NORMA
BRASILEIRA

ABNT NBR ISO 31000

Segunda edição
28.03.2018

Gestão de riscos — Diretrizes

Risk management — Guidelines

ICS 03.100.01

ISBN 978-85-07-07470-0

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS

Número de referência
ABNT NBR ISO 31000:2018
17 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

Página

Figuras

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 pelas partes interessadas no tema objeto da normalização.

Os Documentos Técnicos Internacionais são adotados conforme as regras da ABNT Diretiva 3.

A ABNT chama a atenção para que, apesar de ter sido solicitada manifestação sobre eventuais direitos de patentes durante a Consulta Nacional, estes podem ocorrer e devem ser comunicados à ABNT a qualquer momento (Lei nº 9.279, de 14 de maio de 1996).

Ressalta-se que Normas Brasileiras podem ser objeto de citação em Regulamentos Técnicos. Nestes casos, os órgãos responsáveis pelos Regulamentos Técnicos podem determinar outras datas para exigência dos requisitos desta Norma.

A ABNT NBR ISO 31000 foi elaborada na Comissão de Estudo Especial de Gestão de Riscos (ABNT/CEE-063). O Projeto circulou em Consulta Nacional conforme Edital nº 02, de 07.02.2018 a 08.03.2018.

Esta Norma é uma adoção idêntica, em conteúdo técnico, estrutura e redação, à ISO 31000:2018, que foi elaborada pelo *Technical Committee Risk Management* (ISO/TC 262), conforme ISO/IEC Guide 21-1:2005.

Esta segunda edição cancela e substitui a edição anterior (ABNT NBR ISO 31000:2009), a qual foi tecnicamente revisada.

O Escopo em inglês desta Norma Brasileira é o seguinte:

Scope

This document provides guidelines on managing risk faced by organizations. The application of these guidelines can be customized to any organization and its context.

This document provides a common approach to managing any type of risk and is not industry or sector specific.

Introdução

Este documento é para uso por pessoas que criam e protegem valor nas organizações, gerenciando riscos, tomando decisões, estabelecendo e alcançando objetivos e melhorando o desempenho.

Organizações de todos os tipos e tamanhos enfrentam influências e fatores externos e internos que tornam incerto se elas alcançarão seus objetivos.

Gerenciar riscos é iterativo e auxilia as organizações no estabelecimento de estratégias, no alcance de objetivos e na tomada de decisões fundamentadas.

Gerenciar riscos é parte da governança e liderança, e é fundamental para a maneira como a organização é gerenciada em todos os níveis. Isto contribui para a melhoria dos sistemas de gestão.

Gerenciar riscos é parte de todas as atividades associadas com uma organização e inclui interação com as partes interessadas.

Gerenciar riscos considera os contextos externo e interno da organização, incluindo o comportamento humano e os fatores culturais.

Gerenciar riscos baseia-se nos princípios, estrutura e processos delineados neste documento, como ilustrado na Figura 1. Estes componentes podem já existir total ou parcialmente na organização; contudo, podem necessitar ser adaptados ou melhorados, de forma que gerenciar riscos seja eficiente, eficaz e consistente.

