

Gestão de riscos e a norma ISO 31000: uma abordagem literária

O risco é um fato no âmbito empresarial, gerenciá-lo é a chave para que as empresas possam tomar decisões assertivas que resultem em obtenção de lucros e criação de valores para seus acionistas. O presente estudo tem como objetivo realizar uma revisão de literatura sobre gestão de riscos e analisar algumas características e aplicabilidades apontadas pelos estudiosos sobre a norma internacional de gestão de riscos ISO 31000. Ao consultar alguns modelos propostos na literatura desse tipo de gestão, identifica-se pontos similares no processo, estes resumem-se em: i) Identificação dos riscos; ii) Avaliação; iii) Tratamento e iv) Tomada de decisão. A International Organization for Standardization (ISO) publicou a norma ISO 31000:2009 devido à necessidade de harmonização dos padrões, regulamentações e estruturas de recomendações feitas por normas anteriores, entretanto por ser um modelo generalista que visa propor diretrizes para a gestão de todos os tipos de riscos, alguns estudiosos criticaram severamente seus conceitos e recomendações. Em 2018, a ISO lançou uma versão mais atualizada da norma (ISO 31000:2018), com o intuito de solucionar algumas inconsistências existentes na anterior. Na literatura consultada, identificou-se diversas aplicações da ISO 31000 em modelos de gerenciamento de riscos de variados segmentos empresariais, e mesmo contendo alguns pontos a ser melhorados, conclui-se que as recomendações realizadas por esta norma são de grande relevância para ter-se como base na construção do processo de um modelo de gestão de riscos. Ademais, vale ressaltar que o presente estudo norteará o início da construção de um modelo de gestão de risco para uma determinada organização do estado de Sergipe.

Palavras-chave: Riscos; Gestão de riscos; Normas; Organização; Mitigação.

Risk management and the ISO 31000 standard: a literary approach

Risk is a fact in the business environment, managing it is the key for companies to make assertive decisions that result in profit results and value creation for their shareholders. The present study aims to carry out a review of the literature on risk management and analysis of the characteristics and applicability pointed out by scholars on the international risk management standard ISO 31000. When consulting some models proposed in the literature on the type of management, identification if similar points in the process, these are summarized in: i) Identification of risks; ii) Evaluation; iii) Treatment and iv) Decision making. The International Organization for Standardization (ISO) has published an ISO 31000: 2009 standard due to the need to harmonize the standards, regulations and recommendation structures made by previous standards, however, as it is a generalist model that aims at the guidelines for the management of all types of risks, some scholars have severely criticized their concepts and recommendations. In 2018, ISO released a more updated version of the standard (ISO 31000: 2018), in order to resolve some inconsistencies in the previous one. In the consulted literature, several applications of ISO 31000 were identified in risk management models of various business segments, even with some points to be improved, it is concluded that the recommendations made by this standard are of great importance to be based on in the construction of the process of a risk management model. In addition, it is worth mentioning that the present study will guide the beginning of the construction of a risk management model for an organization provided in the state of Sergipe.

Keywords: Risks; Risk management; Standards; Organization; Mitigation.

Topic: **Planejamento, Estratégia e Competitividade**

Reviewed anonymously in the process of blind peer.

Received: **11/11/2020**

Approved: **22/03/2021**

Thiago de Jesus dos Santos 
Universidade Federal de Sergipe, Brasil
<http://lattes.cnpq.br/2599861239588102>
<http://orcid.org/0000-0003-3577-2003>
thiago.dejesus0705@gmail.com



DOI: 10.6008/CBPC2674-6417.2021.001.0001

Referencing this:

SANTOS, T. J.. Gestão de riscos e a norma ISO 31000: uma abordagem literária. **Management Journal**, v.3, n.1, p.1-14, 2021. DOI: <http://doi.org/10.6008/CBPC2674-6417.2021.001.0001>

INTRODUÇÃO

O risco é um fato no âmbito empresarial, gerenciá-lo é a chave para que as empresas possam tomar decisões assertivas que resultem em obtenção de lucros e criação de valores para seus acionistas. Na medida em que todas as atividades organizacionais envolvem intrinsecamente riscos, os gestores devem atentar-se para esses fenômenos, dado que existe a possibilidade do sucesso ou do fracasso em uma determinada decisão que ocasionará modificações na empresa, logo compete aos administradores avaliarem e mensurarem os riscos envolvidos e devem administrá-los com intuito de reduzir as consequências indesejadas ou maximizar a possibilidade dos eventos desejados (BERGAMINI JUNIOR, 2005).

Há diversos tipos de riscos com características distintas, estes estão diretamente relacionados com o âmbito empresarial da organização e de suas próprias atuações no mercado. Com a criação de novos tipos de estruturas corporativas e com o avanço das tecnologias da informação, novos riscos emergem (NASCIMENTO et al., 2020). A sua gestão refere-se à noção de que eventos incertos podem acontecer e gerar prejuízos para a organizações. Portanto, a administração dos riscos fornece aos gestores o conhecimento de quais riscos as empresas estão expostas (FERNANDES et al., 2014).

Nesse sentido, surge a necessidade e com isso ações de padronização e/ou orientações sobre como implementar eficientemente um sistema de gerenciamento de riscos, com o intuito de alinhar conceitos e processos dessa gestão nas empresas (NASCIMENTO et al., 2020). Santos (2013) apresenta diversas metodologias que buscam padronizar os processos de gestão de riscos, entre as quais destacam-se: FERMA: Risk Management Standard, Norma de Gestão de Riscos Australiana AS/NZS 4360 (2004), Gestão de Risco Empresarial: ERM e a ISO 31000.

