

# A IMPLEMENTAÇÃO DA GESTÃO DE RISCOS À RESPONSABILIDADE SOCIAL COMO ESTRUTURAÇÃO PARA A SUSTENTABILIDADE E A GESTÃO DO CONHECIMENTO

*SIMÕES, Reinaldo Augusto Gomes*

## **Resumo**

Organizações dos mais variados tipos, naturezas, portes e locais almejam desempenho eficaz, não mais apenas financeiro, mas também ambiental e social, na busca da sustentabilidade organizacional ou desenvolvimento sustentável. Buscam na ISO 26000 um guia de referência e orientação. Todavia, vêm encontrando dificuldades em sua implementação, pois os temas de responsabilidade social formalizados pela nova norma são por demais variados e abrangentes. Por sua vez, a norma ISO 26000 tampouco apresenta uma sistemática ou modelo para sua implementação. Organizações também buscam gerenciar os riscos que ameaçam seus objetivos e têm recorrido com sucesso à recente norma ISO 31000, que oferece uma estrutura e um processo para se gerenciar riscos de qualquer tipo ou natureza. Este trabalho tem como objetivo apresentar os elementos e o processo de gestão de riscos da ISO 31000 como sistemática para se implementar a gestão da responsabilidade social, tendo-se como base as orientações da ISO 26000, com a finalidade de contribuir para a sustentabilidade organizacional, e oportunizar a gestão do conhecimento de uma organização de natureza qualquer. Utiliza como metodologia a análise do conteúdo das normas e conclui que é viável a concepção, planejamento e implementação de uma “gestão de riscos à responsabilidade social” que contribua para o desenvolvimento sustentável das organizações.

Palavras-chave: Gestão de riscos. Gestão da responsabilidade social. Sustentabilidade.

## **1 Introdução**

A gestão de riscos é uma prática administrativa que vem sendo aplicada pelos mais variados tipos de organizações há décadas, na tentativa de mitigar (ou oportunizar) diferentes tipos de riscos, através da aplicação de diferentes estratégias e metodologias, mas todas semelhantes e utilizando referenciais conceituais análogos. Como exemplos, desde os estudos relacionados às companhias de seguros e previdência, com seus cálculos atuariais; as instituições financeiras ao gerenciar desde sempre os riscos de mercado e de crédito e, mais recentemente, de liquidez e operacionais; a indústria aeronáutica, aeroespacial, nuclear, química, mecânica, alimentar e de outras especializações; o gerenciamento de projetos e de segurança da informação; as agências de inteligência governamentais; mais ultimamente, as instituições de saúde e hospitalares - o rol de aplicação é extenso e não se limita a estes segmentos.

O desenvolvimento sustentável, por sua vez, é preocupação mais recente dos governos, sociedades e organização de negócio. Dada sua história, que se pode avaliar como ainda incipiente – e à sua natureza de longo prazo – não se fala em gestão *da*, mas *para* a sustentabilidade, pois ainda não há métodos universais ou consenso para medir e gerenciar esta característica. Da mesma forma e tão recente quanto, a gestão do conhecimento e seus métodos de implementação vêm sendo um desafio a estimular acadêmicos e gestores organizacionais em todo o planeta.

Nos anos de 2009 e 2010, a comunidade normativa internacional conquistou finalmente a publicação de duas normas de gestão que, quando seguidas de forma competente, proporcionam um arcabouço para a implementação da gestão de riscos e da gestão de responsabilidade social – a ISO 31000 e a ISO 26000, respectivamente. A primeira apresenta um processo de gestão, enquanto a segunda os elementos que permitem à organização – seja em qual contexto estiver inserida e de qual natureza de atuação a caracterizá-la – comprometer-se e direcionar-se para o desenvolvimento sustentável.

Este trabalho tem como objetivo apresentar os elementos e o processo de gestão de riscos da ISO 31000 como sistemática para se implementar a gestão da responsabilidade social, tendo-se como base as orientações da ISO 26000, com a finalidade de contribuir para a sustentabilidade organizacional, e oportunizar a gestão do conhecimento de uma organização de natureza qualquer.

