

Gestão de riscos e a norma ISO 31000: importância e impasses rumo a um consenso

Germano Mendes Rosa (Instituto Federal de Minas Gerais) germano.rosa@ifmg.edu.br
José Carlos de Toledo (Universidade Federal de São Carlos) toledo@dep.ufscar.br

Resumo:

Este artigo apresenta uma revisão bibliográfica focada na gestão de riscos, na qual abrange-se principalmente a norma internacional ISO 31000, se concentrando em seus principais fundamentos, características, estrutura, processos e críticas. Aborda-se brevemente a norma certificável QSP 31000 e a inclusão prevista da abordagem de risco nas novas versões das normas ISO 9001:2015 e ISO 14001:2015 e em todas as novas normas ISO e futuras revisões de suas normas existentes. O propósito maior deste artigo é compilar informações a respeito do atual desenvolvimento da gestão de riscos e de uma norma internacional relativamente recente, a ISO 31000. Conclui-se discutindo a indissociabilidade entre a gestão de riscos e as atividades organizacionais e a necessidade de maior desenvolvimento das normas de gestão de riscos para abranger com suficiência a todos os aspectos relevantes à gestão de riscos, incluindo uma terminologia mais adequada e consensual.

Palavras chave: Gestão de riscos, Norma ISO 31000, Importância, Críticas.

Risk management and the standard ISO 31000: value and impasses towards an agreement

Abstract

This article brings a literature review focused on risk management discipline covering mainly the international standard ISO 31000, focusing on its main foundations, characteristics, structure, processes, and criticism. It covers up briefly certifiable standard QSP 31000 and the inclusion of expected risk approach in the new versions of ISO 9001: 2015 and ISO 14001: 2015 and in all new ISO standards and future revisions of their existing standards. The main purpose of this article is to compile information about the development of the risk management discipline as well as about ISO 31000, an international and relatively novel standard. It concludes by discussing the inextricable connection between the risk management discipline and the organizational activities and the need for further development of risk management standards for cover with sufficiency to all aspects relevant to risk management discipline, including a more appropriate and consensual terminology.

Key-words: Risk management, ISO 31000, Value, Criticism.

1. Introdução

O risco pode ser entendido como efeito da incerteza sobre o alcance de objetivos, sendo que uma alteração na incerteza também altera o risco (STATE OF VICTORIA, 2015). Assim,

gerenciar riscos constitui atividade indispensável a qualquer âmbito empresarial, uma vez que, resguardada as devidas proporções, o risco incide nos resultados de qualquer atividade ou processo. Portanto, compreender, avaliar e tratar o risco é fundamentalmente importante para garantir o atingimento de objetivos organizacionais.

A avaliação do risco se propõe a sistematizar conhecimento e incertezas sobre fenômenos, processos, atividades e sistemas sob análise, visando estimar potenciais perigos e ameaças, suas causas e consequências, gerando condições de se distinguir o que é tolerável e aceitável e comparar opções para tomada de decisão (AVEN, 2011), constituindo uma ferramenta estrategicamente vital no cenário globalizado.

A gestão de riscos – que contempla a avaliação do risco – combina cultura, sistemas e processos empreendidos por uma organização para coordenar a identificação e o gerenciamento do risco, sendo que uma gestão de riscos bem-feita prevenirá danos ou reduzirá seu efeito (STATE OF VICTORIA, 2015).

Por outro lado, a gestão de riscos é uma área em acelerado desenvolvimento, envolvendo diferentes pontos de vista sobre seu conceito e conteúdo, como deve ser realizada e com qual objetivo. Dessa forma, houve necessidade de normas para estabelecer concordância em relação aos seguintes aspectos (FERMA, 2003):

- a) Terminologia;
- b) Processos de implementação;
- c) Estrutura;
- d) Objetivos.

Consequentemente, não houve carência de elaboração de normas e guias na área de gestão de riscos na última década, o que desencadeou a proliferação descoordenada de normas, ocasionando significativas inconsistências e falta de abordagens adequadas e de terminologias reconhecidas pela indústria (PREDA, 2013). As principais normas e guias sobre gestão de riscos são apresentados no Tabela 1.