A International Organization for Standardization (ISO) publicou a sua primeira série de orientações no ano de 2009, a ISO 31000:2009, devido à necessidade de harmonizações dos padrões, regulamentações e estruturas das normas relacionadas à gestão de riscos publicadas anteriormente. Caracterizando-se como uma norma universal e específica para gestão de riscos, tendo como escopo ser a “norma-das-normas” (FERNANDES et al., 2014). Dois anos depois, foi estabelecido que esse padrão seria revisado para corrigir inconsistências e falhas detectadas (SANTOS, 2013). No ano de 2018, foi publicado a norma ISO 31000:2018 que visa substituir a versão anterior e enfatizar a dinamicidade da gestão de riscos (ABNT, 2018).

Embora diversos trabalhos já tenham sido realizados sobre gestão de riscos, muitos gestores ainda não oferecem a devida importância para as técnicas e etapas desta gestão (KLIEMANN NETO et al., 2018). Deste modo, o presente estudo tem como objetivo realizar uma revisão de literatura sobre gestão de riscos e analisar algumas características e aplicabilidades apontadas pelos os estudiosos sobre a norma internacional de gestão de riscos ISO 31000, visando verificar a hipótese de que a norma ISO 31000 é um conjunto de recomendações relevante a ter-se como base na elaboração de um modelo de gestão de riscos.

METODOLOGIA

A presente pesquisa classifica-se como exploratória, uma vez que um de seus objetivos é

proporcionar maior familiaridade aos leitores sobre o fenômeno estudado e descrever a complexidade e características do problema (RODRIGUES, 2007; FONSECA, 2012). Possibilitando o aumento do conhecimento do pesquisador sobre o fato, o que permite a criação de novas hipóteses e problemas dentro da análise, gerando possibilidades de outras pesquisas mais estruturadas. Neste caso, o estudo precisa ser flexível para promover a observação de vários aspectos relacionados ao fenômeno (SELLTIZ, 1995, citado por OLIVEIRA, 2011). Quanto à forma de abordagem, caracteriza-se como qualitativa, tendo em vista que para o alcance dos objetivos utilizou-se do método de revisão bibliográfica, por meio de análise do conteúdo de jornais, livros, publicações, boletins e pesquisas especializadas no assunto (RODRIGUES, 2007).

REVISÃO TEÓRICA

Conceituações sobre o Risco

De acordo com Renn (1992) e Duarte Junior (1992), o risco é composto de uma heterogeneidade de definições, sendo um elemento intrínseco em todas as operações. Sua definição é multidimensional. Barragan et al. (2006) definem o risco como a possibilidade de ocorrência de um evento futuro não previsto, podendo gerar consequências positivas ou negativas ao objetivo almejado. Na concepção de Almeida (2004), o risco refere-se a efeitos negativos (danos) que podem ocorrer futuramente. O seu tratamento analítico deu-se por causa da invenção dos cálculos de probabilidades realizados por Pascal no século XVII (LIEBER et al., 2002). Surgindo uma fórmula para quantificá-lo:

$$R = P \times D \quad (1)$$

Onde R é o risco, P é a probabilidade de ocorrência de um ou diversos eventos desfavoráveis e D é o valor “prejuízo” associado aos danos. Dessa forma o risco sofre influências tanto pelas alterações do P (condições perigosas) quanto do D (vulnerabilidade e proteções) (ALMEIDA, 2004). Holton (2004) apresenta a definição dada por Frank Knight (1921, citado por HOLTON, 2004) como uma das mais famosas e importantes sobre o fenômeno, donde busca-se diferenciar o risco e a incerteza, pois o risco atrela-se a uma probabilidade mensurável e a incerteza é imensurável. Segundo Cooper et al. (2005), o risco é a consequência da exposição a incerteza, sendo a chance de ocorrer algo que gere impactos sobre os objetivos. Discordando da visão de Almeida (2004), o estudioso alia-se a afirmação de Barragan et al. (2006), onde o risco inclui a possibilidade de perda ou ganho, até mesmo a variação de um resultado planejado, como consequência direta da incerteza. Alessandri et al. (2004) em seus estudos apresentam convergência com a afirmação feita por Knight (1921, citado por HOLTON, 2004), como exposto na Figura 1.

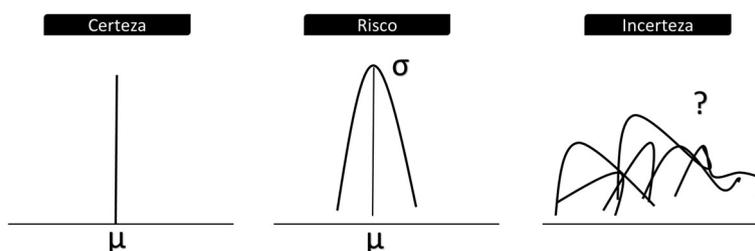


Figura 1: Distinção entre certeza, risco e incerteza. **Fonte:** Adaptado de Alessandri et al. (2004)

Areosa (2008) aponta em sua pesquisa a concepção do estudioso Luhman (1993, citado por AREOSA, 2008) sobre o risco, donde esse fenômeno está relacionado ao processo de tomada de decisão, sendo assim realizado somente no presente e tornando o horizonte temporal muito relevante nesse processo. Segundo o estudioso, o risco é o termo utilizado para problematizar o futuro, uma projeção no presente dos possíveis acontecimentos, entretanto essa análise torna-se muito complexa por causa da incerteza. A Figura 2 apresenta essas definições sistematizadas.

