidos escalões; e

— assegurar níveis apropriados de reconhecimento.

4.3.4 Integração nos processos organizacionais

Convém que a gestão de riscos seja incorporada em todas as práticas e processos da organização, de forma que seja pertinente, eficaz e eficiente. Convém que o processo de gestão de riscos se torne parte integrante, e não separado, desses processos organizacionais. Em particular, convém que a gestão de riscos seja incorporada no desenvolvimento de políticas, na análise crítica, no planejamento estratégico e de negócios, e nos processos de gestão de mudanças.

Convém que exista um plano de gestão de riscos para toda a organização, a fim de assegurar que a política de gestão de riscos seja implementada e que a gestão de riscos seja incorporada em todas as práticas e processos da organização. O plano de gestão de riscos pode ser integrado em outros planos organizacionais, tais como um plano estratégico.

4.3.5 Recursos

Convém que a organização aloque recursos apropriados para a gestão de riscos.

Convém que os seguintes aspectos sejam considerados:

— pessoas, habilidades, experiências e competências;

— recursos necessários para cada etapa do processo de gestão de riscos;

— processos, métodos e ferramentas da organização para serem utilizados para gerenciar riscos;

— processos e procedimentos documentados;

— sistemas de gestão da informação e do conhecimento; e

— programas de treinamento.

4.3.6 Estabelecimento de mecanismos de comunicação e reporte internos

Convém que a organização estabeleça mecanismos de comunicação interna e reporte a fim de apoiar e incentivar a responsabilização e a propriedade dos riscos. Convém que tais mecanismos assegurem que:

— componentes-chave da estrutura da gestão de riscos, e quaisquer alterações subsequentes, sejam comunicados adequadamente;

— exista um processo adequado de reporte interno sobre a estrutura, sua eficácia e os seus resultados;

— as informações pertinentes derivadas da aplicação da gestão de riscos estejam disponíveis nos níveis e nos momentos apropriados; e

— haja processos de consulta às partes interessadas internas.

Convém que estes mecanismos incluam processos para consolidar a informação sobre os riscos, conforme apropriado, a partir de uma variedade de fontes, levando em consideração sua sensibilidade.

4.3.7 Estabelecimento de mecanismos de comunicação e reporte externos

Convém que a organização desenvolva e implemente um plano sobre como se comunicará com partes interessadas externas. Convém que isto envolva:

— engajar as partes interessadas externas apropriadas e assegurar a troca eficaz de informações;

— o reporte externo para atendimento de requisitos legais, regulatórios e de governança;

— fornecer retroalimentação e reportar sobre a comunicação e consulta;

— usar comunicação para construir confiança na organização; e

— comunicar as partes interessadas em evento de crise ou contingência.

Convém que estes mecanismos incluam processos para consolidar a informação sobre os riscos, conforme apropriado, a partir de uma variedade de fontes, levando em consideração sua sensibilidade.

4.4 Implementação da gestão de riscos

4.4.1 Implementação da estrutura para gerenciar riscos

Na implementação da estrutura para gerenciar riscos, convém que a organização:

— defina a estratégia e o momento apropriado para implementação da estrutura;

— aplique a política e o processo de gestão de riscos aos processos organizacionais;

— atenda aos requisitos legais e regulatórios;

— assegure que a tomada de decisões, incluindo o desenvolvimento e o estabelecimento de objetivos, esteja alinhada com os resultados dos processos de gestão de riscos;

— mantenha sessões de informação e treinamento; e

— consulte e comunique-se com as partes interessadas para assegurar que a estrutura da gestão de riscos continue apropriada.

4.4.2 Implementação do processo de gestão de riscos

Convém que a gestão de riscos seja implementada para assegurar que o processo de gestão de riscos descrito na Seção 5 seja aplicado, através de um plano de gestão de riscos, em todos os níveis e funções pertinentes da organização, como parte de suas práticas e processos.