NORMA	ORIGEM	LANÇAMENTO	REVISÃO	DESCRIÇÃO
AS/NZS 4360	Austrália e Nova Zelândia	1995	1999 e 2004	Primeira norma de Gestão de Riscos, servindo de base para definição da norma ISO 31000
HB 436	Austrália e Nova Zelândia	2004	-	Guia para gestão de riscos, anexo da norma AS/NZS 4360:2004
JSI Q 2001	Japão	2001	-	Apresenta definição formal de sistema de gestão de riscos e introduz a melhoria contínua
Guia 73	Internacional	2002	2009	Documento normativo anexo à norma ISO 31000:2009
ISO 31000	Internacional	2009	-	Abrange todos os tipos de risco em qualquer contexto. Construída em torno de três pilares: princípios de gestão de riscos, guia de gestão de riscos e processo de gestão de riscos

Fonte: Baseado em Leitch (2010) e Preda (2013)

Tabela 1 - Principais normas de gestão de riscos

Christensen *et al.* (2003), argumentam que o campo da terminologia é naturalmente fonte de

ambiguidade, gerando controvérsias em muitas áreas científicas, não sendo diferente, portanto, na identificação, estimação, regulação e comunicação do risco.

Devido à importância do tema, a versão 2008 da norma ISO 9001 incorporou requisitos indiretamente ligados à gestão de riscos, tangendo análise gerencial, recursos humanos, infraestrutura, análise dos requisitos relativos ao produto, controle de projeto e desenvolvimento (PREDA, 2013). Já nas revisões das normas ISO 9001:2015 e ISO 14001:2015 é prevista uma vinculação estrutural mais evidente com a gestão de riscos.

Este artigo apresenta uma revisão bibliográfica focada na gestão de riscos, na qual abrange-se principalmente a norma internacional ISO 31000, se concentrando em seus principais fundamentos, características, estrutura e críticas. Aborda-se brevemente a norma certificável QSP 31000, baseada na norma ISO 31000. O propósito maior deste artigo é compilar conhecimento a respeito da gestão de riscos e, principalmente, de uma norma internacional relativamente recente.

Este artigo se divide em cinco seções, incluindo esta, que estabelece a introdução do trabalho. Na seção dois, aborda-se a norma internacional de gestão de riscos ISO 31000, apresentando o conceito de risco estabelecido, sua estrutura, sua organização, seu processo de gestão de riscos e algumas críticas publicadas. Na seção três comenta-se a abordagem de risco na estrutura prevista na nova versão das normas ISO 9001:2015 e ISO 14001:2015. Na seção quatro, é realizada uma breve descrição da norma QSP 31000. Na seção cinco, são realizadas as considerações finais.

2. A Norma ISO 31000

Em 2009, o organismo ISO publicou a norma internacional ISO 31000, genericamente aplicável ao gerenciamento de todas as formas de risco em qualquer contexto industrial (PURDY, 2010).

Entre as principais normas de gestão de risco, a ISO 31000 ocupa papel de destaque, devido ao reconhecimento internacional do organismo ISO (*International Organization for Standardization*). A estrutura da norma ISO 31000 contém (PURDY, 2010):