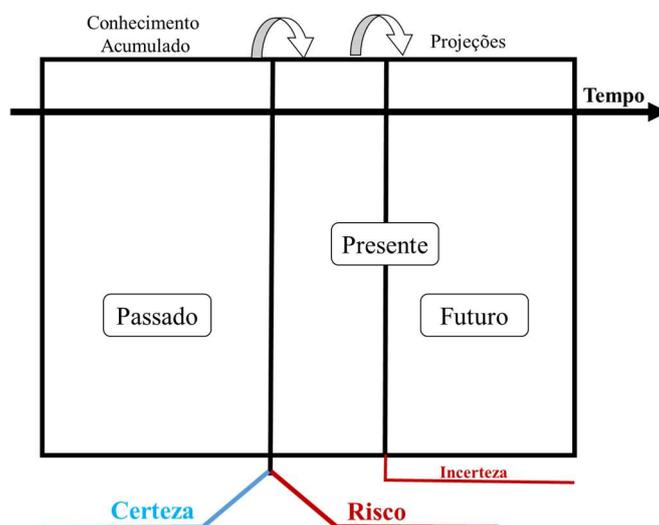


Figura 2: Relação entre o risco e o tempo. Fonte: Adaptado de Areosa (2008).

Segundo Penha et al. (2005), o risco está diretamente relacionado com um determinado retorno de um investimento, aplicação ou empreendimento. De maneira que quanto maior o retorno, maior será o risco (MACHADO, 2015). Tendo em vista a multidimensionalidade e oscilações do conceito sobre o risco, Fischhoff et al. (1984) afirmam que para obtenção de uma definição precisa sobre o fenômeno é necessário um exaustivo trabalho. Logo o risco pode ser considerado como um elemento pertencente ao futuro que está relacionado diretamente com as atividades e decisões do presente (RENN, 1992). Duarte Junior (1993) e Machado (2015) apontam a existência de quatro grandes grupos de riscos: crédito, operacional, mercado e legal e liquidez.

Salienta-se a existência de diversos tipos de riscos além desses apresentados, como afirmam Barragan et al. (2006), contudo para o presente estudo somente será analisado esses quatro grupos. Ademais, salienta-se que os riscos que as empresas estão expostas dependem da natureza de sua atividade (FERNANDES et al., 2014). Sobre os grandes grupos de riscos apresentados, Duarte Junior (1993), Moraes (2003), Zonatto et al. (2009) e Machado (2015) define-os como: **Risco de Crédito:** a possibilidade de ocorrência de perdas relacionadas ao tomador ou contraparte não honrar com suas obrigações financeiras no contrato pactuado, também pode ser considerado a possibilidade de desvalorização do crédito decorrente de um declínio na classificação de risco do tomador, à redução ou ganhos, consentimento de descontos em renegociações e aos custos de recuperação. **Risco Operacional:** refere-se a perdas relacionadas a alguma deficiência, falhas ou decisões relacionadas ao recurso humano, processo, máquinas, acontecimentos ou infraestrutura, ou seja, acontecimentos na área operacional das empresas, que possam

dificultar a realização das suas estratégias. **Risco de Mercado:** é a possibilidade de ocorrência de danos gerados por inconsistências do mercado, também se inclui os riscos ocorridos das operações expostos a variação das taxas de juros, variação cambial e dos preços das mercadorias. **Risco Legal:** Refere-se à legitimidade das organizações, seus registros e legalidades de suas obrigações e direitos. É a probabilidade de perdas decorrentes de desobediências de regulamentos legais que resultam para as entidades o pagamento de multas indenizatórias. **Risco de Liquidez:** a possibilidade da instituição não ser capaz de honrar com suas obrigações esperadas e inesperadas, correntes e futuras, ou seja, uma situação de desequilíbrio entre os ativos negociáveis e os passíveis exigíveis e também um cenário em que a instituição não consiga negociar uma posição a preço mercadológico.

Gerenciamento de riscos

O gerenciamento de riscos gradativamente está sendo incluído nos ambientes empresariais. Diversos títulos têm surgido no mercado para designar o profissional que atuante na área: Gestor de riscos, Chief Risk Officer, Chief Compliance Officer entre outros (PENHA et al., 2005). Salienta-se a existência de uma formação acadêmica, que visa capacitar pessoas para trabalhar com esse fenômeno, o Bacharelado em ciências atuarias, o profissional formado nesse curso chama-se Atuário, sendo-o inteiramente responsável pela mensuração e o gerenciamento dos riscos, através de técnicas estatísticas, matemáticas, probabilísticas e financeiras (IBA, 2020).

A gestão de riscos é responsável pela implantação de um processo de administração eficiente e contínuo na organização (HOLLÓS et al., 2009). Em outras palavras é um processo metódico e organizado que busca a melhoria contínua através de redução de prejuízos e aumento dos benefícios entre as metas e estratégias programadas (BARALDI, 2018), isto é, um conjunto de planejamento, organização, direção e controle dos recursos de uma organização, com o intuito de minimizar os efeitos dos riscos nas quais a mesma está exposta (MACHADO, 2015).