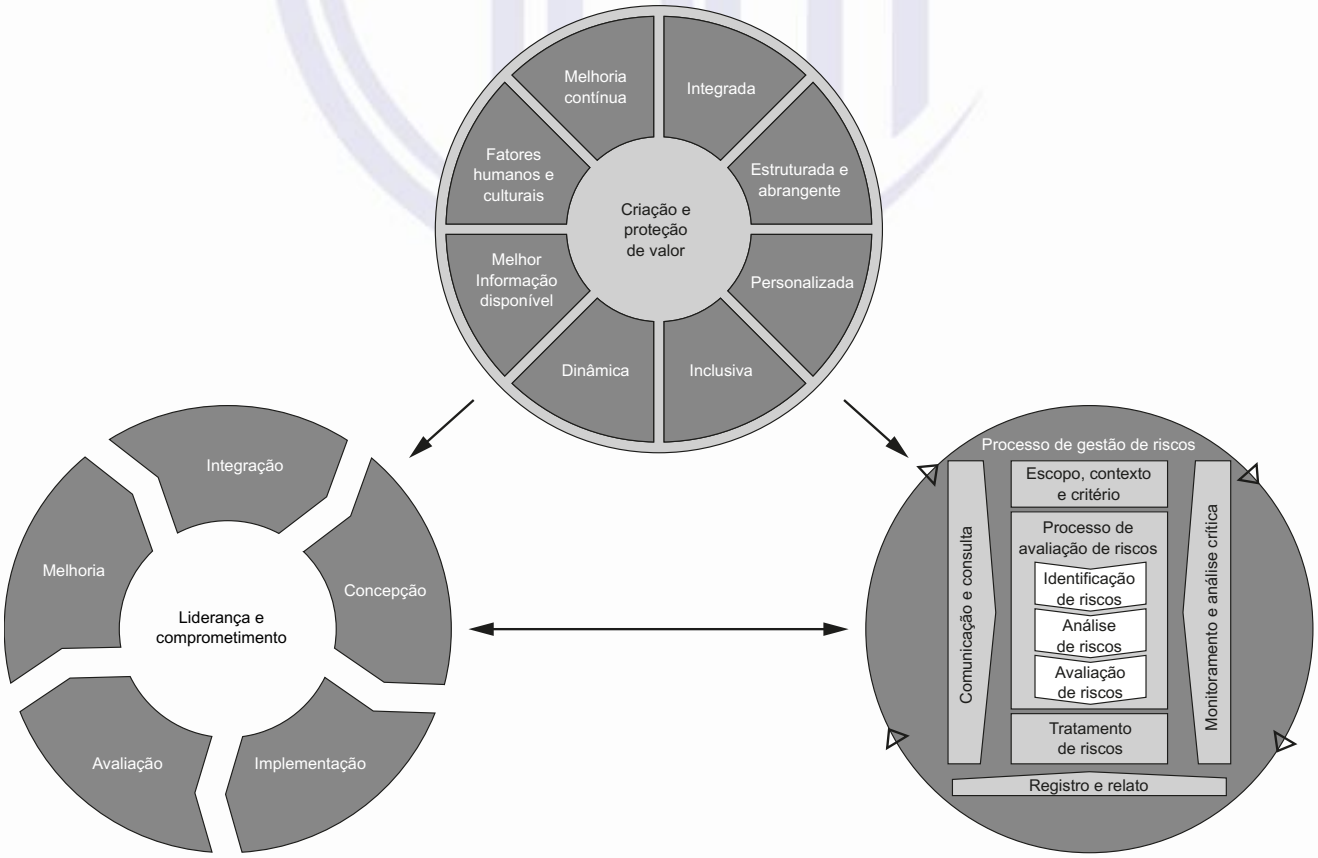

Figura 1 – Princípios, estrutura e processo

Gestão de riscos — Diretrizes

1 Escopo

Este documento fornece diretrizes para gerenciar riscos enfrentados pelas organizações. A aplicação destas diretrizes pode ser personalizada para qualquer organização e seu contexto.

Este documento fornece uma abordagem comum para gerenciar qualquer tipo de risco e não é específico para qualquer indústria ou setor.

Este documento pode ser usado ao longo da vida da organização e aplicado a qualquer atividade, incluindo a tomada de decisão em todos os níveis.

2 Referências normativas

Não há referências normativas neste documento.

3 Termos e definições

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

A ISO e a IEC mantêm bases de dados terminológicos para uso em normalização nos seguintes endereços:

— ISO Online Browsing Platform: disponível em http://www.iso.org/obp

— IEC Electropedia: disponível em http://www.electropedia.org

3.1
risco
efeito da incerteza nos objetivos

Nota 1 de entrada: Um efeito é um desvio em relação ao esperado. Pode ser positivo, negativo ou ambos, e pode abordar, criar ou resultar em oportunidades e ameaças.

Nota 2 de entrada: Objetivos podem possuir diferentes aspectos e categorias, e podem ser aplicados em diferentes níveis.

Nota 3 de entrada: Risco é normalmente expresso em termos de *fontes de risco* (3.4), *eventos* (3.5) potenciais, suas *consequências* (3.6) e suas *probabilidades* (3.7).

3.2
gestão de riscos
atividades coordenadas para dirigir e controlar uma organização no que se refere a *riscos* (3.1)

3.3
parte interessada
pessoa ou organização que pode afetar, ser afetada ou perceber-se afetada por uma decisão ou atividade

Nota 1 de entrada: O termo “parte interessada” pode ser utilizado como alternativa a “*stakeholder*”.

3.4
fonte de risco
elemento que, individualmente ou combinado, tem o potencial para dar origem ao *risco* (3.1)

3.5
evento
ocorrência ou mudança em um conjunto específico de circunstâncias

Nota 1 de entrada: Um evento pode consistir em uma ou mais ocorrências e pode ter várias causas e várias *consequências* (3.6).

Nota 2 de entrada: Um evento pode também ser algo que é esperado, mas não acontece, ou algo que não é esperado, mas acontece.

Nota 3 de entrada: Um evento pode ser uma fonte de risco.

3.6
consequência
resultado de um *evento* (3.5) que afeta os objetivos

Nota 1 de entrada: Uma consequência pode ser certa ou incerta e pode ter efeitos positivos ou negativos, diretos ou indiretos, nos objetivos.

Nota 2 de entrada: As consequências podem ser expressas qualitativa ou quantitativamente.

Nota 3 de entrada: Qualquer consequência pode escalar por meio de efeitos cascata e cumulativos.

3.7
probabilidade
chance de algo acontecer

Nota 1 de entrada: Na terminologia de *gestão de riscos* (3.2), a palavra “probabilidade” é utilizada para referir-se à chance de algo acontecer, não importando se definida, medida ou determinada, ainda que objetiva ou subjetivamente, qualitativa ou quantitativamente, e se descrita utilizando-se termos gerais ou matemáticos (como probabilidade ou frequência durante um determinado período de tempo).