4.5 Monitoramento e análise crítica da estrutura

A fim de assegurar que a gestão de riscos seja eficaz e continua a apoiar o desempenho organizacional, convém que a organização:

— meça o desempenho da gestão de riscos utilizando indicadores, os quais devem ser analisados criticamente, de forma periódica, para garantir sua adequação;

— meça periodicamente o progresso obtido, ou o desvio, em relação ao plano de gestão de riscos;

— analise criticamente de forma periódica se a política, o plano e a estrutura da gestão de riscos ainda são apropriados, dado o contexto externo e interno das organizações;

— reporte sobre os riscos, sobre o progresso do plano de gestão de riscos e como a política de gestão de riscos está sendo seguida; e

— analise criticamente a eficácia da estrutura da gestão de riscos.

4.6 Melhoria contínua da estrutura

Com base nos resultados do monitoramento e das análises críticas, convém que decisões sejam tomadas sobre como a política, o plano e a estrutura da gestão de riscos podem ser melhorados. Convém que essas decisões visem melhorias na capacidade de gerenciar riscos da organização e em sua cultura de gestão de riscos.

5 Processo

5.1 Generalidades

Convém que o processo de gestão de riscos seja

— parte integrante da gestão,

— incorporado na cultura e nas práticas, e

— adaptado aos processos de negócios da organização.

Ele compreende as atividades descritas em 5.2 a 5.6. O processo de gestão de riscos é mostrado na Figura 3.

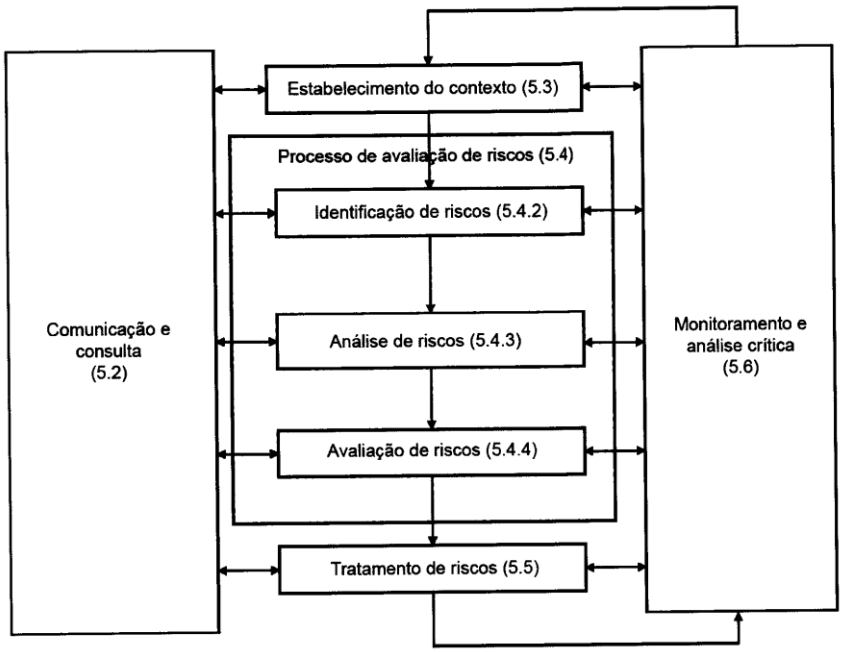

Figura 3 — Processo de gestão de riscos

5.2 Comunicação e consulta

Convém que a comunicação e a consulta às partes interessadas internas e externas aconteçam durante todas as fases do processo de gestão de riscos.

Portanto, convém que os planos de comunicação e consulta sejam desenvolvidos em um estágio inicial. Convém que estes planos abordem questões relacionadas com o risco propriamente dito, suas causas, suas consequências (se conhecidas) e as medidas que estão sendo tomadas para tratá-los. Convém que comunicação e consulta interna e externa eficazes sejam realizadas a fim de assegurar que os responsáveis pela implementação do processo de gestão de riscos e as partes interessadas compreendam os fundamentos sobre os quais as decisões são tomadas e as razões pelas quais ações específicas são requeridas.