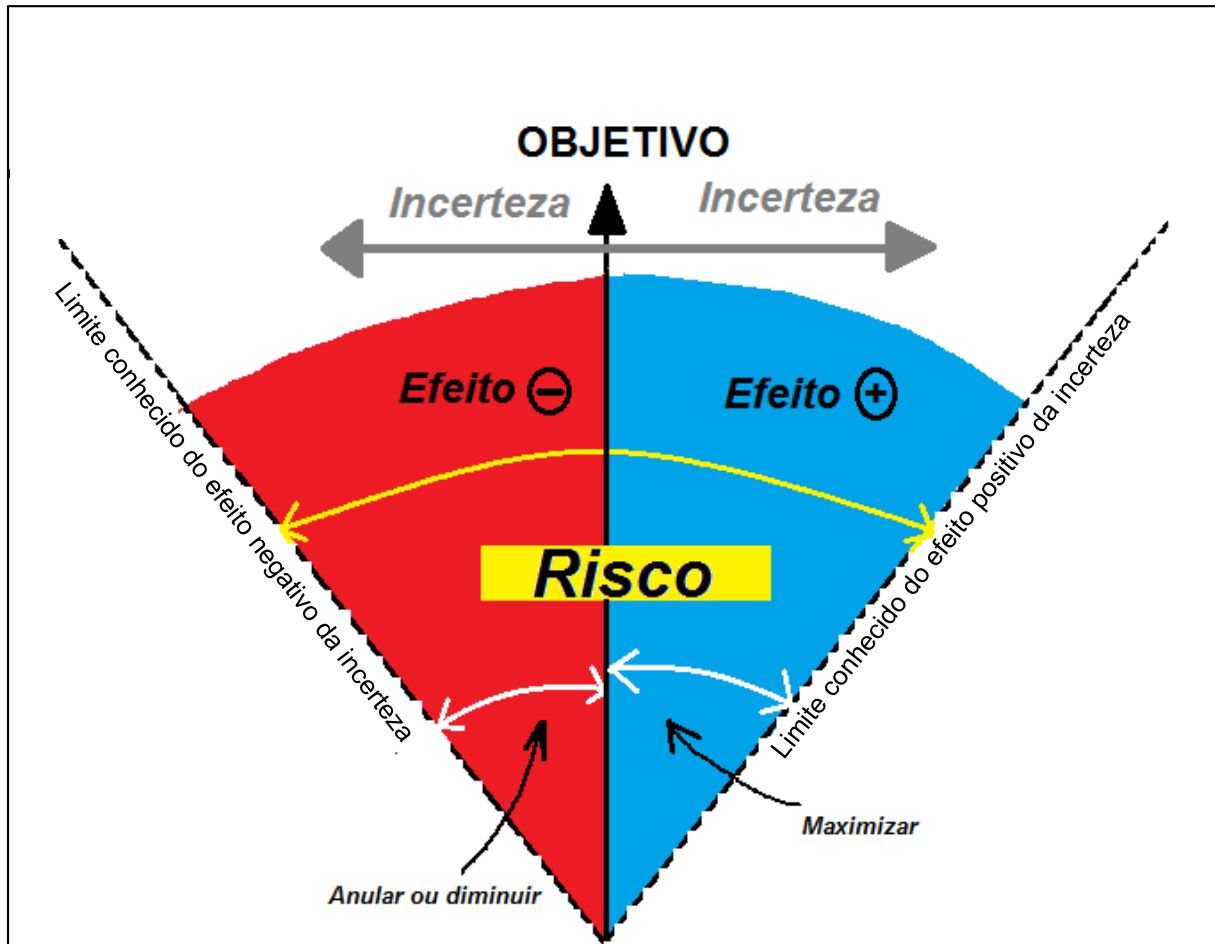
- a) Vocabulário;
- b) Conjunto de critérios de desempenho;
- c) Processo abrangente comum para a identificação, análise, avaliação e tratamento de riscos;
- d) Guia de como o processo de gestão de risco pode ser integrado ao processo de tomada de decisão de qualquer organização.

A definição de risco na norma ISO 31000 muda a preocupação de alguma coisa acontecer pela probabilidade de um efeito nos objetivos. Nesse sentido, gerenciar riscos é um processo de otimização que promove o alcance do objetivo mais provável, assumindo que o risco é fato corriqueiro, não sendo inerentemente bom ou ruim (PURDY, 2010).

Na realidade, a gestão de riscos se associa cada vez mais a ambos os aspectos positivos e negativos das atividades, buscando maximizar o primeiro e anular ou diminuir o segundo (FERMA, 2003).

A Figura 1 oferece uma possível interpretação do risco sobre o objetivo de uma atividade organizacional genérica. A seta central aponta para o objetivo planejado de uma atividade qualquer que, sob efeito da incerteza, está sujeito a produzir resultado real negativo ou abaixo da expectativa (setor limitado pela reta pontilhada à esquerda), bem como positivo ou acima da expectativa (setor limitado pela reta pontilhada à direita). A amplitude da seta interna de ponta dupla representa o risco como produto da incerteza conhecida sobre o objetivo, abrangendo os

efeitos negativo e positivo. Ressalta-se que a probabilidade relacionada aos efeitos positivo e negativo não são necessariamente iguais. Pelo contrário, idealmente o propósito da gestão de riscos é identificar, compreender e tratar o risco de forma a aumentar a probabilidade de atingir-se o efeito positivo em detrimento do efeito negativo.