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

3.8
controle
medida que mantém e/ou modifica o *risco* (3.1)

Nota 1 de entrada: Controles incluem, mas não estão limitados a, qualquer processo, política, dispositivo, prática, ou outras condições e/ou ações que mantêm e/ou modificam o risco.

Nota 2 de entrada: Controles podem nem sempre exercer o efeito modificador pretendido ou presumido.

4 Princípios

O propósito da gestão de riscos é a criação e proteção de valor. Ela melhora o desempenho, encoraja a inovação e apoia o alcance de objetivos.

Os princípios descritos na Figura 2 fornecem orientações sobre as características da gestão de riscos eficaz e eficiente, comunicando seu valor e explicando sua intenção e propósito. Os princípios são a base para gerenciar riscos e convém que sejam considerados quando se estabelecerem a estrutura e os processos de gestão de riscos da organização. Convém que estes princípios possibilitem uma organização a gerenciar os efeitos da incerteza nos seus objetivos.

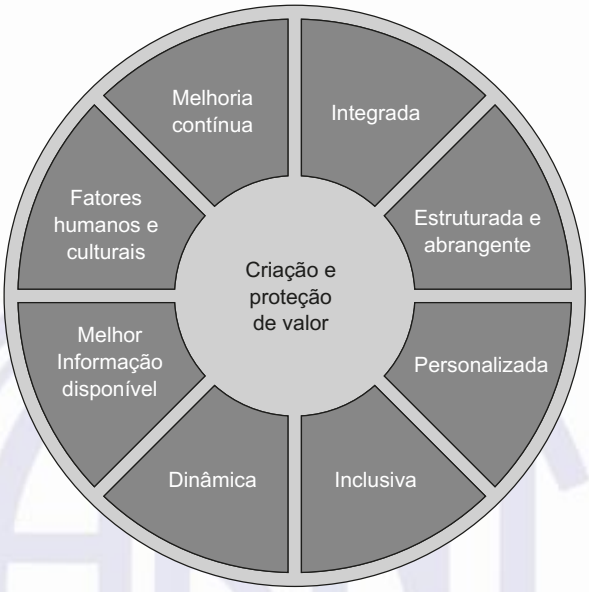

Figura 2 – Princípios

A gestão de riscos eficaz requer os elementos da Figura 2 e pode ser explicada como a seguir.

a) Integrada

A gestão de riscos é parte integrante de todas as atividades organizacionais.

b) Estruturada e abrangente

Uma abordagem estruturada e abrangente para a gestão de riscos contribui para resultados consistentes e comparáveis.

c) Personalizada

A estrutura e o processo de gestão de riscos são personalizados e proporcionais aos contextos externo e interno da organização relacionados aos seus objetivos.

d) Inclusiva

O envolvimento apropriado e oportuno das partes interessadas possibilita que seus conhecimentos, pontos de vista e percepções sejam considerados. Isto resulta em melhor conscientização e gestão de riscos fundamentada.

e) Dinâmica

Riscos podem emergir, mudar ou desaparecer à medida que os contextos externo e interno de uma organização mudem. A gestão de riscos antecipa, detecta, reconhece e responde a estas mudanças e eventos de uma maneira apropriada e oportuna.

f) Melhor informação disponível

As entradas para a gestão de riscos são baseadas em informações históricas e atuais, bem como em expectativas futuras. A gestão de riscos explicitamente leva em consideração quaisquer limitações e incertezas associadas a estas informações e expectativas. Convém que a informação seja oportuna, clara e disponível para as partes interessadas pertinentes.

g) Fatores humanos e culturais

O comportamento humano e a cultura influenciam significativamente todos os aspectos da gestão de riscos em cada nível e estágio.

h) Melhoria contínua

A gestão de riscos é melhorada continuamente por meio do aprendizado e experiências.

5 Estrutura

5.1 Generalidades

O propósito da estrutura da gestão de riscos é apoiar a organização na integração da gestão de riscos em atividades significativas e funções. A eficácia da gestão de riscos dependerá da sua integração na governança e em todas as atividades da organização, incluindo a tomada de decisão. Isto requer apoio das partes interessadas, em particular da Alta Direção.

O desenvolvimento da estrutura engloba integração, concepção, implementação, avaliação e melhoria da gestão de riscos através da organização. A Figura 3 ilustra os componentes de uma estrutura.

Figura 3 – Estrutura

Convém que a organização avalie suas práticas e processos existentes de gestão de riscos, avalie quaisquer lacunas e aborde estas lacunas no âmbito da estrutura.

Convém que os componentes da estrutura e o modo como funcionam em conjunto sejam personalizados para as necessidades da organização.