## **2 Referencial teórico**

### **2.1 A norma ISO 31000 para gestão de riscos**

A Organização Internacional para a Padronização definiu *risco* como “efeito da incerteza nos objetivos” (ABNT, 2009a, definição 2.1). Apesar de muitas organizações já incluírem dentre suas práticas e processos de gestão componentes que fazem parte ou encontram seus equivalentes na gestão de riscos, a norma de referência ISO 31000 pode orientar na condução de uma análise crítica em seus processos de gestão de riscos. Para estas e mesmo outras entidades que não apresentem nenhuma prática formal para gerenciar seus riscos, a norma presta-se para fornecer desde os princípios às diretrizes (genéricas) para este escopo de gestão. Justifica a implementação da gestão de riscos nas organizações que, no contexto atual, “enfrentam influências e fatores internos e externos que tornam incerto se e quando elas atingirão seus objetivos” (ABNT, 2009b, p. 4 e 5). Dentre as contribuições que a implementação da gestão de riscos pode trazer – através de um processo sistemático e lógico – a norma destaca:

- a) aumentar a probabilidade de atingir os objetivos;
- b) melhorar a governança;
- c) melhorar a confiança das partes interessadas;
- d) melhorar o desempenho em saúde, segurança e a proteção ao meio ambiente;
- e) melhorar a aprendizagem organizacional.

Portanto, desde sua introdução, a norma ISO 31000 apresenta um processo que pode auxiliar uma organização – e também garantir às partes interessadas desta (alínea c, acima) – que bons resultados financeiros e de negócio (na alínea b), sociais e ambientais (alínea d) serão mais provavelmente alcançados (alínea a).

Cabe já destacar que, como o próprio escopo da norma estipula, o documento não se destina a fins de certificação ou a servir de requisito de auditoria. Entretanto, alguns meses após sua publicação, já surgiram no mercado normas não oficiais e protocolos de auditoria, embasados e derivados da ISO 31000, que possibilitaram a organizações prestadoras de serviços de auditoria ou certificação emitir declarações de conformidade e certificados, especificamente para instituições hospitalares, financeiras e industriais.

A arquitetura oferecida pelo corpo principal da norma introduz os onze Princípios que devem ser atendidos, definidos pela primeira vez na literatura referente ao tema de riscos (ABNT, 2009b, seção 3) e determinando que a gestão de riscos:

- a) cria e protege valor;
- b) é parte integrante de todos os processos organizacionais;
- c) é parte da tomada de decisões;
- d) aborda explicitamente a incerteza;
- e) é sistemática, estruturada e oportuna;
- f) baseia-se nas melhores informações disponíveis;
- g) é feita sob medida;
- h) considera fatores humanos e culturais;
- i) é transparente e inclusiva;
- j) é dinâmica, iterativa e capaz de reagir a mudanças;
- k) facilita a melhoria contínua da organização.

Em sua seção 4, por sua vez, a ISO 31000 recomenda a implementação de uma estrutura – tradução brasileira para o termo original em inglês *framework*, traduzido em outras normas de gestão também pela palavra *arcabouço* – de gestão de riscos. A estrutura (ABNT, 2009a, definição 2.1.1) é constituída pelos componentes da organização que fornecem os fundamentos (por exemplo, a política, os objetivos, os mandatos e o comprometimento) e os arranjos (dentre os quais os planos, os relacionamentos, as responsabilidades, os recursos, processos e atividades) para a concepção, implementação, monitoramento, análise crítica e melhoria contínua da gestão. A eficácia de funcionamento desta estrutura é um dos determinantes para o sucesso dessa gestão de riscos. A estrutura proposta está reproduzida na figura 1: nela reconhece-se seguir o modelo cíclico do *Plan-Do-Check-Act* (PDCA) de William Edwards Deming (todavia não mencionado em nenhum trecho da norma) e traz de início, em seu topo, o necessário mandato e comprometimento pela alta administração da organização a implementar a gestão de riscos.