Fonte: Elaboração própria

Figura 1 – Interpretação do risco como efeito da incerteza sobre o objetivo

A ISO 31000 apresenta um conjunto de opções genéricas a serem consideradas enquanto um risco é tratado, as quais são (PURDY, 2010):

- Anular o risco, decidindo não dar início ou não prosseguir com a atividade que lhe dá origem;
- Assumir ou aumentar o risco em busca de uma oportunidade;
- Remover a fonte do risco;
- Alterar a probabilidade do risco;
- Mudar as consequências do risco;
- Compartilhar o risco com outra(s) parte(s) (o que inclui contratos e financiamento de risco);
- Reter o risco com decisão fundamentada.

Aven (2011) esclarece que a “avaliação do risco” pertence a um domínio diferente da “tomada de decisão”. Em outras palavras, a primeira atividade dá suporte à segunda, não necessariamente prescrevendo como o risco deve ser tratado.

Segundo Preda (2010), é importante reconhecer que implementar a norma de gestão de riscos representa um desafio por diversas razões, podendo listar:

- a) A norma de gestão de riscos representa algo relativamente novo para muitas organizações;
- b) A norma de gestão de riscos precisa ser ajustada às características e necessidades da organização, requerendo comprometimento da alta direção e apoio de todas as pessoas envolvidas no processo de gestão de riscos;
- c) Alto investimento somado à dificuldade de implementação sem consideração de apoio de consultoria.

São características atribuídas à eficácia da gestão de riscos na norma ISO 31000 (PURDY, 2010):

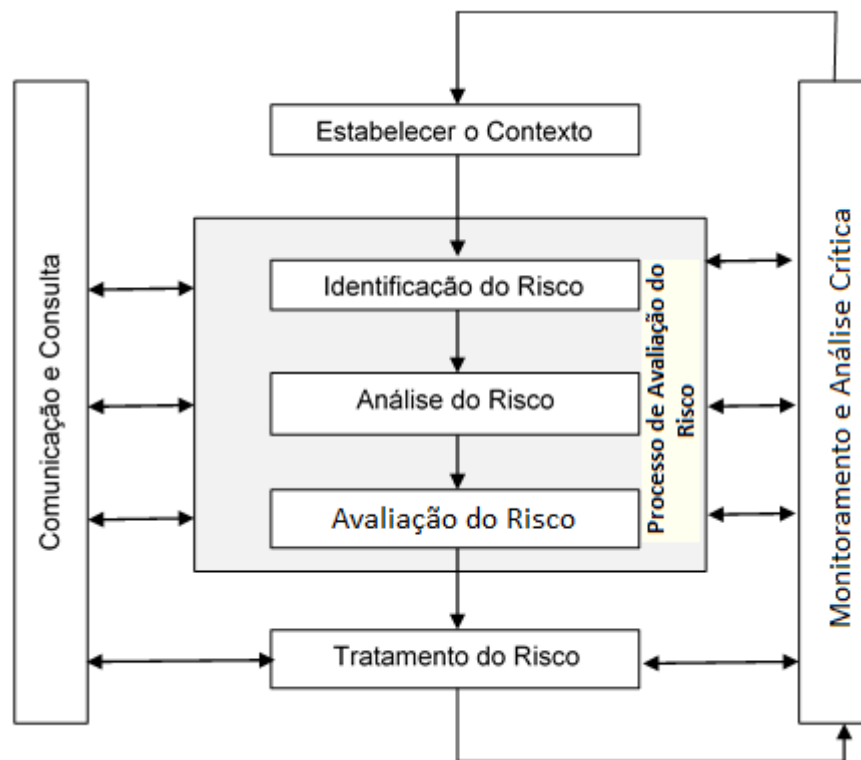
- a) Criar e proteger valor;
- b) Constituir parte integral de todo processo organizacional;
- c) Fazer parte da tomada de decisão;
- d) Fazer referência explícita à incerteza;
- e) Ser sistemática, estruturada e oportuna;
- f) Ser embasada na melhor informação disponível;
- g) Se adequar às necessidades;
- h) Considerar fatores humanos e culturais;
- i) Ser transparente e inclusiva;
- j) Ser dinâmica, iterativa e responsiva à mudança;
- k) Facilitar o processo de melhoria contínua da organização.

