NORMA QSP 31000:2018

Sistemas de Gestão de Riscos - Requisitos

3ª Edição – Julho 2018

Alinhada ao Anexo SL das Diretivas ISO e à nova ISO 31000:2018

QSP – Centro da Qualidade, Segurança e Produtividade

Sistemas de Gestão de Riscos

Requisitos

ESTA É UMA PRÉ-VISUALIZAÇÃO DA NORMA DE REQUISITOS QSP 31000:2018.

SUMÁRIO

1 – ESCOPO

Esta Norma QSP especifica requisitos para um sistema de gestão de riscos, aplicando-se a qualquer tipo de risco, independentemente de sua natureza, quer tenha consequências positivas ou negativas.

Este documento não é específico para qualquer indústria ou setor, podendo ser usado ao longo da vida da organização e aplicado a qualquer atividade, incluindo a tomada de decisão em todos os níveis.

Esta Norma QSP destina-se também para fins de auditoria de segunda e terceira partes.

2 – TERMOS E DEFINIÇÕES

Para os efeitos deste documento, aplicam-se os termos e definições da ABNT NBR ISO 31000:2018, do ABNT ISO GUIA 73, da PAS 99 (2ª edição) e da ABNT NBR ISO 9000:2015.

3 – PRINCÍPIOS

Os princípios de gestão de riscos declarados na ABNT NBR ISO 31000:2018 foram levados em consideração durante o desenvolvimento desta Norma QSP.

4 – SISTEMA DE GESTÃO DE RISCOS

4.1 – Generalidades

O propósito de um sistema de 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 do sistema de gestão de riscos engloba integração, concepção, implementação, avaliação e melhoria da gestão de riscos através da organização. A Figura 1 ilustra os componentes do sistema de gestão de riscos para esta Norma QSP.

A política de gestão de riscos deve ser comunicada na organização e às partes interessadas, como apropriado.

4.4.3 – Atribuindo papéis organizacionais, autoridades, responsabilidades e responsabilizações

A Alta Direção e os órgãos de supervisão, onde aplicável, devem assegurar que as autoridades, responsabilidades e responsabilizações para os papéis pertinentes à gestão de riscos sejam atribuídas e comunicadas a todos os níveis da organização.

A Alta Direção e os órgãos de supervisão, onde aplicável, devem:

a) enfatizar que a gestão de riscos é uma responsabilidade principal;
b) identificar indivíduos que possuam responsabilização e tenham autoridade para gerenciar riscos (proprietários dos riscos).

4.4.4 – Alocando recursos

A Alta Direção e os órgãos de supervisão, onde aplicável, devem assegurar a alocação de recursos apropriados para a gestão de riscos, incluindo:

a) pessoas, habilidades, experiência e competência;
b) processos, métodos e ferramentas da organização a serem usados na gestão de riscos;
c) processos e procedimentos documentados;
d) sistemas de gestão da informação e do conhecimento;
e) necessidades de treinamento e desenvolvimento profissional;
f) capacidades e restrições dos recursos existentes.

4.4.5 – Estabelecendo comunicação e consulta

A organização deve estabelecer uma abordagem aprovada para comunicação e consulta, para apoiar o sistema de gestão de riscos e facilitar a aplicação eficaz da gestão de riscos.

Os métodos e conteúdo da comunicação e consulta devem refletir as expectativas das partes interessadas, onde for pertinente.

A comunicação e a consulta devem assegurar que a informação pertinente seja coletada, consolidada, sintetizada e compartilhada, como apropriado, que o retorno seja fornecido e que as melhorias sejam implementadas.

4.4.6 – Requisitos legais e outros requisitos

A organização deve:

a) determinar e ter acesso aos requisitos legais e outros requisitos relacionados a suas fontes de risco;
b) determinar como estes requisitos legais e outros requisitos aplicam-se à organização;
c) considerar requisitos legais e outros requisitos quando estabelecer, implementar, manter e melhorar continuamente seu sistema de gestão de riscos.

A organização deve manter informação documentada de seus requisitos legais e outros requisitos.

NOTA: Requisitos legais e outros requisitos podem resultar em ameaças e oportunidades para a organização.

4.4.7 – Planejamento de contingências e continuidade de negócios

A organização deve estabelecer, implementar e manter o(s) processo(s) necessário(s) para:

a) identificar contingências potenciais;
b) responder a situações de contingência reais;
c) tomar ações para prevenir ou mitigar as consequências decorrentes de situações de contingência, apropriadas à magnitude da contingência e aos potenciais impactos;
d) testar periodicamente as ações de resposta planejadas, onde viável;
e) periodicamente, analisar criticamente e revisar o(s) processo(s) e as ações de resposta planejadas, em particular, após a ocorrência de situações de contingência ou testes; e
f) prover informações pertinentes e treinamento relacionado à preparação e resposta a contingências, como apropriado, para as partes interessadas, incluindo pessoas que realizam trabalho sob o seu controle.