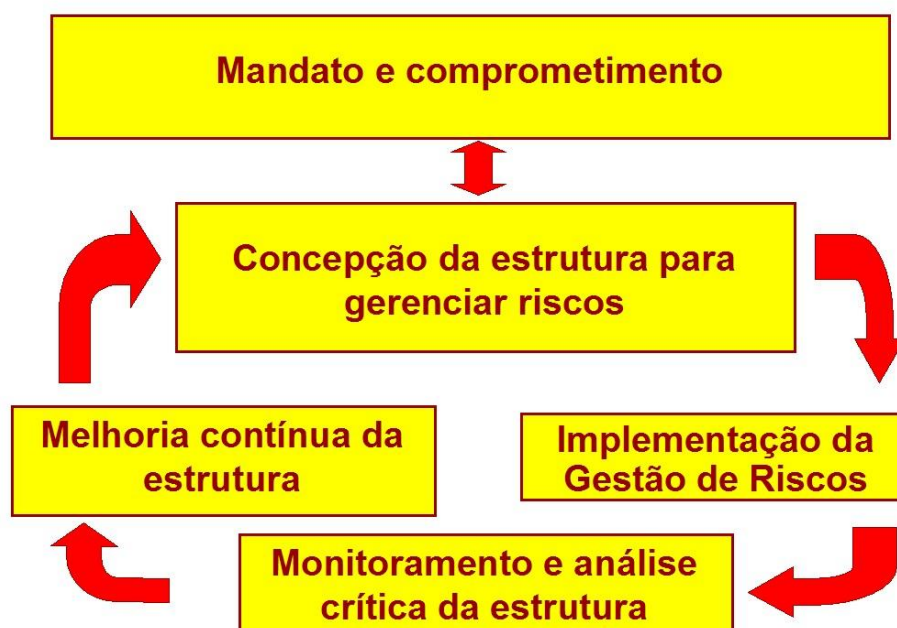


Fig. 1 – Relacionamento entre os componentes da estrutura para gerenciar riscos (adaptado de ABNT, 2009b, figura 2).

Não é propósito deste trabalho detalhar esta estrutura, mas apenas o componente da Concepção, pois auxiliará nos objetivos propostos. Para o desempenho eficaz, a norma não estipula um sistema de gestão, mas sim orientações para auxiliar a integrar, através desta estrutura, a gestão de riscos no sistema de gestão (formal ou não) global da organização. Dentre as atividades para concepção (planejamento) da estrutura, a ISO 31000 inclui os seguintes elementos:

- a) entendimento da organização e de seu contexto – avaliar previamente o contexto externo (inclui ambientes, fatores-chave, tendências, relações e percepções das partes interessadas externas) e o contexto interno (inclui governança e estrutura organizacional; políticas, objetivos e estratégias; capacidades; sistemas de informação; relações e percepções das partes interessadas internas);
- b) estabelecimento da política de gestão de riscos – estabelecer claramente os objetivos e o comprometimento da organização;
- c) responsabilização – assegurar responsabilidades e autoridades para gerenciar riscos e seu reconhecimento;
- d) integração nos processos organizacionais – incorporar a gestão de riscos a todas as práticas e processos; elaborar plano de gestão de riscos para toda a organização);
- e) recursos – alocar recursos relacionados a pessoas; processos, métodos e ferramentas; procedimentos; sistemas de gestão da informação e conhecimento; treinamento.
- f) estabelecimento de mecanismos de comunicação e reporte internos;
- g) estabelecimento de mecanismos de comunicação e reporte externos.

Em sua seção 5, a ISO 31000 recomenda a implementação de um processo de gestão de riscos, conforme representado na figura 2. Processos semelhantes são encontrados em diversas referências e guias conhecidos para a gestão de riscos de tipos específicos, como nas publicações pelo *Project Management Institute (PMI)* e seu *Project Management Body of Knowledge (PMBOK)*, pelo *Committee of Sponsoring Organizations of the Treadway Commission (COSO)*, *Occupational Health and Safety Assessment Series* (norma *OHSAS 18001*), norma de gestão de riscos em segurança da informação (*ISO/IEC 27005*) e outras publicações. Mas este processo, baseado no anteriormente proposto pela norma australiano-neozelandesa *AS/NZS 4360*, é genérico para qualquer tipo de natureza de riscos.

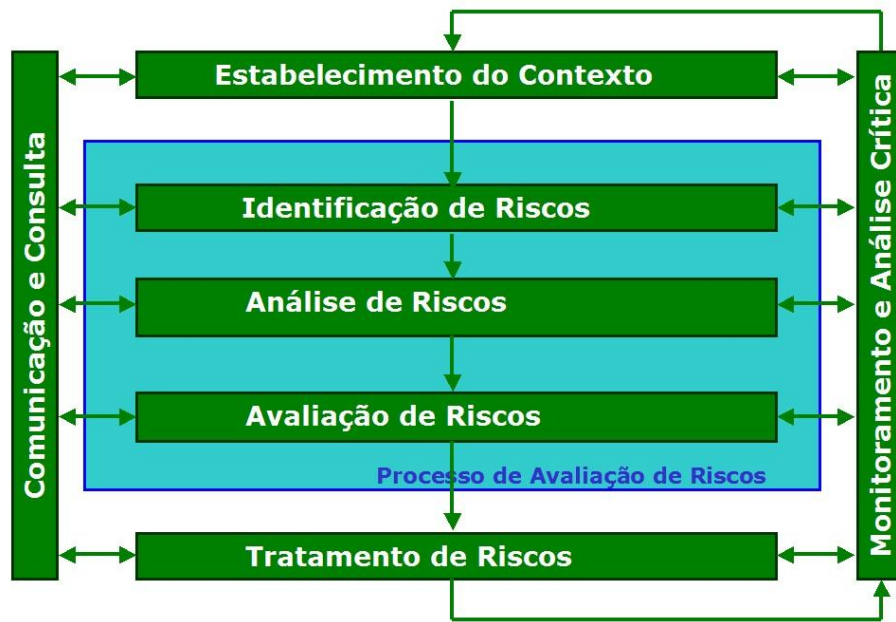


Fig. 2 – Processo de gestão de riscos (adaptado de ABNT, 2009b, figura 3).