De acordo com Alberton (1996), essa gestão pode ser definida como a ciência que almeja a proteção dos recursos humanos, materiais e financeiros de uma entidade, mediante a mitigação ou aceitação de determinados riscos. Tendo seu início na década de 70 associando-se ao mercado de seguros, ampliou-se com o decorrer dos tempos para diversos setores das instituições públicas e privadas, possibilitando o estabelecimento de prioridades e auxiliando na tomada de decisão, baseando-se em estatística e em probabilidades que mensuram a ocorrência e a magnitude dos possíveis eventos no planejamento da entidade (HOLLÓS et al., 2009).

É de suma importância o alinhamento entre a gestão de riscos e o modelo de governança corporativa da empresa. Portanto, antes de sua implementação, deve ser revisado o modelo de governança interna da entidade pois a liberdade exagerada é prejudicial, mas excesso de regras também podem afetar negativamente o desempenho da empresa (MACHADO, 2015).

Sua intervenção é de forma prospectiva, com o escopo de identificar e antecipar os possíveis acontecimentos para definir alternativas que solucionem os possíveis impactos nos objetivos e que garantam

uma tomada de decisão precisa, a fim de alcançar a eficiência e a eficácia (AMARO, 2005). Silva et al. (2010) atualizaram o estudo de Ferreira et al. (2005, citado por SILVA et al., 2010) e expuseram algumas abordagens de autores sobre os processos seguidos no gerenciamento de riscos, identificando similaridades nos modelos propostos e classificando-os segundo a sua possível etapa (P) referindo-se ao Planejamento e (C) ao controle, como apresentado no Quadro 1.

Quadro 1: Processos para o gerenciamento de riscos.

| Autores | Processo de Gerenciamento de riscos | | | | | | |
|----------------------|--|---|---|---|--------|------------------------------------|-------------------------------------|
| Boehm et al. (1994) | Definição obrigatória do gerenciamento de riscos (P) | Rever metas (P) | Identificar riscos (P) | Analisar riscos (P) | riscos | Planejar o controle dos riscos (P) | Controlar e monitorar os riscos (C) |
| Kontio (1996) | Rever as metas definidas (P) | Identificação dos riscos (P) | Analisar os riscos (P) | Planejar o controle dos riscos (P) | dos | Controlar os riscos (C) | - |
| Kezner (1998) | Identificação dos riscos (P) | Qualificação dos riscos (P) | Resposta a riscos (P) | Controle dos riscos/lições aprendidas (C) | dos | - | - |
| Smith et al. (2002) | Identificação dos riscos (P) | Análise dos riscos (P) | Priorização dos riscos e mapa de riscos (P) | Redução dos riscos (C) | dos | Monitoração dos riscos (C) | - |
| Hollós et al. (2009) | Estabelecer o contexto (P) | Identificação dos riscos (P) | Avaliação dos riscos (P) | Tratar os riscos (C) | (C) | - | - |
| Machado (2015) | Desenvolvimento da compreensão dos riscos (P) | Apreciação das causas e fontes de risco (P) | Avaliação dos riscos (P) | Análise das consequências positivas e negativas (C) | das | Tratar os riscos (C) | - |

Fonte: Adaptado de Silva et al. (2010).

Nota-se a diversidade de abordagens sobre uma arquitetura para o gerenciamento de riscos. Podendo ser realizado de forma centralizada (um setor responsável pelo desenvolvimento de técnicas para avaliação do risco) ou de forma distribuída (cada setor desenvolve seus métodos para a gestão do mesmo). Recomenda-se para as empresas que estão iniciando a implementação dessa gestão em seus âmbitos, utilizarem a forma centralizada. Ao decorrer do tempo com a disseminação da cultura do gerenciamento dos riscos, pode-se flexibilizar a gestão para as áreas que precisem de técnicas específicas (PENHA et al., 2005).

De maneira concomitante com a afirmação de Fernandes et al. (2014) sobre que os riscos que as empresas estão expostas estão diretamente relacionadas com a sua natureza, Penha et al. (2005) explicitam que o modelo para o gerenciamento dos riscos e a escolha das técnicas para a sua realização também seguirão o princípio da dependência sobre as atividades e finalidades expostas.

Mesmo com as múltiplas abordagens sobre as etapas para a gestão de riscos, identifica-se processos similares em todos os modelos propostos. Na Figura 3 apresenta-se um resumo sintético dos procedimentos para uma gestão de riscos em consonância com os autores expressados no Quadro 1 e com Penha et al. (2005), Almeida (2004), Hollós et al. (2009), Rabechini Junior et al. (2012) e Silva et al. (2010).

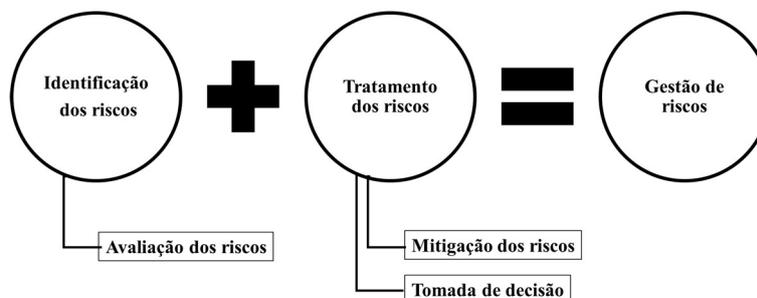


Figura 3: Sistematização resumida de um gerenciamento de riscos.