Atualmente, a norma ISO é composta pelas seguintes normas e complementos (ISO, 2015):

- a) ISO 31000:2009: princípios e diretrizes;
- b) Guia 73:2009: vocabulário;
- c) ISO/IEC 31010:2009: técnicas para o processo de avaliação de riscos;
- d) ISO/TR 31004:2010 – orientação para implementação da ISO 31000.

2.1 Processo de Gestão de Riscos

Na abordagem da norma ISO 31000, o processo de gestão de riscos é representado pelo diagrama mostrado na Figura 2.



Fonte: Adaptado de Purdy (2010, p. 883)

Figura 2 – Diagrama do processo de gestão de riscos da norma ISO 31000

As etapas contidas no diagrama da Figura 1 são explicadas como segue (PURDY, 2010):

- a) Estabelecer o Contexto – dispara o processo de avaliação do risco, definindo o que a organização quer alcançar e os fatores internos e externos que podem influenciar o sucesso do alcance desses objetivos;
- b) Identificação do risco – implica a aplicação do processo sistemático para compreender o que pode acontecer, como, quando e por quê;
- c) Análise do risco – se relaciona com a compreensão de cada risco, suas consequências e probabilidades;
- d) Avaliação do risco – envolve tomada de decisão sobre o nível do risco e prioridade de atenção através da aplicação do critério desenvolvido na ocasião em que o contexto foi estabelecido.
- e) Tratamento do risco – se refere ao processo pelo qual os controles existentes são aperfeiçoados ou novos controles são desenvolvidos e implementados. Compreende a avaliação e seleção de opções, o que inclui análise de custos e benefícios e avaliação de novos riscos que podem ser gerados a partir de cada opção e, desse modo, priorizando e implementando o tratamento selecionado segundo o processo planejado.

Os elementos “comunicação e consulta” e “monitoramento e análise crítica” são considerados agentes de ação contínua do processo de gestão de riscos. A comunicação e consulta implica no envolvimento de *stakeholders* internos e externos, objetivando considerar seus pontos de vista, conhecendo seus objetivos por meio de envolvimento planejado. O monitoramento e análise crítica preveem a tomada de ação no momento em que surgirem novos riscos que mudem os riscos existentes, como produto de mudança nos objetivos organizacionais ou nos ambientes interno e externo (PURDY, 2010).

Purdy (2010) ressalta que o objetivo do diagrama apresentado na norma ISO 31000 não é prover propriamente um fluxograma da gestão de riscos, mas mostrar o relacionamento entre cláusulas da norma que definem tal processo.

De acordo com Preda (2013), os passos recomendados para implementar a ISO 31000 são:

- a) Conquistar apoio/adesão da direção para implementação da norma, incluindo recursos necessários;
- b) Formar comitê de implementação, cujo gerente representante da organização seja apontado pela alta direção. Pessoas com bom conhecimento sobre os processos organizacionais e boa comunicação oral e escrita devem ser incluídas como membros (o papel pode ser desempenhado pelo gerente da qualidade ou da informação);
- c) Estabelecer plano de implementação que descreva o processo, as especialidades necessárias e as funções;
- d) Prover treinamento e suporte técnico;
- e) Organizar atividades de conscientização, comunicando o objetivo da implementação da norma de gestão de riscos, suas vantagens, seu funcionamento, funções e responsabilidades;
- f) Garantir que o processo baseado na norma esteja alinhado aos processos da organização;
- g) Desenvolver documentos de gestão de riscos (política, plano, processo, instruções de trabalho);
- h) Obter aprovação da diretoria para toda documentação implementada;
- i) Publicar, informar e obter *feedback* dos envolvidos;
- j) Implementar o processo de gestão de riscos (podendo realizar período de teste);
- k) Realizar auditoria interna;
- l) Realizar análise crítica pela diretoria.