5.2 Liderança e comprometimento

Convém que a Alta Direção e os órgãos de supervisão, onde aplicável, assegurem que a gestão de riscos esteja integrada em todas as atividades da organização, e convém que demonstrem liderança e comprometimento por:

— personalizar e implementar todos os componentes da estrutura;

— emitir uma declaração ou política que estabeleça uma abordagem, plano ou curso de ação da gestão de riscos;

— assegurar que os recursos necessários sejam alocados para gerenciar riscos;

— atribuir autoridades, responsabilidades e responsabilização nos níveis apropriados dentro da organização;

Isto vai ajudar a organização a:

— alinhar a gestão de riscos com seus objetivos, estratégia e cultura;

— reconhecer e abordar todas as obrigações, bem como seus compromissos voluntários;

— estabelecer a quantidade e o tipo de risco que pode ou não ser assumido para orientar o desenvolvimento de critérios, assegurando que sejam comunicados à organização e às suas partes interessadas;

— comunicar o valor da gestão de riscos para a organização e suas partes interessadas;

— promover o monitoramento sistemático de riscos;

— assegurar que a estrutura de gestão de riscos permaneça apropriada ao contexto da organização.

NOTA BRASILEIRA O termo "*accountability*" foi traduzido como "responsabilização" com o sentido de "responsabilidade por atribuições e atos", ou seja, por prestar contas. Assim, o termo "*accountable*" é entendido como "responsabilizado".

A Alta Direção é responsabilizada por gerenciar riscos, enquanto os órgãos de supervisão são responsabilizados por supervisionar a gestão de riscos. Com frequência, é requerido ou esperado que os órgãos de supervisão:

— assegurem que os riscos sejam adequadamente considerados no estabelecimento dos objetivos da organização;

— compreendam os riscos aos quais a organização está exposta na busca de seus objetivos;

— assegurem que sistemas para gerenciar estes riscos estejam implementados e operem eficazmente;

— assegurem que estes riscos sejam apropriados no contexto dos objetivos da organização;

— assegurem que a informação sobre estes riscos e sua gestão seja apropriadamente comunicada.

5.3 Integração

A integração da gestão de riscos apoia-se em uma compreensão das estruturas e do contexto organizacional. Estruturas diferem, dependendo do propósito, metas e complexidade da organização. O risco é gerenciado em todas as partes da estrutura da organização. Todos na organização têm responsabilidade por gerenciar riscos.

A governança orienta o rumo da organização, suas relações externas e internas, e as regras, processos e práticas necessárias para alcançar o seu propósito. As estruturas de gestão traduzem a direção da governança para a estratégia e os objetivos associados requeridos para alcançar níveis desejados de desempenho sustentável e viabilidade a longo prazo. Determinar a responsabilização pela gestão de riscos e os papéis de supervisão no âmbito de uma organização é parte integrante da governança da organização.

Integrar a gestão de riscos em uma organização é um processo dinâmico e iterativo, e convém que seja personalizado para as necessidades e cultura da organização. Convém que a gestão de riscos seja uma parte, e não separada, do propósito organizacional, governança, liderança e comprometimento, estratégia, objetivos e operações.

5.4 Concepção

5.4.1 Entendendo a organização e seu contexto

Ao conceber a estrutura para gerenciar riscos, convém que a organização examine e entenda seus contextos externo e interno.

Examinar o contexto externo da organização pode incluir, mas não está limitado a:

— fatores sociais, culturais, políticos, jurídicos, regulatórios, financeiros, tecnológicos, econômicos e ambientais, em âmbito internacional, nacional, regional ou local;

— direcionadores-chave e tendências que afetem os objetivos da organização;

— relacionamentos, percepções, valores, necessidades e expectativas das partes interessadas externas;

— relações e compromissos contratuais;

— complexidade das redes de relacionamento e dependências.

Examinar o contexto interno da organização pode incluir, mas não está limitado a:

— visão, missão e valores;

— governança, estrutura organizacional, papéis e responsabilizações;

— estratégia, objetivos e políticas;

— cultura da organização;

— normas, diretrizes e modelos adotados pela organização;

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

— dados, sistemas de informação e fluxos de informação;

— relacionamentos com partes interessadas internas, levando em consideração suas percepções e valores;

— relações contratuais e compromissos;

— interdependências e interconexões.

5.4.2 Articulando o comprometimento com a gestão de riscos

Convém que a Alta Direção e os órgãos de supervisão, onde aplicável, demonstrem e articulem o seu comprometimento contínuo com a gestão de riscos por meio de uma política, uma declaração ou outras formas que claramente transmitam os objetivos e o comprometimento com a gestão de riscos de uma organização. Convém que o comprometimento inclua, mas não se limite a:

— o propósito da organização para gerenciar riscos e vínculos com seus objetivos e outras políticas;

— reforçar a necessidade de integrar a gestão de riscos na cultura global da organização;

— liderar a integração da gestão de riscos nas atividades principais do negócio e na tomada de decisão;

— autoridades, responsabilidades e responsabilizações;

— tornar disponíveis os recursos necessários;

— a maneira pela qual os objetivos conflitantes são tratados;

— medição e relato no âmbito dos indicadores de desempenho da organização;

— análise crítica e melhoria.

Convém que o comprometimento com a gestão de riscos seja comunicado na organização e às partes interessadas, como apropriado.

5.4.3 Atribuindo papéis organizacionais, autoridades, responsabilidades e responsabilizações

Convém que a Alta Direção e os órgãos de supervisão, onde aplicável, assegurem que as autoridades, responsabilidades e responsabilizações para os papéis pertinentes à gestão de riscos sejam atribuídas e comunicadas a todos os níveis da organização, e convém que:

— enfatizem que a gestão de riscos é uma responsabilidade principal;

— identifiquem indivíduos que possuam responsabilização e tenham autoridade para gerenciar riscos (proprietários dos riscos).