Identificação e avaliação dos riscos

Os riscos devem ser mapeados de forma sistêmica e abrangente (HOLLÓS et al., 2009). Os de relevância inferior também deverão ser identificados, mesmo com a possibilidade de uma não apreciação dos superiores, ou seja, mapeiam-se todos os riscos que necessitem de uma decisão gerenciada (PENHA et al., 2005).

Há diversas técnicas para identificação dos riscos, o requerimento de sua utilização dependerá da cultura, governança corporativa e situação da organização. Entre as técnicas pode-se citar análises de balanços patrimoniais, análise de correlação linear entre variáveis, ações dos concorrentes, Brainstorming, entrevistas, técnica Delphi, análise de verificação, análise de diagramas: causa e efeito, análise dos pontos fortes, fracos, oportunidades e ameaças (SWOT), entre outras (PENHA et al., 2005; SILVA et al., 2010).

Enfatiza-se a grande necessidade de um objetivo claro para a identificação dos riscos, com uma linguagem concisa e definida pelo horizonte de tempo e metas definidas. Sua identificação é um processo planejado e sistemático. Os riscos identificados devem ser expressos de forma clara e detalhada, apresentando-se o contexto, as condições e realidade para que os mesmos sejam analisados (NÓBREGA, 2007).

A avaliação dos riscos é um dos processos iniciais do gerenciamento, permitindo identificar as medidas que devem ser tomadas para a solução ou mitigação de tal fato, iniciando o processo de apreciação dos riscos, por meio de uma análise sistemática de todos os aspectos organizacionais envolvidos (CARVALHO, 2013).

Para sua avaliação faz-se necessário o reconhecimento das ameaças no ambiente interno e externo que a organização ou o objeto do estudo está exposto, analisando-os e definindo critérios de acordo com as suas prioridades. Tornando-se um processo cíclico e de extrema importância no sistema de gestão, visto que em diversas organizações pode-se surgir ou desaparecer diversos fatores indesejados, bem como os mesmos já identificados com mudanças na probabilidade de ocorrência e/ou na gravidade das causas (LEOPOLDINO, 2004).

Avaliação Qualitativa e Quantitativa

Através de uma análise qualitativa determina-se as características dos riscos e a sua relevância para o sucesso ou fracasso dos objetivos da empresa. Para sua realização utiliza-se palavras e escalas com o intuito

de mensurar à magnitude das consequências que o evento atrelado a incerteza pode ocasionar aos envolvidos (NÓBREGA, 2007).

Tendo em antemão realizado o levantamento dos riscos, deve-se classificá-los através da existência do controle, avistando os processos e negócio da empresa, de modo que se a situação estiver ótima, significa que os riscos envolvidos estão sub ou supercontrolados. Os subcontratados resultam em grande exposição a riscos, enquanto os supercontrolados resultam em aumento de custos (BERGAMINI JUNIOR, 2005).

Entre as diversas ferramentas a serem empregadas nas análises, encontra-se a matriz de riscos, que pode ser empregada em diversos fenômenos dessa e de várias naturezas (PAULO et al., 2007). De acordo com Bergamini Junior (2005), a averiguação dos riscos através de uma matriz expressa de forma concisa e eficiente os seus impactos entre os envolvidos, possibilitando uma maior precisão no conhecimento de sua relevância, levando-se em consideração três fatores: i) a probabilidade de ocorrência; ii) seus impactos iii) efeitos.

No que concerne à análise quantitativa dos riscos, Nóbrega (2007) explicita como ocorre o processo de analisar as probabilidades de cada risco e como quantificar suas consequências para a empresa. Para tais análises faz-se necessário os resultados obtidos tanto na identificação, quanto na qualificação dos riscos, além de informações sobre a tolerância da empresa sobre os riscos, bases históricas da organização, etc. Matias Junior (2006) define a análise quantitativa como o procedimento responsável pela representação das incertezas como variáveis aleatórias e modeladas por distribuições de probabilidade. Do mesmo modo, Duarte et al. (2012) apontam a possibilidade de quantificação dos riscos identificados por meio de modelos matemáticos.

Existem diversas ferramentas e técnicas para a realização de uma eficiente quantificação analítica dos riscos, entre elas encontram-se a análise da árvore de decisão e a simulação de Monte Carlo, ambos podem ser desenvolvidos em softwares. A árvore de decisão utiliza as possibilidades de escolhas a serem tomadas e as possíveis consequências geradas utilizando as probabilidades dos riscos. Já para a técnica de Monte Carlo, utiliza-se a função densidade de probabilidade de uma distribuição e a geração de números aleatórios para a realização de simulações dos possíveis eventos, podendo-se aplicar testes estatísticos mais adequados no modelo apresentado (NÓBREGA, 2007; MATIAS JUNIOR, 2006).

Tratamento e mitigação dos riscos e tomadas de decisões

Quando os efeitos dos riscos não puderem ser ignorados pela organização, deve-se desenvolver medidas que façam os mesmos sofrerem alterações com a sua implementação ou com o decorrer do tempo, visando a redução de seus impactos. Esse processo tem grande relevância e deve ser realizado e revisado periodicamente (RELIM et al., 2020). Penha et al. (2005) apontam alguns procedimentos para a mitigação dos riscos, entre eles encontra-se a identificação de um plano de ação para o mesmo, podendo ser: i) Plano Proativo- através de ações antecipadas com o objetivo de reduzir as probabilidades do problema ocorrer; ii) Plano de Contenção- reduzindo os impactos do risco, por meio da redução dos efeitos das consequências; iii) Plano de Contingência- realização de ações que respondam aos problemas ocasionados pelo risco.