Uma abordagem de equipe consultiva pode:

— auxiliar a estabelecer o contexto apropriadamente;

— assegurar que os interesses das partes interessadas sejam compreendidos e considerados;

— auxiliar a assegurar que os riscos sejam identificados adequadamente;

— reunir diferentes áreas de especialização em conjunto para análise dos riscos;

— assegurar que diferentes pontos de vista sejam devidamente considerados quando da definição dos critérios de risco e na avaliação dos riscos;

— garantir o aval e o apoio para um plano de tratamento;

— aprimorar a gestão de mudanças durante o processo de gestão de riscos; e

— desenvolver um plano apropriado para comunicação e consulta interna e externa.

A comunicação e consulta às partes interessadas são importantes na medida em que elas fazem julgamentos sobre riscos com base em suas percepções. Essas percepções podem variar devido às diferenças de valores, necessidades, suposições, conceitos e preocupações das partes interessadas. Como os seus pontos de vista podem ter um impacto significativo sobre as decisões tomadas, convém que as percepções das partes interessadas sejam identificadas, registradas e levadas em consideração no processo de tomada de decisão.

Convém que a comunicação e a consulta facilitem a troca de informações verdadeiras, pertinentes, exatas e compreensíveis, levando em consideração os aspectos de confidencialidade e integridade das pessoas.

5.3 Estabelecimento do contexto

5.3.1 Generalidades

Ao estabelecer o contexto, a organização articula seus objetivos, define os parâmetros externos e internos a serem levados em consideração ao gerenciar riscos, e estabelece o escopo e os critérios de risco para o restante do processo. Mesmo que muitos destes parâmetros sejam similares àqueles considerados na concepção da estrutura da gestão de riscos (ver 4.3.1), ao se estabelecer o contexto para o processo de gestão de riscos, eles precisam ser considerados com mais detalhe. Em particular, como eles se relacionam com o escopo do respectivo processo de gestão de riscos.

5.3.2 Estabelecimento do contexto externo

O contexto externo é o ambiente externo no qual a organização busca atingir seus objetivos.

Entender o contexto externo é importante para assegurar que os objetivos e as preocupações das partes interessadas externas sejam considerados no desenvolvimento dos critérios de risco. O contexto externo é baseado no contexto de toda a organização, porém com detalhes específicos sobre requisitos legais e regulatórios, percepções de partes interessadas e outros aspectos dos riscos específicos para o escopo do processo de gestão de riscos.

O contexto externo pode incluir, mas não está limitado a:

— ambientes cultural, social, político, legal, regulatório, financeiro, tecnológico, econômico, natural e competitivo, quer seja internacional, nacional, regional ou local;

— fatores–chave e tendências que tenham impacto sobre os objetivos da organização; e

— relações com as partes interessadas externas e suas percepções e valores.

5.3.3 Estabelecimento do contexto interno

O contexto interno é o ambiente interno no qual a organização busca atingir seus objetivos.

Convém que o processo de gestão de riscos esteja alinhado com a cultura, processos, estrutura e estratégia da organização. O contexto interno é algo dentro da organização que pode influenciar a maneira pela qual uma organização gerenciará os riscos. Convém que ele seja estabelecido, porque:

a) a gestão de riscos ocorre no contexto dos objetivos da organização;

b) convém que os objetivos e os critérios de um determinado projeto, processo ou atividade sejam considerados tendo como base os objetivos da organização como um todo; e

c) algumas organizações deixam de reconhecer oportunidades para atingir seus objetivos estratégicos, de projeto ou de negócios, o que afeta o comprometimento, a credibilidade, a confiança e o valor organizacional.