2.3 Críticas à norma ISO 31000

Leitch (2010) aponta que por consequência da norma ISO 31000 se estabelecer de forma internacional e amplamente aplicável a todas as atividades industriais, ela influenciará significativamente conceitos e, portanto, a própria linguagem utilizada por ícones da área, fazendo com que algumas ideias sobre gerenciamento de riscos ganhem ênfase em detrimento de outras.

Apesar da importância da norma ISO 31000 para a gestão de riscos, são expressivas a responsabilidade e a dificuldade de tanger uma área tão complexa. Leitch (2010) expõe uma série de falhas, fraquezas e inconsistências observadas na norma ISO 31000, conforme se observa exemplos na Tabela 2.

ASPECTO	TIPO	EXPLANAÇÃO
Terminologia	Inconsistência	- Muitas definições de termos usados na norma utilizam palavras cujos significados são mais confusos que o próprio termo em definição (e.g. “estrutura de gestão de riscos” é definida como um conjunto de “componentes”) - Evita termos matemáticos, utilizando palavras com sentido genérico e impreciso (e.g. não há definição clara para as palavras “probability” e “likelihood”)
Escolha dos tratamentos para os riscos	Falha	A abordagem prescreve a precipitação da tomada de decisão, levando a escolhas ilógicas
Agregação dos riscos	Fraqueza	Apesar da norma considerar a possibilidade de ocorrer mais de um risco ao mesmo tempo no critério de risco, não há orientação sobre sua agregação
Conformidade com a norma	Falha	Atualmente a norma não é auditável e inclui requisitos que não podem ser cumpridos na prática

Fonte: Baseado em Leitch (2010)

Tabela 2 - Exemplos de falhas, fraquezas e inconsistências na norma ISO 31000

3. Abordagem do risco nas novas normas ISO e revisão das suas normas existentes

Reafirmando-se a importância da gestão de riscos de forma geral nos processos de gestão, as revisões definitivas das normas ISO 9001:2015 e ISO 14001:2015, além de preverem uma estrutura de alto nível visando facilitar o processo de integração de seus sistemas, elas devem especificar também requisitos com a finalidade de propiciar entendimento do conceito de risco e da determinação dos riscos como uma base para o planejamento e implementação dos processos desses sistemas de gestão (ABNT/CB-025, 2015; ABNT/CB-038, 2015). Todas essas mudanças estão previstas nas diretivas do Anexo SL (FONSECA, 2014; BSI, 2015; DE CICCIO, 2015; ISO, 2015b; TÜVRHEINLAND, 2015)

De forma particular, a revisão da norma ISO 9001:2015 introduz a “mentalidade de risco”, que consiste em considerar e tratar o risco como atividade rotineira nas atividades e processos da organização (ISO/TC 176/SC2, 2014) e sua inclusão confere mais credibilidade à norma (FONSECA, 2014). Tal conceito esteve implícito em edições anteriores dessa norma, como, por exemplo, na realização de ações preventivas (ABNT/CB-025, 2015). Uma das mais importantes mudanças previstas é a utilização de uma abordagem sistemática do risco, ao invés de trata-lo como componente isolado do sistema de gestão da qualidade, implicando sua consideração em toda a norma (ISO/TC 176/SC2, 2014; FERREIRA, 2014).

É importante ressaltar que em ambas as versões revisadas das normas ISO 9001:2015 e ISO 14001:2015 as ditas “ações preventivas” presentes em suas versões ainda em vigor deverão ser substituídas pela abordagem de avaliação do risco (ABNT/CB-025, 2015; ABNT/CB-038, 2015).

Note-se que as mudanças previstas devem ser aplicadas também nos novos lançamentos de normas ISO, bem como na revisão de suas normas existentes.

4. Norma QSP 31000

Em razão da norma ISO 31000 não ser certificável (LEITCH, 2010; BRIS; KECLÍKOVÁ, 2012; QSP, 2015; ISO, 2015a), o Centro da Qualidade, Segurança e Produtividade para o Brasil e América Latina – QSP, desenvolveu e lançou em 2010 uma norma certificável denominada QSP 31000, baseada na norma ISO 31000. Para tanto, a norma QSP 31000 englobou grande parte da ISO 31000, transformando suas recomendações em itens objetivamente verificáveis.