O processo também é caracterizado pela utilização do modelo cíclico do PDCA (não mencionado na ISO 31000). Destaca-se o eixo central, com um bloco interno que representa o *risk assessment* (termo em inglês traduzido na norma brasileira como “processo de avaliação de riscos”) e que equivale à avaliação global do risco.

Estes são os elementos do processo de gestão de riscos:

- a) comunicação e consulta;
- b) estabelecimento do contexto;
- c) identificação de riscos;
- d) análise de riscos;
- e) avaliação de riscos;
- f) tratamento de riscos;
- g) monitoramento e análise crítica.

A concepção do processo é um dos destaques desta norma. O processo em si é lógico e sistemático, cíclico, sem um ponto de início, mas a norma começa por descrever o elemento de Comunicação e Consulta (ABNT, 2009b, item 5.2). A característica mais marcante da comunicação e consulta na ISO 31000 é sua recomendação de que ela seja aplicada logo no início da implementação do processo e que envolva as partes interessadas internas e externas durante todo o decorrer das fases do processo de gestão de riscos. Em outros termos: a comunicação e a consulta devem ocorrer contínua e permanentemente: esta é uma elemento-chave que a prática demonstra caracterizar a gestão de qualquer organização com desempenho eficaz (seja uma empresa pública ou privada, uma instituição, um empreendimento, um grupo, uma família).

Em seguida, a norma aborda novamente o Estabelecimento do Contexto, reproduzindo literalmente parte do texto e das recomendações descritas na seção da Estrutura – o que permite interpretar que, a cada oportunidade de implementação do processo de gestão de riscos, o contexto da organização seja restabelecido, renovado, atualizado, referenciado para a situação em questão. Mas além dos contextos externo e interno da organização, a norma

recomenda o estabelecimento do contexto do processo de gestão de riscos: para a atividade ou parte de organização em que o processo está sendo aplicado, é sugerido estabelecer seus objetivos, escopo, estratégias e parâmetros. Esta recomendação é coerente e consistente em relação à própria definição de risco: para se gerenciar os riscos, é previamente necessário conhecer os objetivos que podem ser especificamente afetados. Para a adequada avaliação dos riscos, a norma também orienta que neste momento, previamente, sejam já definidos os critérios de avaliação de riscos (que só serão aplicados em etapa posterior à identificação e análise dos riscos).

Segue-se o bloco chamado “processo de avaliação de riscos”, compreendendo a identificação do risco (com suas fontes e causas, eventos de risco, conseqüências), seguida pela análise do risco (atribuição de valores qualitativos ou quantitativos de probabilidades – ou frequências – e de conseqüências – também denominadas em outras metodologias como gravidade, severidade ou magnitude dos efeitos potenciais – e a combinação destes valores num valor único, o chamado nível do risco). Este processo de avaliação se finaliza pela avaliação do risco propriamente dita, ou seja, pela comparação do nível do risco com um critério de referência de risco (previamente definido na fase de contextualização) que vai indicar a aceitação do risco na situação atual ou a definição de tratamentos que irão mitigar o risco negativo ou aumentar o risco positivo.

O resultado da avaliação fornece uma indicação para o gestor proprietário do risco de uma opção de aceitação ou não do risco. Entretanto, a decisão final é de sua responsabilidade. A fase de Tratamento de riscos é aquela que envolve a seleção entre uma ou mais opções para modificar o nível do risco, e sua implementação (imediate ou na forma de um plano de tratamento de riscos – a forma como a ISO 31000 nomeia os também chamados planos de ação ou programas de gestão). Aqui são fundamentais as competências do gestor e das equipes no equilíbrio entre os custos e esforços para implementação, e os benefícios decorrentes, relacionado aos objetivos e também relativos a requisitos legais, requisitos regulamentares e, neste item (ABNT, 2009b, item 5.5.2) a norma explicita a responsabilidade social e a proteção ao meio ambiente: neste ponto pode ser articulada a gestão de riscos com a gestão da responsabilidade social e a gestão para o desenvolvimento sustentável.

Finalmente, processo de gestão de riscos conforme a ISO 31000 abrange o Monitoramento e a Análise Crítica: devem ser planejados desde o início do processo como parte integrante da gestão de riscos e envolver verificação (checagem) e vigilância (supervisão e inspeção) regulares, podendo ocorrer periodicamente ou como resposta a um fato ou evento específico – em suma, acompanhamento permanente.