É necessário compreender o contexto interno. Isto pode incluir, mas não está limitado a:

— governança, estrutura organizacional, funções e responsabilidades;

— políticas, objetivos e estratégias implementadas para atingi-los;

— capacidades, entendidas em termos de recursos e conhecimento (por exemplo, capital, tempo, pessoas, processos, sistemas e tecnologias);

— sistemas de informação, fluxos de informação e processos de tomada de decisão (formais e informais);

— relações com as partes interessadas internas, e suas percepções e valores;

— cultura da organização;

— normas, diretrizes e modelos adotados pela organização, e

— forma e extensão das relações contratuais.

5.3.4 Estabelecimento do contexto do processo de gestão de riscos

Convém que sejam estebelecidos os objetivos, as estratégias, o escopo e os parâmetros das atividades da organização, ou daquelas partes da organização em que o processo de gestão de riscos está sendo aplicado. Convém que a gestão dos riscos seja realizada com plena consciência da necessidade de justificar os recursos utilizados na gestão de riscos. Convém que os recursos requeridos, as responsabilidades e as autoridades, além dos registros a serem mantidos, também sejam especificados.

O contexto do processo de gestão de riscos irá variar de acordo com as necessidades de uma organização. Ele pode envolver, mas não está limitado a:

— definição das metas e objetivos das atividades de gestão de riscos;

— definição das responsabilidades pelo processo e dentro da gestão de riscos;

— definição do escopo, bem como da profundidade e da amplitude das atividades da gestão de riscos a serem realizadas, englobando inclusões e exclusões específicas;

— definição da atividade, processo, função, projeto, produto, serviço ou ativo em termos de tempo e localização;

— definição das relações entre um projeto, processo ou atividade específicos e outros projetos, processos ou atividades da organização;

— definição das metodologias de processo de avaliação de riscos;

— definição da forma como são avaliados o desempenho e a eficácia na gestão dos riscos;

— identificação e especificação das decisões que têm que ser tomadas; e

— identificação, definição ou elaboração dos estudos necessários, de sua extensão e objetivos, e dos recursos requeridos para tais estudos.

A atenção para estes e outros fatores pertinentes pode ajudar a assegurar que a abordagem adotada para a gestão de riscos seja apropriada às circunstâncias, à organização e aos riscos que afetam a realização de seus objetivos.

5.3.5 Definição dos critérios de risco

Convém que a organização defina os critérios a serem utilizados para avaliar a significância do risco. Convém que os critérios reflitam os valores, objetivos e recursos da organização. Alguns critérios podem ser impostos por, ou derivados de requisitos legais e regulatórios e outros requisitos que a organização subscreva. Convém que os critérios de risco sejam compatíveis com a política de gestão de riscos da organização (ver 4.3.2), definidos no início de qualquer processo de gestão de riscos e analisados criticamente de forma contínua.

Ao definir os critérios de risco, convém que os fatores a serem considerados incluam os seguintes aspectos:

— a natureza e os tipos de causas e de consequências que podem ocorrer e como elas serão medidas;

— como a probabilidade será definida;

— a evolução no tempo da probabilidade e/ou consequência(s);

— como o nível de risco deve ser determinado;

— os pontos de vista das partes interessadas;

— o nível em que o risco se torna aceitável ou tolerável; e

— se convém que combinações de múltiplos riscos sejam levadas em consideração e, em caso afirmativo, como e quais combinações convém que sejam consideradas.

5.4 Processo de avaliação de riscos

5.4.1 Generalidades

O processo de avaliação de riscos é o processo global de identificação de riscos, análise de riscos e avaliação de riscos.

NOTA A IEC 31010 fornece orientação sobre técnicas de processo de avaliação de riscos.

5.4.2 Identificação de riscos

Convém que a organização identifique as fontes de risco, áreas de impactos, eventos (incluindo mudanças nas circunstâncias) e suas causas e consequências potenciais. A finalidade desta etapa é gerar uma lista abrangente de riscos baseada nestes eventos que possam criar, aumentar, evitar, reduzir, acelerar ou atrasar a realização dos objetivos. É importante identificar os riscos associados com não perseguir uma oportunidade. A identificação abrangente é crítica, pois um risco que não é identificado nesta fase não será incluído em análises posteriores.