A estrutura para a gestão de riscos foi transformada em um Sistema de Gestão de Riscos (SGR), agregando requisitos de documentação, auditoria interna etc. (QSP, 2015).

Segundo QSP (2015), as vantagens de se implementar um SGR segundo a norma QSP 31000 compreendem:

- a) Aumento da probabilidade de atingir objetivos;
- b) Estímulo à gestão proativa;
- c) Atenção constante às necessidades de identificar e tratar riscos na organização;
- d) Capacidade aguçada de identificar oportunidades e ameaças;
- e) Garantia de conformidade à normas internacionais e requisitos legais e regulamentares pertinentes;
- f) Melhoria da comunicação das informações financeiras;
- g) Melhoria da governança;
- h) Aumento da confiança entre *stakeholders*;
- i) Base confiável para tomada de decisão e planejamento;
- j) Melhoria de controles;
- k) Alocação e utilização com eficácia de recursos destinados ao tratamento de riscos;
- l) Melhoria da eficácia e eficiência operacional;
- m) Melhoria do desempenho em segurança e saúde e proteção ao meio ambiente;
- n) Melhoria da prevenção de perdas e a gestão de incidentes;
- o) Melhoria da aprendizagem organizacional;
- p) Aumento da resiliência da organização.

Destaca-se que há pouca publicação sobre a norma QSP 31000, o que dificulta a obtenção de maiores detalhes sobre seu processo de implementação e certificação.

5. Considerações Finais

Realizou-se neste artigo uma revisão bibliográfica sobre a gestão de riscos, abordando com maior detalhamento a norma internacional ISO 31000. Tendo em vista a importância da gestão de riscos, sublinhada neste artigo na previsão da incorporação da abordagem do risco em importantes normas, citando as novas versões das normas ISO 9001:2015 e ISO 14001:2015, assim como em todas as novas normas ISO e futuras revisões de suas normas existentes. Foram abordadas tanto características positivas quanto críticas sobre a norma ISO 31000, sublinhando que, de modo geral, as normas de gestão de risco, apesar de bastante discutidas e difundidas, carecem de maior desenvolvimento para atingir o ponto de abranger, com devida suficiência, todos os aspectos relevantes que envolvam a gestão de riscos, principalmente no tocante à análise do risco e à tomada de decisão.

Até atingir-se tal ponto, apesar da expectativa de inclusão da avaliação de risco na estrutura das novas normas ISO e futuras revisões de suas normas existentes, estima-se que haja um longo caminho a ser percorrido, demandando esforços tanto acadêmicos quanto empíricos, a começar por estabelecer uma terminologia consensual, mais adequada e funcional.

Concluindo, acredita-se não restarem dúvidas a respeito da importância da gestão de riscos no âmbito de qualquer sistema de gestão. Pelo contrário, aponta-se aqui uma provável indissociabilidade entre a gestão de riscos e as atividades organizacionais. Em que se pese ao esforço de desenvolvimento da norma QSP 31000, ressalta-se que a norma ISO 31000 se limita a princípios e recomendações para a estruturação do processo de gestão de risco, não estabelecendo propriamente um modelo de sistema de gestão de riscos. Talvez o que justifique tal precaução ou impossibilidade seja, na realidade, uma condição da própria indissociabilidade,

não permitindo tratar completamente e de forma isolada o processo de gestão de risco desvinculado de um contexto, tanto em termos de disciplina à qual se refere (qualidade, meio ambiente, saúde e segurança etc.) quanto da própria organização à qual a norma seja aplicada.

Referências

ABNT-CB-025. Associação Brasileira de Normas Técnicas – Comitê Brasileiro de Gestão da Qualidade. *Projeto de revisão da norma NBR ISO 9001:2015*. 2015. Disponível em: <<http://www.qsp.org.br/app.shtml>>. Acesso em 02 set. 2015.

ABNT-CB-038. Associação Brasileira de Normas Técnicas – Comitê Brasileiro de Gestão Ambiental. *Projeto de revisão da norma NBR ISO 14001:2015*. 2015. Disponível em: <<http://www.qsp.org.br/app.shtml>>. Acesso em 02 set. 2015.