Este é outro elemento de destaque no processo de gestão proposto pela norma, pois, assim como a Comunicação e Consulta, também o Monitoramento deveria ocorrer contínua e permanentemente ao longo de todo o processo, abordando os tratamentos e planos de tratamento dos riscos; a avaliação, análise (probabilidades e conseqüências) e a identificação de riscos, o aparecimento de novos riscos; o acompanhamento dos contextos – enfim, tanto a estabilidade quanto toda e qualquer mudança a ocorrer. Outro grande segredo da boa gestão, conjuntamente à comunicação e consulta regulares, é o monitoramento contínuo, o chamado popularmente como “olho do dono”. Lamentavelmente, em épocas de restrição de recursos e enxugamento de processos, a nobre função de monitoramento do gestor é em geral relevada.

Encerra a norma ISO 31000 um item relativo a registros do processo de gestão de riscos (ABNT, 2009b, item 5.7). Como não se trata de norma voltada a auditoria ou certificação, ela

não se constitui de requisitos – mas de recomendações – e não prescreve a necessidade de procedimentos (documentados ou formais, ou não). A rastreabilidade (e a preservação do conhecimento) das atividades, o planejamento e a fundamentação para a melhoria pode se dar através de registros (não necessariamente controlados de modo formal). O modo de registrar, conforme recomendado pela norma, deveria levar em consideração, por exemplo, as necessidades de aprendizagem; os benefícios da reutilização de informações; os custos de manutenção de registros; as necessidades de registros legais, regulamentares e operacionais; acessibilidade e facilidade de recuperação e outros fatores da organização.

## **2.2 A norma ISO 26000 para gestão da responsabilidade social**

Em novembro de 2010 publicou-se em Genebra, Suíça, a norma ISO 26000 de diretrizes sobre responsabilidade social (ABNT, 2010), sendo a versão brasileira elaborada pela Comissão de Estudo Especial de Responsabilidade Social, que também participou da criação do documento internacional. Foi elaborada na busca de atender as organizações e suas partes interessadas em termos de comportamento socialmente responsável, preocupadas no contexto mundial atual da necessidade de um desempenho organizacional não apenas em termos de lucro, mas em relação aos impactos na sociedade em que opera e no meio ambiente. Vem para atender às preocupações de que, a longo prazo, as atividades da organização dependem da saúde dos ecossistemas (locais e mundiais) e das características da sociedade em que estão inseridas (também em abrangência universal). Afirma que “o objetivo da responsabilidade social é contribuir para o desenvolvimento sustentável”.

Em sua Introdução, esta norma defende que o desempenho em responsabilidade social e a percepção da organização pelas suas partes interessadas poderão influenciá-la em termos de vantagem competitiva; reputação; capacidade de atrair e manter trabalhadores (crítica no Brasil no momento atual), conselheiros, acionistas, sócios e clientes; moral, comprometimento e produtividade dos empregados e funcionários; percepção de investidores e patrocinadores em geral e na relação com outras empresas, governos, mídia, pares, clientes e comunidade.

Assim como a ISO 31000, é uma norma de diretrizes e orientações – e não de requisitos, auditoria, nem voltada a certificações – e é genérica, voltada para organizações de qualquer tipo, porte ou localização.

A norma traz já em sua parte introdutória a figura de uma visão geral esquemática (ABNT, 2010, figura 1), não reproduzida neste artigo. Não faz parte do conjunto de sessões da norma e sua finalidade se limita a ajudar na compreensão do extenso documento (mais de 110 páginas). Não se trata de modelo de sistema, estrutura, tampouco de processo de gestão. Não pode ser considerada um processo ou, nem é cíclica. Não inclui o desenvolvimento sustentável dentro de seu escopo, apenas como finalidade de contribuição.

Uma das características mais marcantes da ISO 26000 é sua vasta amplitude e o elevado grau de detalhamento em suas explicações, o que a torna, além de um guia, um verdadeiro manual de gestão da responsabilidade social. Quem a consulta, independentemente de sua área de formação ou atuação, obtém um verdadeiro “curso” de responsabilidade social, que traz as melhores e mais atualizadas práticas que uma organização pode reconhecer e selecionar para implementação. A tabela 1 contém as sete seções nas quais a norma se divide, acompanhadas de uma breve descrição de seus respectivos conteúdos.

Tabela 1 – Seções da norma ISO 26000 e resumo de seu conteúdo.