Convém que a identificação inclua todos os riscos, estando suas fontes sob o controle da organização ou não, mesmo que as fontes ou causas dos riscos possam não ser evidentes. Convém que a identificação de riscos inclua o exame de reações em cadeia provocadas por consequências específicas, incluindo os efeitos cumulativos e em cascata. Convém que também seja considerada uma ampla gama de consequências, ainda que a fonte ou causa do risco não esteja evidente. Além de identificar o que pode acontecer, é necessário considerar possíveis causas e cenários que mostrem quais consequências podem ocorrer. Convém que todas as causas e consequências significativas sejam consideradas.

Convém que a organização aplique ferramentas e técnicas de identificação de riscos que sejam adequadas aos seus objetivos e capacidades e aos riscos enfrentados. Informações pertinente e atualizadas são importantes na identificação de riscos. Convém que incluam informações adequadas sobre os fatos por trás dos acontecimentos, sempre que possível. Convém que pessoas com um conhecimento adequado sejam envolvidas na identificação dos riscos.

5.4.3 Análise de riscos

A análise de riscos envolve desenvolver a compreensão dos riscos. A análise de riscos fornece uma entrada para a avaliação de riscos e para as decisões sobre a necessidade dos riscos serem tratados, e sobre as estratégias e métodos mais adequados de tratamento de riscos. A análise de riscos também pode fornecer uma entrada para a tomada de decisões em que escolhas precisam ser feitas e as opções envolvem diferentes tipos e níveis de risco.

A análise de riscos envolve a apreciação das causas e as fontes de risco, suas consequências positivas e negativas, e a probabilidade de que essas consequências possam ocorrer. Convém que os fatores que afetam as consequências e a probabilidade sejam identificados. O risco é analisado determinando–se as conseqüências e sua probabilidade, e outros atributos do risco. Um evento pode ter várias consequências e pode afetar vários objetivos. Convém que os controles existentes e sua eficácia e eficiência também sejam levados em consideração.

Convém que a forma em que as consequências e a probabilidade são expressas e o modo com que elas são combinadas para determinar um nível de risco reflitam o tipo de risco, as informações disponíveis e a finalidade para a qual a saída do processo de avaliação de riscos será utilizada. Convém que isso tudo seja compatível com os critérios de risco. É também importante considerar a interdependência dos diferentes riscos e suas fontes.

Convém que a confiança na determinação do nível de risco e sua sensibilidade a condições prévias e premissas sejam consideradas na análise e comunicadas eficazmente para os tomadores de decisão e, quando apropriado, a outras partes interessadas. Convém que sejam estabelecidos e ressaltados fatores como a divergência de opinião entre especialistas, a incerteza, a disponibilidade, a qualidade, a quantidade e a contínua pertinência das informações, ou as limitações sobre a modelagem.

A análise de riscos pode ser realizada com diversos graus de detalhe, dependendo do risco, da finalidade da análise e das informações, dados e recursos disponíveis. Dependendo das circunstâncias, a análise pode ser qualitativa, semiquantitativa ou quantitativa, ou uma combinação destas.

As consequências e suas probabilidades podem ser determinadas por modelagem dos resultados de um evento ou conjunto de eventos, ou por extrapolação a partir de estudos experimentais ou a partir dos dados disponíveis. As consequências podem ser expressas em termos de impactos tangíveis e intangíveis. Em alguns casos, é necessário mais que um valor numérico ou descritor para especificar as consequências e suas probabilidades em diferentes períodos, locais, grupos ou situações.

5.4.4 Avaliação de riscos

A finalidade da avaliação de riscos é auxiliar na tomada de decisões com base nos resultados da análise de riscos, sobre quais riscos necessitam de tratamento e a prioridade para a implementação do tratamento.