AVEN, T. *Selective critique of risk assessments with recommendations for improving methodology and practise*. Reliability Engineering and System Safety. Vol. 96, n. 5, p. 509-514, 2011.

BRIS, P.; KECLÍKOVÁ, K. *Quality process management in healthcare facilities*. In: European Conference on Management Leadership and Governance, 8., 2012, Pafos. Proceedings of the 8th European Conference on Management Leadership and Governance. Pafos: Neapolis University, 2012, p. 66-74.

BSI. British Standards Institution. *Apresentando o anexo SL: a nova estrutura de alto nível para todas as normas de sistemas de gestão do futuro*. 2015. Disponível em: < <http://www.bsigroup.com/LocalFiles/pt-BR/Entendendo%20o%20Anexo%20SL.pdf>>. Acesso em: 02 set. 2015.

CHRISTENSEN, F.M. et al. *Risk terminology: a platform for common understanding and better communication*. Journal of Hazardous Materials. Vol. 103, n. 3, p. 181-203, 2003.

DE CICCIO, F. *O que você deveria saber sobre a gestão de riscos nas novas ISO 9001 e ISO 14001:2015 (webinar)*. Disponível em: <<https://www.youtube.com/watch?v=7W8jieFiwFE&feature=youtu.be&list=PLcctAmzruX5iUmGN7ZIU2TZRGilU6pqJ>>. Acesso em 01 de set. 2015.

FERREIRA, M. *A norma ISO 9001:2015: nova estrutura e alterações previstas*. 2014. Disponível em <http://www.ctcv.pt/seminarios/iso/conteudos/MF_ISO%209001_14001%20CTCV.pdf>. Acesso em 07 set. 2015.

FERMA. Federation of European Risk Management Association. *Norma de gestão de riscos*. 2003. Disponível em: < <http://www.ferma.eu/app/uploads/2011/11/a-risk-management-standard-portuguese-version.pdf>>. Acesso em: 14 jan. 2015.

FONSECA, L.M. *ISO 9001:2015 revision*. In: International Conference on Quality Engineering and Management, 1., 2014, Guimarães. Proceedings of the 1st International Conference on Quality Engineering and Management. Guimarães: ICQEM, 2014, p. 391-400.

ISO. International Organization for Standardization. *Introduction to ISO 14001:2015*. 2015a. Disponível em: < www.iso.org/iso/introduction_to_iso_14001.pdf>. Acesso em: 15 set. 2015.

ISO. International Organization for Standardization. *ISO 31000:2009*. 2015b. Disponível em :< http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=43170>. Acesso em: 13 jan. 2015.

ISO/TC 176/SC2. *“Risk” in ISO 9001:2015. Document N1222*. 2014. Disponível em <https://www.standard.no/Global/PDF/Kvalitet/ISO-TC176-SC2_N1222_N1222_-_Risk_in_ISO_9001_2014-07.pdf>. Acesso em: 15 set. 2015.

LEITCH, M. *ISO 31000: 2009: the new international standard on risk management*. Risk Analysis. Vol. 30, n. 6, p. 887-892, 2010.

PRED, C. *Implementing a risk management standard*. Journal of Defense Resources Management. Vol. 4, n. 1, p. 111-120, 2013.

PURDY, G. *ISO 31000 2009: setting a new standard for risk management*. Risk Analysis. Vol. 30, n. 6, p. 881-886, 2010.

QSP. Centro da Qualidade, Segurança e Produtividade. *Gestão de riscos*. Disponível em: <http://www.qsp.org.br/gestao_riscos.shtml>. Acesso em: 20 fev. 2015.

STATE OF VICTORIA. *Victorian government risk management framework practice guide*. 2015. Disponível em :<<https://www.vmia.vic.gov.au/~media/internet/content-documents/risk/risk-tools/risk-management-guide/vmia-practice-guide-may-2015.pdf>>. Acesso em 30 set. 2015.

TÜVRHEINLAND. *Revisão da norma ISO 9001:2015: mudanças e seu impacto*. 2015. Disponível em: <http://www.tuv.com/media/portuguese/newsletter_pdf/november/Article_1_-_Iso9001.pdf>. Acesso em 15 set. 2015.