5.4.4 Alocando recursos

Convém que a Alta Direção e os órgãos de supervisão, onde aplicável, assegurem a alocação de recursos apropriados para a gestão de riscos, que podem incluir, mas não estão limitados a:

— pessoas, habilidades, experiência e competência;

— processos, métodos e ferramentas da organização a serem usados na gestão de riscos;

— processos e procedimentos documentados;

— sistemas de gestão da informação e do conhecimento;

— necessidades de treinamento e desenvolvimento profissional.

Convém que a organização considere as capacidades e restrições dos recursos existentes.

5.4.5 Estabelecendo comunicação e consulta

Convém que a organização estabeleça uma abordagem aprovada para comunicação e consulta para apoiar a estrutura e facilitar a aplicação eficaz da gestão de riscos. Comunicação envolve compartilhar informação com públicos-alvo. A consulta também envolve o fornecimento de retorno pelos participantes, com a expectativa de que isto contribuirá para as decisões e sua formulação ou outras atividades. Convém que os métodos e conteúdo da comunicação e consulta reflitam as expectativas das partes interessadas, onde for pertinente.

Convém que a comunicação e a consulta sejam oportunas e assegurem que a informação pertinente seja coletada, consolidada, sintetizada e compartilhada, como apropriado, e que o retorno seja fornecido e as melhorias sejam implementadas.

5.5 Implementação

Convém que a organização implemente a estrutura de gestão de riscos por meio de:

— desenvolvimento de um plano apropriado, incluindo prazos e recursos;

— identificação de onde, quando e como diferentes tipos de decisões são tomadas pela organização, e por quem;

— modificação dos processos de tomada de decisão aplicáveis, onde necessário;

— garantia de que os arranjos da organização para gerenciar riscos sejam claramente compreendidos e praticados.

A implementação bem-sucedida da estrutura requer o engajamento e a conscientização das partes interessadas. Isso permite que as organizações abordem explicitamente a incerteza na tomada de decisão, enquanto também asseguram que qualquer incerteza nova ou posterior possa ser levada em consideração à medida que ela surja.

Adequadamente concebida e implementada, a estrutura de gestão de riscos assegurará que o processo de gestão de riscos é parte de todas as atividades da organização, incluindo a tomada de decisão, e que as mudanças nos contextos externo e interno serão adequadamente capturadas.

5.6 Avaliação

Para avaliar a eficácia da estrutura de gestão de riscos, convém que a organização:

— mensure periodicamente o desempenho da estrutura de gestão de riscos em relação ao seu propósito, planos de implementação, indicadores e comportamento esperado;

— determine se permanece adequada para apoiar o alcance dos objetivos da organização.

5.7 Melhoria

5.7.1 Adaptação

Convém que a organização monitore e adapte continuamente a estrutura de gestão de riscos para abordar as mudanças externas e internas. Ao fazer isso, a organização pode melhorar seu valor.

5.7.2 Melhoria contínua

Convém que organização melhore continuamente a adequação, suficiência e eficácia da estrutura de gestão de riscos e a forma como o processo de gestão de riscos é integrado.

À medida que lacunas ou oportunidades de melhoria pertinentes são identificadas, convém que a organização desenvolva planos e tarefas e os atribua àqueles responsabilizados pela implementação. Uma vez implementadas, convém que estas melhorias contribuam para o aprimoramento da gestão de riscos.

6 Processo

6.1 Generalidades

O processo de gestão de riscos envolve a aplicação sistemática de políticas, procedimentos e práticas para as atividades de comunicação e consulta, estabelecimento do contexto e avaliação, tratamento, monitoramento, análise crítica, registro e relato de riscos. Este processo é ilustrado na Figura 4.