A avaliação de riscos envolve comparar o nível de risco encontrado durante o processo de análise com os critérios de risco estabelecidos quando o contexto foi considerado. Com base nesta comparação, a necessidade do tratamento pode ser considerada.

Convém que as decisões levem em conta o contexto mais amplo do risco e considerem a tolerância aos riscos assumida por partes que não a própria organização que se beneficia do risco. Convém que as decisões sejam tomadas de acordo com os requisitos legais, regulatórios e outros requisitos.

Em algumas circunstâncias, a avaliação de riscos pode levar à decisão de se proceder a uma análise mais aprofundada. A avaliação de riscos também pode levar à decisão de não se tratar o risco de nenhuma outra forma que seja manter os controles existentes. Esta decisão será influenciada pela atitude perante o risco da organização e pelos critérios de risco que foram estabelecidos.

5.5 Tratamento de riscos

5.5.1 Generalidades

O tratamento de riscos envolve a seleção de uma ou mais opções para modificar os riscos e a implementação dessas opções. Uma vez implementado, o tratamento fornece novos controles ou modifica os existentes.

Tratar riscos envolve um processo cíclico composto por:

— avaliação do tratamento de riscos já realizado;

— decisão se os níveis de risco residual são toleráveis;

— se não forem toleráveis, a definição e implementação de um novo tratamento para os riscos; e

— avaliação da eficácia desse tratamento.

As opções de tratamento de riscos não são necessariamente mutuamente exclusivas ou adequadas em todas as circunstâncias. As opções podem incluir os seguintes aspectos:

a) ação de evitar o risco ao se decidir não iniciar ou descontinuar a atividade que dá origem ao risco;

b) tomada ou aumento do risco na tentativa de tirar proveito de uma oportunidade;

c) remoção da fonte de risco;

d) alteração da probabilidade;

e) alteração das consequências;

f) compartilhamento do risco com outra parte ou partes (incluindo contratos e financiamento do risco); e

g) retenção do risco por uma decisão consciente e bem embasada.

5.5.2 Seleção das opções de tratamento de riscos

Selecionar a opção mais adequada de tratamento de riscos envolve equilibrar, de um lado, os custos e os esforços de implementação e, de outro, os benefícios decorrentes, relativos a requisitos legais, regulatórios ou quaisquer outros, tais como o da responsabilidade social e o da proteção do ambiente natural. Convém que as decisões também levem em consideração os riscos que demandam um tratamento economicamente não justificável, como, por exemplo, riscos severos (com grande consequência negativa), porém raros (com probabilidade muito baixa).

Várias opções de tratamento podem ser consideradas e aplicadas individualmente ou combinadas. A organização, normalmente, beneficia-se com a adoção de uma combinação de opções de tratamento.

Ao selecionar as opções de tratamento de riscos, convém que a organização considere os valores e as percepções das partes interessadas, e as formas mais adequadas para se comunicar com elas. Quando as opções de tratamento de riscos podem afetar o risco no resto da organização ou com as partes interessadas, convém que todos os envolvidos participem da decisão. Embora igualmente eficazes, alguns tratamentos podem ser mais aceitáveis para algumas das partes interessadas do que para outras.

Convém que o plano de tratamento identifique claramente a ordem de prioridade em que cada tratamento deva ser implementado.

O tratamento de riscos, por si só, pode introduzir riscos. Um risco significativo pode derivar do fracasso ou da ineficácia das medidas de tratamento de riscos. O monitoramento precisa fazer parte do plano de tratamento de forma a garantir que as medidas permaneçam eficazes.

O tratamento de riscos também pode introduzir riscos secundários que necessitam ser avaliados, tratados, monitorados e analisados criticamente. Convém que esses riscos secundários sejam incorporados no mesmo plano de tratamento do risco original e não tratados como um novo risco. Convém que a ligação entre estes riscos seja identificada e preservada.