Seção	Nome	Conteúdo
1	Escopo	Fornece orientações diversas referentes à responsabilidade social (abordadas nas seções seguintes).
2	Termos e definições	27 termos e definições.
3	Compreensão da responsabilidade social	Histórico da responsabilidade social das organizações, tendências atuais e características da responsabilidade social.
4	Princípios da responsabilidade social	<ul style="list-style-type: none"> <li>- <i>Accountability</i> (prestação de contas);</li> <li>- transparência;</li> <li>- comportamento ético;</li> <li>- respeito pelos interesses das partes interessadas;</li> <li>- respeito pelo estado de direito;</li> <li>- respeito pelas normas internacionais de comportamento;</li> <li>- respeito pelos direitos humanos.</li> </ul>
5	Reconhecimento da responsabilidade social e engajamento das partes interessadas	Reconhecimento da responsabilidade social, identificação e engajamento das partes interessadas,



Tabela 1 – Seções da norma ISO 26000 e resumo de seu conteúdo (continuação).

Seção	Nome	Conteúdo
6	Orientações sobre temas centrais da responsabilidade social	<ol style="list-style-type: none"> <li>1. Governança organizacional;</li> <li>2. direitos humanos;</li> <li>3. práticas de trabalho;</li> <li>4. meio ambiente;</li> <li>5. práticas leais de operação;</li> <li>6. questões relativas ao consumidor;</li> <li>7. envolvimento e desenvolvimento da comunidade.</li> </ol>
7	Orientações sobre a integração da responsabilidade social por toda a organização	<ul style="list-style-type: none"> <li>- Relação das características de uma organização com a responsabilidade social.</li> <li>- Compreensão da responsabilidade social da organização.</li> <li>- Práticas para integrar a responsabilidade social em toda a organização.</li> <li>- Comunicação sobre responsabilidade social.</li> <li>- Fortalecimento da credibilidade em relação à responsabilidade social.</li> <li>- Análise e aprimoramento das ações e práticas relativas à responsabilidade social.</li> <li>- Iniciativas voluntárias de responsabilidade social.</li> </ul>

O texto da norma é também intercalado por 17 *boxes* contendo explicações e contextualização sobre órgãos internacionais, temas e exemplos de responsabilidade social, relação da norma com organizações, acordos internacionais e outros, que auxiliam o leitor no entendimento global da responsabilidade social.

A norma é recente e há poucas publicações sobre sua implementação. A *American Society for Quality (ASQ)* foi provavelmente a primeira organização a publicar um guia com recomendações para implementação da ISO 26000 (BERNHART, 2011), porém sem se basear em um modelo de gestão, mas sim em tópicos orientativos e sugere uma seqüência de etapas de implementação em formato de PDCA:

- a) conduzir uma autoavaliação;
- b) identificar e montar a equipe de implementação;
- c) engajar as partes interessadas internas e externas;
- d) determinar o que é significativo para a organização;
- e) estabelecer metas mensuráveis e rascunhar o plano de responsabilidade social;
- f) implementar o plano e iniciar o monitoramento do progresso;
- g) comunicar e reportar;
- h) repetir o processo de autoavaliação, melhorias e comunicações permanentes.

### 3 Metodologia

Este estudo teórico baseou-se na leitura e análise do conteúdo das normas de gestão de riscos (ISO 31000) e de gestão de responsabilidade social (ISO 26000) e na identificação elementos em que a estrutura e o processo de gestão propostos pela primeira norma pode contribuir para preenchimento das lacunas metodológicas da segunda.

A aplicação deste método transcorreu e amadureceu no decorrer da preparação e aplicação de cursos de capacitação nos temas pelo autor, a partir do ano de 2006 (ainda utilizando como referência a antecessora norma AS/NZS 4360:2004, prosseguindo com as normas ABNT NBR ISO 31000:2009 e ABNT NBR ISO 26000:2010) até a data atual.

### 4 Resultados

A norma ISO 31000 de gestão de riscos (bem como, há mais tempo, sua antecessora AS/ZNS 4360) tem sido aplicada com sucesso como referência para implementação da gestão de riscos. No Brasil, os hospitais da Unimed (em Belo Horizonte, MG) e Biocor Instituto (em Nova Lima, MG) conquistaram certificações de seus sistemas de gestão de riscos a partir de protocolo e norma derivados das normas de gestão de riscos. No âmbito internacional, a empresa espanhola de energia Abengoa também obteve uma certificação em gestão de riscos baseada na ISO 31000. Em nosso país, dezenas de organizações e centenas de profissionais já se capacitaram em gestão de riscos através de instituições como o Centro da Qualidade, Segurança e Produtividade para o Brasil e a América Latina (QSP), em São Paulo, SP.