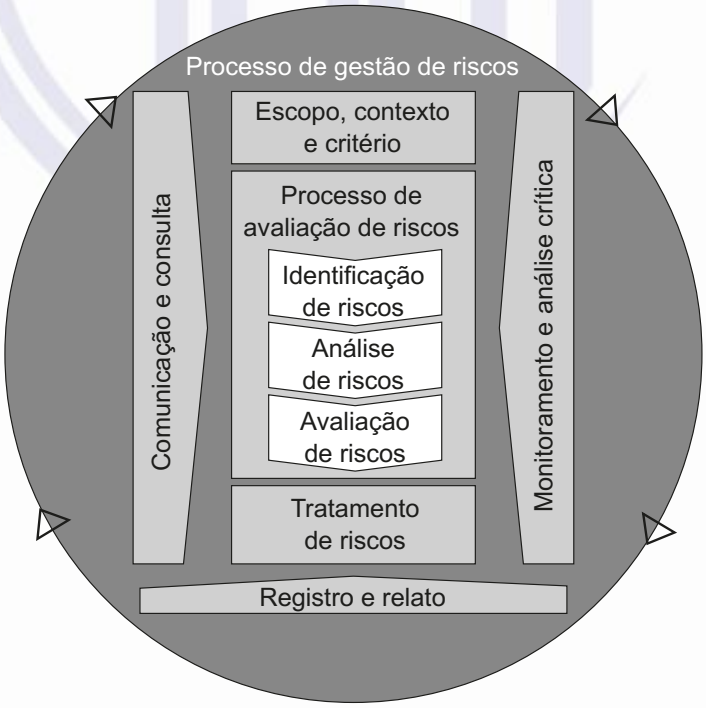

Figura 4 – Processo

Convém que o processo de gestão de riscos seja parte integrante da gestão e da tomada de decisão, e seja integrado na estrutura, operações e processos da organização. Pode ser aplicado nos níveis estratégico, operacional, de programas ou de projetos.

Pode haver muitas aplicações do processo de gestão de riscos em uma organização, personalizadas para alcançar objetivos e para se adequar aos contextos externo e interno nos quais são realizadas.

Convém que a natureza dinâmica e variável do comportamento humano e cultura seja considerada ao longo do processo de gestão de riscos.

Embora o processo de gestão de riscos seja frequentemente apresentado como sequencial, na prática ele é iterativo.

6.2 Comunicação e consulta

O propósito da comunicação e consulta é auxiliar as partes interessadas pertinentes na compreensão do risco, na base sobre a qual decisões são tomadas e nas razões pelas quais ações específicas são requeridas. A comunicação busca promover a conscientização e o entendimento do risco, enquanto a consulta envolve obter retorno e informação para auxiliar a tomada de decisão. Convém que uma coordenação estreita entre as duas facilite a troca de informações factuais, oportunas, pertinentes, precisas e compreensíveis, levando em consideração a confidencialidade e integridade da informação, bem como os direitos de privacidade dos indivíduos.

Convém que ocorram comunicação e consulta com partes interessadas apropriadas externas e internas, no âmbito de cada etapa e ao longo de todo o processo de gestão de riscos.

Comunicação e consulta visam a:

— reunir diferentes áreas de especialização para cada etapa do processo de gestão de riscos;

— assegurar que pontos de vista diferentes sejam considerados apropriadamente ao se definirem critérios de risco e ao se avaliarem riscos;

— fornecer informações suficientes para facilitar a supervisão dos riscos e a tomada de decisão;

— construir um senso de inclusão e propriedade entre os afetados pelo risco.

6.3 Escopo, contexto e critérios

6.3.1 Generalidades

O propósito do estabelecimento do escopo, contexto e critérios é personalizar o processo de gestão de riscos, permitindo um processo de avaliação de riscos eficaz e um tratamento de riscos apropriado. Escopo, contexto e critérios envolvem a definição do escopo do processo, a compreensão dos contextos externo e interno.

6.3.2 Definindo o escopo

Convém que a organização defina o escopo de suas atividades de gestão de riscos.

Como o processo de gestão de riscos pode ser aplicado em diferentes níveis (por exemplo, estratégico, operacional, programa, projeto ou outras atividades), é importante ser claro sobre o escopo em consideração, os objetivos pertinentes a serem considerados e o seu alinhamento aos objetivos organizacionais.

Ao planejar a abordagem, as considerações incluem:

— objetivos e decisões que precisam ser tomadas;

— resultados esperados das etapas a serem realizadas no processo;

— tempo, localização, inclusões e exclusões específicas;

— ferramentas e técnicas apropriadas para o processo de avaliação de riscos;

— recursos requeridos, responsabilidades e registros a serem mantidos;

— relacionamentos com outros projetos, processos e atividades.

6.3.3 Contextos externo e interno

Os contextos externo e interno são o ambiente no qual a organização procura definir e alcançar seus objetivos.

Convém que o contexto do processo de gestão de riscos seja estabelecido a partir da compreensão dos ambientes externo e interno no qual a organização opera, e convém que reflita o ambiente específico da atividade ao qual o processo de gestão de riscos é aplicado.

Compreender o contexto é importante porque:

— a gestão de riscos ocorre no contexto dos objetivos e atividades da organização;

— fatores organizacionais podem ser uma fonte de risco;

— propósito e escopo do processo de gestão de riscos podem estar inter-relacionados com os objetivos da organização como um todo;

Convém que a organização estabeleça os contextos externo e interno do processo de gestão de riscos, considerando os fatores mencionados em 5.4.1.

6.3.4 Definindo critérios de risco

Convém que a organização especifique a quantidade e o tipo de risco que podem ou não assumir em relação aos objetivos. Convém também que estabeleça critérios para avaliar a significância do risco e para apoiar os processos de tomada de decisão. Convém que os critérios de risco sejam alinhados à estrutura de gestão de riscos e sejam personalizados para o propósito específico e o escopo da atividade em consideração. Convém que os critérios de risco reflitam os valores, objetivos e recursos da organização e sejam consistentes com as políticas e declarações sobre gestão de riscos. Convém que os critérios de risco sejam estabelecidos levando em consideração as obrigações da organização e os pontos de vista das partes interessadas.