Palma et al. (2011) em suas análises realizaram a implementação da gestão de riscos em uma determinada organização e como resposta aos riscos utilizou-se a estratégia de mitigação. Os estudiosos estabeleceram procedimentos que seriam efetuados antes da realização da atividade central, além disso, assim como proposto por Penha et al. (2005), os mesmos sugeriram o desenvolvimento de um plano de ação que apontasse como a atividade deveria ser feita e o prazo de realização.

A tomada de decisão é condicionada por diversos fatores como apresentado na Figura 4. A gestão de riscos, responsável pelo desenvolvimento de processos e estruturas que dimensionem os riscos que as entidades estão expostas, proporcionam aos gestores à análise e decisão de quais planejamentos irão seguir, quais devem ser priorizados, onde e como investir apropriadamente seu capital e auxilia na tomada de decisão dos procedimentos a serem adotados para resposta ao risco, seja através de sua mitigação ou aceitação (ALESSANDRI et al., 2004; AMARO, 2005; WESTERMAN et al., 2008).

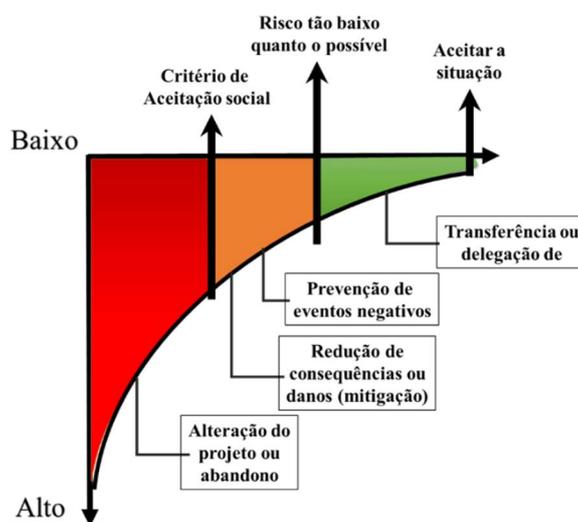


Figura 4: Filosofia geral da gestão de risco e tomada de decisão. Fonte: Adaptado de Almeida (2004).

No tocante as respostas aos riscos, Kliemann Neto et al. (2018) define-as em quatro categorias, sendo elas: i) **Mitigar:** redução da probabilidade e/ou impacto dos riscos, podendo ser realizado por um novo curso de ação, modificações, intensificações em procedimentos, entre outros; ii) **Evitar o risco:** Refere-se a alteração do planejamento com o intuito de eliminar o possível evento. Embora não seja possível a eliminação de todos os riscos, diversos podem ser evitados, a partir de uma melhoria na comunicação entre a equipe, não realização de negócios com fornecedores desconhecidos, etc.; iii) **Aceitar:** envolve a compreensão do risco e de suas consequências, decidindo aceitá-lo, ou seja, caso o risco ocorra, a equipe deverá agir tendo ciência de seus possíveis efeitos. A aceitação é utilizada quando a probabilidade do risco é pequena ou seus impactos são menos relevantes; iv) **Transferir:** consiste na transferência da gestão de riscos à outra pessoa, ou seja, uma terceirização. Como exemplo pode citar o transporte de mercadoria por uma empresa especializada, o risco referente ao transporte passa a ser gerenciado pela empresa contratada.

ISO 31000: Risk Management

A demanda por uma norma internacional específica para o gerenciamento de riscos fez a ISO

identificar que existia uma diversidade de setores e grupos de trabalhos que desenvolviam procedimentos com base em conceitos e pressupostos distintos, resultando muitas inconsistências entre as implementações. Tendo em vista essa identificação, em outubro de 2009, criou-se a ISO 31000, desenvolvida por um grupo de especialistas de mais de 30 países, com o intuito padronizar e integrar todos os conceitos, pressupostos, regulamentações e frameworks anteriormente realizados, por meio de um processo conciso e abrangente que busque estabelecer orientações genéricas sobre a estrutura e a implementação de um sistema que auxilie as organizações gerirem de forma eficiente, eficaz e coerente os riscos que as mesmas estão expostas (SANTOS, 2013; FERNANDES et al., 2014).

A ISO 31000 pode ser aplicada a qualquer tipo de risco e em qualquer seguimento de organizações, suas normas tratam-se de recomendações de um processo de gestão de riscos. Tendo que sua estrutura básica é dividida em três setores, sendo eles: princípios para a gestão, estrutura e processos (CRUZ et al., 2019). Sua implementação auxilia as organizações a cumprir os normativos e requerimentos legais seguindo os padrões internacionais. Resultando no aumento da visão da necessidade de tratar e monitorar os riscos, crescimento da confiança no planejamento realizado e na tomada de decisão, melhoria na identificação de oportunidades nas ameaças, nos controles, na prevenção de perdas e na gestão de incidentes (SANTOS, 2013; ROSA et al., 2015; CRUZ et al., 2019).

Esse modelo, como outros padrões genéricos, baseia-se na lógica processual e nos princípios administrativos básicos de “planejamento, organização, direção e controle”. Esses princípios são baseados na ideia que o risco pode ser considerado um aspecto claramente definido e gerenciável. Essa gestão utiliza-se de indicadores mensuráveis, integrados a avaliação e ao desempenho da empresa. Tendo como critério em grande parte para avaliação dos riscos a lógica probabilística, considerando diversos aspectos, como as causas e consequências, probabilidade de ocorrência e magnitude dos riscos (LALONDE et al., 2012).