A sistemática do processo de gestão de riscos fornecido pela ISO 31000 (e não somente: também por diversas metodologias como a do *PMBOK*, *COSO*, *OHSAS 18001*, entre outras) demonstram na prática a viabilidade do método, dada a comentada eficácia no desempenho alcançado pelas diversas organizações. Infelizmente, ainda não há estudos acadêmicos que comprovem os resultados da gestão de riscos desta organizações, mas a manutenção das certificações pode ser considerada como um dado de sucesso.

Como a norma ISO 26000 traz diretrizes e orientações gerais – as mais variadas e completas – a referentes à responsabilidade social, mas não um modelo ou método de implementação da gestão da responsabilidade social, optou-se pela utilização de uma sistemática mais elaborada que o PDCA proposto por Bernhart (2011): a estrutura e o processo de gestão de riscos da ISO 31000. Esta abordagem é mais completa que a da ASQ, mas não conflita com ela: a complementa.

Nesta linha de raciocínio, a implementação da gestão de responsabilidade social pode ser entendida como a de uma gestão de riscos à responsabilidade social, ou seja, riscos que ameacem (ou oportunizem) as expectativas da sociedade ou os interesses das partes interessadas. Pela sistemática da estrutura e do processo de gestão de riscos, o primeiro passo para se iniciar o planejamento da implementação da ISO 26000 em uma organização qualquer deve ser o entendimento da organização e de seu contexto (interno e externo), na terminologia da ISO 31000. Ferramentas clássicas de gestão que a prática demonstra poderem cumprir esta função são a análise SWOT (Forças, fraquezas, oportunidades e ameaças), um diagnóstico do tipo *gap analysis*, ou o plano estratégico da empresa (se existente). Este raciocínio analógico está representado na primeira linha da tabela 2.

Sucessivamente, reconhece-se para cada orientação da Seção 7 da ISO 26000 os elementos de uma estrutura de gestão de riscos e do processo de gestão de riscos, já consagrados pelas implementações orientadas pela ISO 31000.

## 5 Conclusões

Organizações públicas e privadas, de diversos ramos de atuação, buscam capacitação e informação para implementarem a gestão da responsabilidade social, desde a norma americana SA 8000, passando pela norma brasileira NBR 16001 (não abordadas por este artigo). Diversas organizações, como a Fundação Getúlio Vargas, o Centro da Qualidade, Segurança e Produtividade para o Brasil e a América Latina, e discutem em fóruns, eventos e *workshops* como implementar a nova norma internacional ISO 26000.

Dada a inexistência de uma metodologia específica referenciada pela norma, apresentou-se a sistemática já consagrada da ISO 31000 como referência para a gestão de responsabilidade social de forma a atender plenamente a ISO 26000. Constatou-se que todas as orientações desta última encontram uma equivalente saída na primeira.

Propõe-se que esta metodologia seja aplicada em diferentes organizações para verificar sua viabilidade. Finalmente, propõe-se nomear esta integração de sistemáticas como “gestão de riscos à responsabilidade social”, encarando-se os objetivos a serem preservados como as expectativas e interesses da sociedade e das partes interessadas. Ter-se-á na organização que a implementar, conseqüentemente, também uma contribuição para a gestão da sustentabilidade. Enfim, como a abordagem engloba intenso e abrangente levantamento de informações, avaliação, tratamento, divulgação e monitoramento rastreável das informações, está-se contribuindo também para a gestão do conhecimento organizacional.

## 6. Referências bibliográficas

ABNT ISO GUIA 73:2009 - Gestão de riscos – Vocabulário. Rio de Janeiro: Associação Brasileira de Normas Técnicas, 2009a.

ABNT NBR ISO 31000:2009 - Gestão de riscos - Princípios e diretrizes. Rio de Janeiro: Associação Brasileira de Normas Técnicas, 2009b.

ABNT NBR ISO 26000:2010 – Diretrizes sobre responsabilidade social. Rio de Janeiro: Associação Brasileira de Normas Técnicas, 2010.

BERNHART, Michelle. ISO 26000 Practice in practice: a user guide. ASQ Quality Press, 2011.

Tabela 2 – Orientações sobre a integração da responsabilidade social pela norma ISO 26000 e como atendê-las pela Estrutura e pelo Processo de gestão de riscos da ISO 31000.

ISO 26000 Orientações		ISO 31000 Estrutura	ISO 31000 Processo	Exemplos de ferramentas
7.2 Relação das características de uma organização com a responsabilidade social.		4.3.1 Entendimento da organização e seu contexto.		Análise SWOT. Diagnóstico <i>gap-analysis</i> . Plano estratégico.
7.3 Compreensão da responsabilidade social da organização.	7.3.1 <i>Due dilligence</i> .	4.3.2 Estabelecimento de uma política de gestão de riscos.		Política autorizada pela Alta Administração.
	7.3.2 Determinação da relevância e significância dos temas centrais.	4.4 Implementação da gestão dos riscos	5.4.2 Identificação dos riscos. 5.4.3 Análise dos riscos. 5.4.4 Avaliação dos riscos.	Matriz ou planilha de avaliação de riscos.
	7.3.3 Esfera de influência da organização.		5.4.2 Identificação dos riscos. 5.5 Tratamento de riscos.	Matriz ou planilha de avaliação de riscos.