A organização deve manter informação documentada na extensão necessária, para ter confiança de que o(s) processo(s) seja(m) realizado(s) conforme planejado(s).

NOTA: A ABNT NBR ISO 22313:2015 fornece orientações sobre sistemas de gestão de continuidade de negócios.

4.5 – Implementação da gestão de riscos

4.5.1 – Implementação do sistema de gestão de riscos

A organização deve implementar e manter o sistema de gestão de riscos por meio de:

a) desenvolvimento de um plano apropriado, incluindo prazos e recursos;
b) identificação de onde, quando e como diferentes tipos de decisões são tomadas pela organização, e por quem;
c) modificação dos processos de tomada de decisão aplicáveis, onde necessário;
d) garantia de que os arranjos da organização para gerenciar riscos sejam claramente compreendidos e praticados.

A organização deve assegurar o engajamento e a conscientização das partes interessadas na implementação do sistema de gestão de riscos.

A organização deve abordar explicitamente a incerteza na tomada de decisão e assegurar que qualquer incerteza nova ou posterior seja levada em consideração à medida que surja.

O sistema de gestão de riscos deve assegurar que o processo de gestão de riscos seja parte de todas as atividades da organização, incluindo a tomada de decisão, e deve assegurar que as mudanças nos contextos externo e interno sejam adequadamente capturadas.

4.5.1.1 – Informação documentada

O sistema de gestão de riscos deve incluir:

a) a política de gestão de riscos;
b) o plano de gestão de riscos;
c) os planos de comunicação e consulta às partes interessadas externas e internas;
d) os planos de tratamento de riscos;
e) informação documentada, determinada pela organização como sendo necessária para a eficácia do sistema de gestão de riscos.

NOTA: A extensão da informação documentada para um sistema de gestão de riscos pode diferir de uma organização para outra, devido:
- ao porte da organização e seu tipo de atividades, processos, produtos e serviços;
- à necessidade de demonstrar o atendimento aos seus requisitos legais e outros requisitos;
- à complexidade de processos e suas interações;
- à competência de pessoas que realizam trabalho sob o controle da organização.

4.5.1.1.1 – Criando e atualizando

Ao criar e atualizar informação documentada, a organização deve assegurar apropriados(as):

a) identificação e descrição (por exemplo, um título, data, autor ou número de referência);
b) formato (por exemplo, linguagem, versão do *software*, gráficos) e meio (por exemplo, eletrônico);
c) análise crítica e aprovação quanto à adequação e suficiência.

4.5.1.1.2 – Controle de informação documentada

A informação documentada requerida pelo sistema de gestão de riscos e por esta Norma QSP deve ser controlada para assegurar que:

a) ela esteja disponível e adequada para uso, onde e quando for necessário;
b) ela esteja protegida adequadamente (por exemplo, contra perda de confidencialidade, uso impróprio ou perda de integridade).

Para o controle de informação documentada, a organização deve abordar as seguintes atividades, como aplicável:

i. distribuição, acesso, recuperação e uso;
ii. armazenamento e preservação, incluindo preservação de legibilidade;
iii. controle de alterações (por exemplo, controle de versão);
iv. retenção e disposição.

A informação documentada de origem externa, determinada pela organização como necessária para o planejamento e operação do sistema de gestão de riscos deve ser identificada, como apropriado, e controlada.

NOTA: Acesso pode implicar uma decisão quanto à permissão para somente ver a informação documentada, ou a permissão e autoridade para ver e alterar a informação documentada.

4.5.2 – Implementação do processo de gestão de riscos

A organização deve assegurar que o processo de gestão de riscos, descrito na seção 5, seja aplicado em todos os níveis e funções pertinentes da organização, como parte de suas práticas e processos.

4.6 – Avaliação, monitoramento e análise crítica

4.6.1 – Avaliação do sistema de gestão de riscos

A organização deve avaliar a eficácia do sistema de gestão de riscos por meio de:

a) mensuração periódica do desempenho do sistema de gestão de riscos em relação ao seu propósito, planos de implementação, indicadores e comportamento esperado;
b) determinação de se o sistema de gestão de riscos permanece adequado para apoiar o alcance dos objetivos da organização.

5.2 – Comunicação e consulta

A comunicação e consulta às partes interessadas apropriadas externas e internas devem ocorrer no âmbito de cada etapa e ao longo de todo o processo de gestão de riscos.