Olechowski (2016) aponta em seu estudo onze princípios que a ISO propõe que se forem executados corretamente levarão a uma efetiva administração dos riscos. Esses princípios foram a base de suas análises, ao ponto do autor identificar a existência de algumas abstrações entre eles e explicar que isso dá-se por conta das generalizações realizadas sobre um conceito tão amplo quanto o de gestão de riscos. Os princípios afirmam que o gerenciamento dos riscos: i) Cria valores; ii) Faz parte da tomada de decisão; iii) É Sistemático, Estruturado e oportuno; iv) Dinâmico, interativo e responsivo; v) Adaptável; vi) Transparente e inclusivo; vii) Está incluso em toda a organização de processos; viii) Aborda diretamente a incerteza; ix) Considera os valores humanos e culturais; x) Baseia-se em boas informações e xi) Incentiva a melhoria contínua.

Oliveira et al. (2017) apresentam o processo proposto pela ISO 31000:2009 exposto na Figura 5 e apontam que a etapa da comunicação é muito relevante, pois seu escopo é que todos os envolvidos tenham ciência dos motivos pelo qual as decisões e ações estão sendo tomadas. O estabelecimento do contexto refere-se à ação da empresa em articular suas metas e definir as condições internas e externas que a mesma está envolvida. Outras etapas explicadas pelos estudiosos são: identificar os riscos, analisá-los para tomar decisões sobre os melhores métodos e estratégias a serem utilizadas, avaliá-los para descobrir quais deles precisam de tratamento e/ou prioridade, tratá-los por meio de uma ou mais técnicas que visem a sua

modificação, monitorá-los e revisá-los criticamente através de um processo cíclico que vise garantir a excelência da gestão ou até mesmo identificar pontos que necessitam ser alterados.

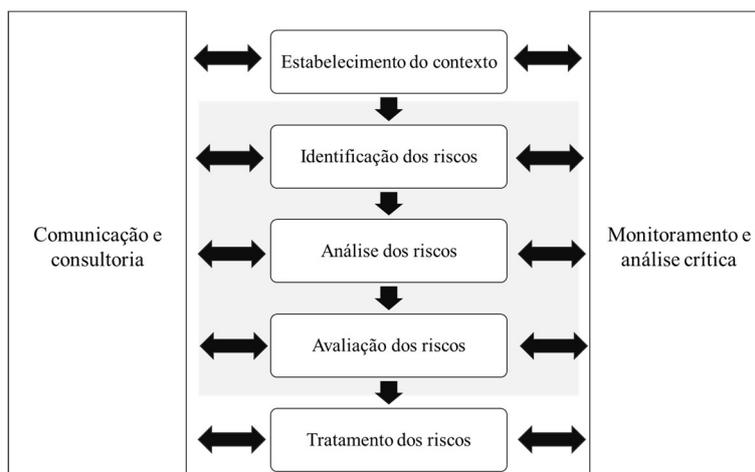


Figura 5: Processo de Gestão de riscos proposto pela Norma ISO 31000:2009. **Fonte:** Adaptado da ABNT (2009).

Muitos autores criticaram negativamente essa norma. Um autor em 2010 considerou que os termos utilizados na ISO 31000:2009 são muito vagos e não auxiliam eficientemente os gestores. Segundo o autor existe alguns requisitos idealistas que são impossíveis de serem cumpridos e alguns direcionam até a decisões ilógicas.

Um autor em 2010 identificou uma certa ambiguidade entre termos apresentados na norma, podendo-se citar a definição de apetite do risco e tolerância ao risco, o autor também apontou que a definição dada pela norma sobre a gestão de riscos pode ser melhorada para que se evite más interpretações. Em consonância com as críticas deste autor, sobre termos definidos no modelo, um outro autor lamenta que a definição dada para o risco não seja clara e nem matematicamente completa.

Lalonde et al. (2012) identificaram que algumas falhas da aplicação das recomendações da ISO 31000:2009 dá-se por conta dos usuários que cometem equívocos na interpretação ou na implementação de alguma atividade. Afirmando que o fato da norma ser genérica pode contribuir para uma melhoria de todo o processo de gestão de seus riscos. Aven (2011) afirma que a definição dada para aversão ao risco é apresentada de maneira equivocada.

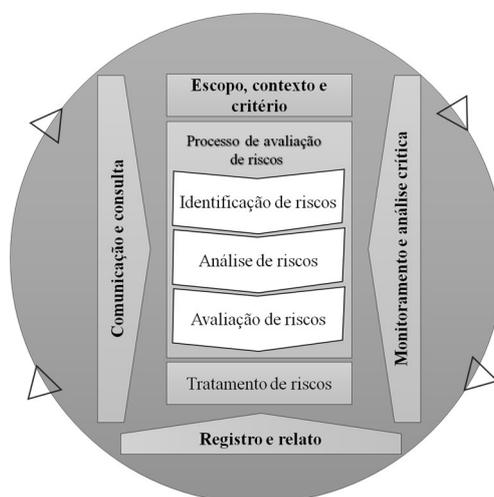


Figura 6: Processo de Gestão de riscos proposto pela Norma ISO 31000:2018. **Fonte:** Adaptado da ABNT (2019).