5.5.3 Preparando e implementando planos para tratamento de riscos

A finalidade dos planos de tratamento de riscos é documentar como as opções de tratamento escolhidas serão implementadas. Convém que as informações fornecidas nos planos de tratamento incluam:

— as razões para a seleção das opções de tratamento, incluindo os benefícios que se espera obter;

— os responsáveis pela aprovação do plano e os responsáveis pela implementação do plano;

— ações propostas;

— os recursos requeridos, incluindo contingências;

— medidas de desempenho e restrições;

— requisitos para a apresentação de informações e de monitoramento; e

— cronograma e programação.

Convém que os planos de tratamento sejam integrados com os processos de gestão da organização e discutidos com as partes interessadas apropriadas.

Convém que os tomadores de decisão e outras partes interessadas estejam cientes da natureza e da extensão do risco residual após o tratamento do risco. Convém que o risco residual seja documentado e submetido a monitoramento, análise crítica e, quando apropriado, a tratamento adicional.

5.6 Monitoramento e análise crítica

Convém que o monitoramento e a análise crítica sejam planejados como parte do processo de gestão de riscos e envolvam a checagem ou vigilância regulares. Podem ser periódicos ou acontecer em resposta a um fato específico.

Convém que as responsabilidades relativas ao monitoramento e à análise crítica sejam claramente definidas.

Convém que os processos de monitoramento e análise crítica da organização abranjam todos os aspectos do processo da gestão de riscos com a finalidade de:

— garantir que os controles sejam eficazes e eficientes no projeto e na operação;

— obter informações adicionais para melhorar o processo de avaliação dos riscos;

— analisar os eventos (incluindo os "quase incidentes"), mudanças, tendências, sucessos e fracassos e aprender com eles;

— detectar mudanças no contexto externo e interno, incluindo alterações nos critérios de risco e no próprio risco, as quais podem requerer revisão dos tratamentos dos riscos e suas prioridades; e

— identificar os riscos emergentes.

O progresso na implementação dos planos de tratamento de riscos proporciona uma medida de desempenho. Os resultados podem ser incorporados na gestão, na mensuração e na apresentação de informações (tanto externa quanto internamente) a respeito do desempenho global da organização.

Convém que os resultados do monitoramento e da análise crítica sejam registrados e reportados externa e internamente conforme apropriado, e também convém que sejam utilizados como entrada para a análise crítica da estrutura de gestão de riscos (ver 4.5).

5.7 Registros do processo de gestão de riscos

Convém que as atividades de gestão de riscos sejam rastreáveis. No processo de gestão de riscos, os registros fornecem os fundamentos para a melhoria dos métodos e ferramentas, bem como de todo o processo.

Convém que as decisões relativas à criação de registros levem em consideração:

— a necessidade da organização de aprendizado contínuo;

— os benefícios da reutilização de informações para fins de gestão;

— os custos e os esforços envolvidos na criação e manutenção de registros;

— as necessidades de registros legais, regulatórios e operacionais;

— o método de acesso, facilidade de recuperação e meios de armazenamento;

— o período de retenção; e

— a sensibilidade das informações.

Anexo A
(infomativo)

Atributos de uma gestão de riscos avançada

A.1 Generalidades

Convém que as organizações visem um nível de desempenho apropriado de sua estrutura da gestão de riscos em consonância com a criticidade das decisões a serem tomadas. A lista de atributos abaixo representa um nível alto de desempenho para gerenciar riscos. Para auxiliar as organizações a medir seu próprio desempenho a partir desses critérios, alguns indicadores tangíveis são fornecidos para cada atributo.

A.2 Resultados-chave

A.2.1 A organização tem um entendimento atual, correto e abrangente de seus riscos.

A.2.2 Os riscos da organização estão dentro de seus critérios de risco.

A.3 Atributos

A.3.1 Melhoria contínua

A ênfase é colocada sobre a melhoria contínua na gestão de riscos através do estabelecimento de metas de desempenho organizacional, através da mensuração e de análises críticas, além das subsequentes mudanças de processos, sistemas, recursos, capacidade e habilidades.