A organização deve desenvolver planos de comunicação e consulta. Tais planos devem abordar questões relacionadas com o risco propriamente dito, suas causas, suas consequências (se conhecidas) e as medidas que estão sendo tomadas para tratá-lo.

A comunicação e a consulta devem:

a) reunir diferentes áreas de especialização para cada etapa do processo de gestão de riscos;
b) assegurar que pontos de vista diferentes sejam considerados apropriadamente ao se definirem critérios de risco e ao se avaliarem riscos;
c) fornecer informações suficientes para facilitar a supervisão dos riscos e a tomada de decisão;
d) construir um senso de inclusão e propriedade entre os afetados pelo risco.

5.3 – Escopo, contexto e critérios

5.3.1 – Generalidades

A organização deve personalizar o processo de gestão de riscos por meio do estabelecimento do escopo, contexto e critérios de risco.

5.3.2 – Definindo o escopo

A organização deve definir o escopo da aplicação do processo de gestão de riscos em diferentes níveis (estratégico, operacional, programa, projeto ou outras atividades), bem como deve considerar:

a) objetivos e decisões que precisam ser tomadas;
b) resultados esperados das etapas a serem realizadas no processo;
c) tempo, localização, inclusões e exclusões específicas;
d) ferramentas e técnicas apropriadas para o processo de avaliação de riscos;
e) recursos requeridos, responsabilidades e registros a serem mantidos;
f) relacionamentos com outros projetos, processos e atividades.

5.3.3 – Contextos externo e interno

O contexto do processo de gestão de riscos deve ser estabelecido a partir da compreensão dos ambientes externo e interno no qual a organização opera, e deve refletir o ambiente específico da atividade ao qual o processo de gestão de riscos é aplicado.

A organização deve estabelecer os contextos externo e interno do processo de gestão de riscos, considerando os fatores mencionados em 4.4.1.

5.3.4 – Definindo critérios de risco

A organização deve especificar a quantidade e o tipo de risco que pode ou não assumir em relação aos objetivos, bem como deve estabelecer critérios para avaliar a significância do risco e para apoiar os processos de tomada de decisão.

Os critérios de risco devem:

a) ser alinhados ao sistema de gestão de riscos;

b) ser personalizados para o propósito específico e o escopo da atividade em consideração;
c) refletir os valores, objetivos e recursos da organização;
d) ser consistentes com a política de gestão de riscos;
e) ser estabelecidos levando em consideração as obrigações da organização e os pontos de vista das partes interessadas;
f) ser estabelecidos no início do processo de avaliação de riscos;
g) ser continuamente analisados criticamente e alterados, se necessário.

Para estabelecer os critérios de risco, a organização deve também considerar, como aplicável:

i. a natureza e o tipo de incertezas que podem afetar resultados e objetivos (tanto tangíveis quanto intangíveis);
ii. como as consequências (tanto positivas quanto negativas) e as probabilidades serão definidas e medidas;
iii. fatores relacionados ao tempo;
iv. consistência no uso de medidas;
v. como o nível de risco será determinado;
vi. como as combinações e sequências de múltiplos riscos serão levadas em consideração;
vii. a capacidade da organização.

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.

O processo de avaliação de riscos deve ser conduzido de forma sistemática, iterativa e colaborativa, com base no conhecimento e nos pontos de vista das partes interessadas, usando a melhor informação disponível, complementada por investigação adicional, como necessário.

NOTA: A ISO/IEC 31010 fornece orientação sobre técnicas e ferramentas do processo de avaliação de riscos.

5.4.2 – 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. Os seguintes fatores e o relacionamento entre estes fatores devem ser considerados, como aplicável:

a) fontes tangíveis e intangíveis de risco;
b) causas e eventos;
c) ameaças e oportunidades;
d) vulnerabilidades e capacidades;
e) mudanças nos contextos externo e interno;
f) indicadores de riscos emergentes;
g) natureza e valor dos ativos e recursos;
h) consequências e seus impactos nos objetivos;
i) limitações de conhecimento e de confiabilidade da informação;
j) fatores temporais;
k) vieses, hipóteses e crenças dos envolvidos.

NORMA QSP 31000:2018

Sistemas de Gestão de Riscos - Requisitos

A norma QSP 31000:2018 **não é comercializada**. Ela pode ser utilizada por organizações (associadas e/ou clientes conveniados com o QSP) que desejam implementar, manter, melhorar e, se for o caso, certificar seu Sistema de Gestão de Riscos baseado na ISO 31000:2018.

qsp@qsp.org.br
11 3704-3200

QSP – Centro da Qualidade, Segurança e Produtividade