Tabela 2 – Orientações sobre a integração da responsabilidade social pela norma ISO 26000 e como atendê-las pela Estrutura e pelo Processo de gestão de riscos da ISO 31000 (continuação).

ISO 26000 Orientações		ISO 31000 Estrutura	ISO 31000 Processo	Exemplos de ferramentas
7.4 Práticas para integrar a responsabilidade social em toda a organização.	7.4.1 Conscientização e desenvolvimento de competências para a responsabilidade social.	4.3.3 Responsabilização. 4.3.5 Recursos 4.3.6 Estabelecimento de mecanismos de comunicação e reporte internos. 4.3.7 Estabelecimento de mecanismos de comunicação e reporte externos.	5.2 Comunicação e consulta.	Plano de capacitação e treinamentos. Plano de comunicação e consulta. Políticas e procedimentos.
	7.4.2 Determinação da direção de uma organização rumo à responsabilidade social.	4.3.2 Estabelecimento de uma política de gestão de riscos. 4.3.3 Responsabilização.		Políticas e procedimentos.
	7.4.3 Como trazer a responsabilidade social para a governança, os sistemas e os procedimentos de uma organização.	4.3.4 Integração nos processos organizacionais.	5.5 Tratamento de riscos	Planos de tratamento de riscos. Políticas e procedimentos.

Tabela 2 – Orientações sobre a integração da responsabilidade social pela norma ISO 26000 e como atendê-las pela Estrutura e pelo Processo de gestão de riscos da ISO 31000 (continuação).

ISO 26000 Orientações		ISO 31000 Estrutura	ISO 31000 Processo	Exemplos de ferramentas
7.5 Comunicação sobre responsabilidade social.	<p>7.5.1 O papel da comunicação na responsabilidade social.</p> <p>7.5.2 Características das informações relacionadas à responsabilidade social.</p> <p>7.5.3 Tipos de comunicação sobre a responsabilidade social.</p> <p>7.5.4 Diálogo com partes interessadas na comunicação sobre responsabilidade social.</p>	<p>4.3.6 Estabelecimento de mecanismos de comunicação e reporte internos.</p> <p>4.3.7 Estabelecimento de mecanismos de comunicação e reporte externos.</p>	5.2 Comunicação e consulta.	Plano de comunicação e consulta. Políticas e procedimentos.
7.6 Fortalecimento da credibilidade em relação à responsabilidade social.	<p>7.6.1 Métodos para fortalecer a credibilidade.</p> <p>7.6.2 Fortalecimento da credibilidade de relatórios e declarações de responsabilidade social.</p> <p>7.6.3 Solução de conflitos ou desavenças entre a organização e suas partes interessadas</p>	<p>4.3.6 Estabelecimento de mecanismos de comunicação e reporte internos.</p> <p>4.3.7 Estabelecimento de mecanismos de comunicação e reporte externos.</p>	5.2 Comunicação e consulta.	Plano de comunicação e consulta. Políticas e procedimentos. Comitê de crise. Plano de continuidade do negócio.

Tabela 2 – Orientações sobre a integração da responsabilidade social pela norma ISO 26000 e como atendê-las pela Estrutura e pelo Processo de gestão de riscos da ISO 31000 (continuação).

ISO 26000 Orientações		ISO 31000 Estrutura	ISO 31000 Processo	Exemplos de ferramentas
7.7 Análise e aprimoramento das ações e práticas relativas à responsabilidade social.	7.7.2 Monitoramento de atividades de responsabilidade social. 7.7.3 Análise do progresso e desempenho em responsabilidade social da organização. 7.7.4 Aumento da confiabilidade da coleta de dados e informações e gestão. 7.7.5 Melhorias no desempenho	4.5 Monitoramento e análise crítica da estrutura. 4.6 Melhoria contínua da estrutura	5.6 Monitoramento e análise crítica.	Plano de monitoramento de riscos. Relatório de análise crítica. Auditorias.
7.8 Iniciativas voluntárias de responsabilidade social.	7.8.2 Natureza voluntária da participação. 7.8.3 Considerações. 7.8.4 Notas sobre o Anexo <sup>a</sup>	4.4 Implementação da gestão de riscos.		