Isso pode ser indicado pela existência de metas explícitas de desempenho contra as quais o desempenho da gerência individual e da organização é medido. O desempenho da organização pode ser publicado e comunicado. Normalmente, haverá pelo menos uma análise crítica anual de desempenho e, em seguida, uma revisão de processos e o estabelecimento de objetivos de desempenho revisados para o período seguinte.

Esta avaliação de desempenho da gestão dos riscos é parte integrante do sistema corporativo de avaliação e mensuração do desempenho de departamentos e indivíduos.

A.3.2 Responsabilização integral pelos riscos

Formas avançadas de gestão de riscos incluem uma forma de responsabilização abrangente, integralmente aceita e muito bem definida, relativa aos riscos, controles e tarefas do tratamento dos riscos. Indivíduos designados aceitam suas responsabilidades, são adequadamente qualificados, e possuem recursos adequados para verificar controles, monitorar riscos, melhorar os controles, e comunicar-se eficazmente com as partes interessadas internas e externas sobre os riscos e sua gestão.

Isto pode ser indicado quando todos os membros de uma organização estão totalmente conscientes dos riscos, controles e tarefas para os quais são responsáveis. Normalmente, isso estará registrado em descrições de cargo/posição, em bancos de dados ou sistemas de informação. Convém que a definição das funções e responsabilidades relativas à gestão dos riscos faça parte de todos os programas de formação da organização.

A organização assegura que aqueles responsáveis estão equipados para desempenhar completamente as suas funções, fornecendo-lhes a autoridade, tempo, treinamento, recursos e habilidades suficientes para assumirem suas responsabilidades.

A.3.3 Aplicação da gestão de riscos em todas as tomadas de decisão

O processo de tomada de decisão dentro da organização, seja qual for o nível de sua importância e significância, envolve explicitamente a consideração dos riscos e aplicação da gestão de riscos em algum grau apropriado.

Isto pode ser indicado por registros de reuniões e decisões que demonstrem que discussões explícitas sobre os riscos ocorreram. Além disso, convém que seja possível ver que todos os componentes da gestão de riscos estão representados dentro dos processos-chave para a tomada de decisão na organização, por exemplo, para as decisões sobre a alocação de capital, sobre grandes projetos e sobre reestruturação e mudanças organizacionais. Por estas razões, uma base sólida de gestão de riscos é vista dentro da organização como fornecendo a base para a governança eficaz.

A.3.4 Comunicação contínua

Formas avançadas de gestão de riscos incluem comunicações contínuas com partes interessadas internas e externas, incluindo informativos ou relatórios abrangentes e freqüentes a respeito do desempenho da gestão de riscos, como parte da boa governança.

Isto pode ser indicado pela comunicação com as partes interessadas como parte integrante e essencial da gestão de riscos. A comunicação é corretamente vista como um processo bidirecional, de tal forma que decisões bem informadas possam ser tomadas sobre o nível de riscos e sobre a necessidade de tratamento, de acordo com critérios de risco abrangentes e adequadamente estabelecidos.

Reportes externos e internos, abrangentes e freqüentes, sobre os riscos significativos e sobre o desempenho da gestão de riscos, contribuem substancialmente para uma governança eficaz dentro de uma organização.

A.3.5 Integração total na estrutura de governança da organização

A gestão de riscos é vista como central nos processos de gestão da organização, de tal forma que os riscos sejam considerados em termos do efeito da incerteza sobre os objetivos. O processo e a estrutura de governança são baseados na gestão de riscos. A gestão de riscos eficaz é considerada por gestores como sendo essencial para a realização dos objetivos da organização.

Isto é indicado pela linguagem dos gestores e por importantes materiais escritos na organização que utilizam o termo "incerteza" em conexão com riscos. Esse atributo normalmente também aparece refletido nas declarações de política da organização, em especial as relativas à gestão de riscos. Normalmente, esse atributo é verificado por meio de entrevistas com gestores e da evidência de suas ações e declarações.