Embora convenha que os critérios de risco sejam estabelecidos no início do processo de avaliação de riscos, eles são dinâmicos; e convém que sejam continuamente analisados criticamente e alterados, se necessário.

Para estabelecer os critérios de risco, convém considerar:

— a natureza e o tipo de incertezas que podem afetar resultados e objetivos (tanto tangíveis quanto intangíveis);

— como as consequências (tanto positivas quanto negativas) e as probabilidades serão definidas e medidas;

— fatores relacionados ao tempo;

— consistência no uso de medidas;

— como o nível de risco será determinado;

— como as combinações e sequências de múltiplos riscos serão levadas em consideração;

— a capacidade da organização.

6.4 Processo de avaliação de riscos

6.4.1 Generalidades

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

Convém que o processo de avaliação de riscos seja conduzido de forma sistemática, iterativa e colaborativa, com base no conhecimento e nos pontos de vista das partes interessadas. Convém que use a melhor informação disponível, complementada por investigação adicional, como necessário.

6.4.2 Identificação de riscos

O propósito da identificação de riscos é encontrar, reconhecer e descrever riscos que possam ajudar ou impedir que uma organização alcance seus objetivos. Informações pertinentes, apropriadas e atualizadas são importantes na identificação de riscos.

A organização pode usar uma variedade de técnicas para identificar incertezas que podem afetar um ou mais objetivos. Convém que os seguintes fatores e o relacionamento entre estes fatores sejam considerados:

— fontes tangíveis e intangíveis de risco;

— causas e eventos;

— ameaças e oportunidades;

— vulnerabilidades e capacidades;

— mudanças nos contextos externo e interno;

— indicadores de riscos emergentes;

— natureza e valor dos ativos e recursos;

— consequências e seus impactos nos objetivos;

— limitações de conhecimento e de confiabilidade da informação;

— fatores temporais;

— vieses, hipóteses e crenças dos envolvidos.

Convém que a organização identifique os riscos, independentemente de suas fontes estarem ou não sob seu controle. Convém considerar que pode haver mais de um tipo de resultado, o que pode resultar em uma variedade de consequências tangíveis ou intangíveis.

6.4.3 Análise de riscos

O propósito da análise de riscos é compreender a natureza do risco e suas características, incluindo o nível de risco, onde apropriado. A análise de riscos envolve a consideração detalhada de incertezas, fontes de risco, consequências, probabilidade, eventos, cenários, controles e sua eficácia. Um evento pode ter múltiplas causas e consequências e pode afetar múltiplos objetivos.

A análise de riscos pode ser realizada com vários graus de detalhamento e complexidade, dependendo do propósito da análise, da disponibilidade e confiabilidade da informação, e dos recursos disponíveis. As técnicas de análise podem ser qualitativas, quantitativas ou uma combinação destas, dependendo das circunstâncias e do uso pretendido.

Convém que a análise de riscos considere fatores como:

— a probabilidade de eventos e consequências;

— a natureza e magnitude das consequências;

— complexidade e conectividade;

— fatores temporais e volatilidade;

— a eficácia dos controles existentes;

— sensibilidade e níveis de confiança.

A análise de riscos pode ser influenciada por qualquer divergência de opiniões, vieses, percepções do risco e julgamentos. Influências adicionais são a qualidade da informação utilizada, as hipóteses e as exclusões feitas, quaisquer limitações das técnicas e como elas são executadas. Convém que estas influências sejam consideradas, documentadas e comunicadas aos tomadores de decisão.

Eventos altamente incertos podem ser difíceis de quantificar. Isso pode ser um problema ao analisar eventos com consequências severas. Nestes casos, usar uma combinação de técnicas geralmente fornece maior discernimento.

A análise de riscos fornece uma entrada para a avaliação de riscos, para decisões sobre se o risco necessita ser tratado e como, e sobre a estratégia e os métodos mais apropriados para o tratamento de riscos. Os resultados propiciam discernimento para decisões, em que escolhas estão sendo feitas e as opções envolvem diferentes tipos e níveis de risco.

6.4.4 Avaliação de riscos

O propósito da avaliação de riscos é apoiar decisões. A avaliação de riscos envolve a comparação dos resultados da análise de riscos com os critérios de risco estabelecidos para determinar onde é necessária ação adicional. Isto pode levar a uma decisão de:

— fazer mais nada;

— considerar as opções de tratamento de riscos;

— realizar análises adicionais para melhor compreender o risco;

— manter os controles existentes;

— reconsiderar os objetivos.

Convém que as decisões levem em consideração o contexto mais amplo e as consequências reais e percebidas para as partes interessadas externas e internas.

Convém que o resultado da avaliação de riscos seja registrado, comunicado e então validado nos níveis apropriados da organização.

6.5 Tratamento de riscos

6.5.1 Generalidades

O propósito do tratamento de riscos é selecionar e implementar opções para abordar riscos.

O tratamento de riscos envolve um processo iterativo de:

— formular e selecionar opções para tratamento do risco;

— planejar e implementar o tratamento do risco;

— avaliar a eficácia deste tratamento;

— decidir se o risco remanescente é aceitável;

— se não for aceitável, realizar tratamento adicional.

6.5.2 Seleção de opções de tratamento de riscos

Selecionar a(s) opção(ões) mais apropriada(s) de tratamento de riscos envolve balancear os benefícios potenciais derivados em relação ao alcance dos objetivos, face aos custos, esforço ou desvantagens da implementação.

As opções de tratamento de riscos não são necessariamente mutuamente exclusivas ou apropriadas em todas as circunstâncias. As opções para tratar o risco podem envolver um ou mais dos seguintes:

— evitar o risco ao decidir não iniciar ou continuar com a atividade que dá origem ao risco;

— assumir ou aumentar o risco de maneira a perseguir uma oportunidade;

— remover a fonte de risco;

— mudar a probabilidade;

— mudar as consequências;

— compartilhar o risco (por exemplo, por meio de contratos, compra de seguros);

— reter o risco por decisão fundamentada.

A justificativa para o tratamento de riscos é mais ampla do que apenas considerações econômicas, e convém que leve em consideração todas as obrigações da organização, compromissos voluntários e pontos de vista das partes interessadas. Convém que a seleção de opções de tratamento de riscos seja feita de acordo com os objetivos da organização, critérios de risco e recursos disponíveis.

Ao selecionar opções de tratamento de riscos, convém que a organização considere os valores, percepções e potencial envolvimento das partes interessadas, e as formas mais apropriadas para com elas se comunicar e consultar. Embora igualmente eficazes, alguns tratamentos de riscos podem ser mais aceitáveis para algumas partes interessadas do que para outras.

Ainda que cuidadosamente concebido e implementado, o tratamento de riscos pode não produzir os resultados esperados e pode produzir consequências não pretendidas. Monitoramento e análise crítica precisam ser parte integrante da implementação do tratamento de riscos, para assegurar que as diferentes formas de tratamento se tornem e permaneçam eficazes.

O tratamento de riscos também pode introduzir novos riscos que precisem ser gerenciados.

Se não houver opções de tratamento disponíveis ou se as opções de tratamento não modificarem suficientemente o risco, convém que este seja registrado e mantido sob análise crítica contínua.

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

6.5.3 Preparando e implementando planos de tratamento de riscos

O propósito dos planos de tratamento de riscos é especificar como as opções de tratamento escolhidas serão implementadas de maneira que os arranjos sejam compreendidos pelos envolvidos, e o progresso em relação ao plano possa ser monitorado. Convém que o plano de tratamento identifique claramente a ordem em que o tratamento de riscos será implementado.

Convém que os planos de tratamento sejam integrados nos planos e processos de gestão da organização, em consulta com as partes interessadas apropriadas.

Convém que as informações fornecidas no plano de tratamento incluam:

— a justificativa para a seleção das opções de tratamento, incluindo os benefícios esperados a serem obtidos;

— aqueles que são responsabilizáveis e responsáveis por aprovar e implementar o plano;

— as ações propostas;

— os recursos requeridos, incluindo contingências;

— as medidas de desempenho;

— as restrições;

— os relatos e monitoramento requeridos;

— quando se espera que ações sejam tomadas e concluídas.

6.6 Monitoramento e análise crítica

O propósito do monitoramento e análise crítica é assegurar e melhorar a qualidade e eficácia da concepção, implementação e resultados do processo. Convém que o monitoramento contínuo e a análise crítica periódica do processo de gestão de riscos e seus resultados sejam uma parte planejada do processo de gestão de riscos, com responsabilidades claramente estabelecidas.

Convém que monitoramento e análise crítica ocorram em todos os estágios do processo. Monitoramento e análise crítica incluem planejamento, coleta e análise de informações, registro de resultados e fornecimento de retorno.

Convém que os resultados do monitoramento e análise crítica sejam incorporados em todas as atividades de gestão de desempenho, medição e relatos da organização.

6.7 Registro e relato

Convém que o processo de gestão de riscos e seus resultados sejam documentados e relatados por meio de mecanismos apropriados. O registro e o relato visam:

— comunicar atividades e resultados de gestão de riscos em toda a organização;

— fornecer informações para a tomada de decisão;

— melhorar as atividades de gestão de riscos;

— auxiliar a interação com as partes interessadas, incluindo aquelas com responsabilidade e com responsabilização por atividades de gestão de riscos.

Convém que as decisões relativas à criação, retenção e manuseio de informação documentada levem em consideração, mas não se limitem a, o seu uso, a sensibilidade da informação e os contextos externo e interno.

O relato é parte integrante da governança da organização e convém que melhore a qualidade do diálogo com as partes interessadas e apoie a Alta Direção e os órgãos de supervisão a cumprirem suas responsabilidades. Os fatores a considerar para o relato incluem, mas não estão limitados a:

— diferentes partes interessadas e suas necessidades específicas de informação e requisitos;

— custo, frequência e pontualidade do relato;

— método de relato;

— pertinência da informação para os objetivos organizacionais e para a tomada de decisão.

Bibliografia

[1] ABNT NBR IEC 31010, *Gestão de riscos – Técnicas para o processo de avaliação de riscos*