Com o objetivo de suprir algumas dessas fragilidades, lançou-se a ISO 31000:2018 com uma abordagem mais didática em seus processos apresentados na Figura 6, focando no aspecto estratégico das organizações e enfatizando que o gerenciamento de riscos deve ser inserido em todas as etapas dos projetos (CORRÊA, 2019; BERMÚDEZ et al., 2019). Comparando com a versão anterior, a alteração para uma forma circular e com setas enfatiza que o processo de gestão é cíclico e dinâmico, além disso acrescentou-se uma nova etapa de registro e relatos (CORRÊA, 2019).

Esse padrão é genérico e pode ser aplicado em qualquer tipo de risco como já apresentado anteriormente. Bermúdez et al. (2019) desenvolveram um modelo de gerenciamento de riscos com base nas diretrizes da ISO 31000:2018 para uma clínica médica e afirmaram que as recomendações da norma foram de grande relevância no desenvolvimento das etapas a serem estabelecidas, Zacari (2018) utilizou-as como uma das bases para oferecer uma forma sistemática de gestão de riscos em operação *omnichannel* de empresas varejistas. Por meio do padrão estudado, Dewi et al. (2019) desenvolveram um modelo e enfatizaram a eficiência na identificação e mitigação dos riscos operacionais, mostrando que as diretrizes genéricas da norma ISO 31000:2018 são válidas e que compete aos gestores as adaptarem para o escopo de sua organização (OLECHOWSKI, 2016).

CONCLUSÕES

O presente estudo teve como objetivo realizar uma revisão de literatura sobre gestão de riscos e analisar algumas características e aplicabilidades apontadas pelos os estudiosos sobre a norma internacional de gestão de riscos ISO 31000. Averiguou-se na literatura múltiplas definições relacionadas ao risco, enfatizando a sua distinção de incerteza, além disso foi possível analisar quatro grandes grupos de riscos, contudo salienta-se a existência de outros tipos do fenômeno que não foram relatados explicitamente nesse estudo.

Percebe-se que a gestão dos riscos é de suma importância para que uma empresa tenha sucesso em seus planejamentos e possa manter-se ativa em cenários altamente competitivos. Essa gestão proporciona aos interessados identificarem e prevenirem possíveis acontecimentos, a fim de que tomem boas decisões, por meio de definições de planos ou ações alternativas que sanem ou amenizem os impactos indesejados nas organizações. Na literatura consultada, identificou-se similaridades entre as etapas dos modelos de gestão de riscos propostos, essas etapas similares foram sintetizadas no estudo e alguns dos seus processos e técnicas utilizadas foram explanados.

Abordou-se algumas características relatadas pelos estudiosos sobre a aplicabilidade e sugestões realizados pela ISO 31000:2009 e sobre a versão mais recente a ISO:31000:2018. Nota-se a existência de pontos a serem melhorados no padrão, o fato da ISO propor processos e recomendações generalistas, resulta em más interpretações e até mesmo aplicações erradas de suas sugestões, contudo cabe aos gestores compreenderem as necessidades da sua organização ou setor, analisarem os cenários que estão inseridos e adaptarem as sugestões da norma para a sua realidade. Portanto, conclui-se que a norma ISO 31000 é um conjunto de recomendações e princípios relevantes a serem considerados na construção das etapas e

processos de um modelo de gestão de riscos.

O presente trabalho norteará um futuro projeto que tem como objetivo o desenvolvimento de um modelo de gestão de risco com base na norma ISO 31000 para uma organização do estado de Sergipe.

REFERÊNCIAS

- ABNT. Associação Brasileira de Normas Técnicas. **ABNT NBR ISO 31000:2009 Gestão de Riscos: Princípios e Diretrizes**. Rio de Janeiro: ABNT, 2009.
- ABNT. Associação Brasileira de Normas Técnicas. **ABNT NBR ISO 31000:2018 Gestão de Riscos: Princípios e Diretrizes**. Rio de Janeiro: ABNT, 2018.
- ALBERTON, A.. **Uma metodologia para auxiliar no gerenciamento de riscos e na seleção de alternativas de investimentos em segurança**. Dissertação (Mestrado em Engenharia de Produção) - Universidade Federal de Santa Catarina, Florianópolis, 1996.
- ALESSANDRI, T. M.; FORD, D. N.; LANDER, D. M.; LEGGIO, K. B.; TAYLOR, M.. Managing risk and uncertainty in complex capital projects. **The Quarterly review of economics and finance**, v.44, n.5, p.751-767, 2004. DOI: <https://doi.org/10.1016/j.qref.2004.05.010>
- ALMEIDA, A. B.. O conceito de risco socialmente aceitável como componente crítico de uma gestão do risco aplicada aos recursos hídricos. In: CONGRESO DE LA AGUA, ASOCIACIÓN PORTUGUESA DE RECURSOS HÍDRICOS (APRH), 7. **Anais**. 2004.
- AMARO, A.. Consciência e cultura do risco nas organizações. **Territorium**, n.12, p.5-9, 2005. DOI: https://doi.org/10.14195/1647-7723_12_1
- AREOSA, J.. O risco no âmbito da teoria social. In: CONGRESSO PORTUGUÊS DE SOCIOLOGIA, 6. **Anais**. 2008.
- AVEN, T.. On the new ISO guide on risk management terminology. **Reliability Engineering and System Safety**, v.96, n.7, p.719-726, 2011. DOI: <https://doi.org/10.1016/j.res.2010.12.020>
- BARALDI, P.. **Gerenciamento de riscos empresariais Timburi**. São Paulo: Cia do eBook, 2018.
- BARRAGAN, L. G.; WEFFORT, E. F. J.; ARANHA, M. P. S.. O processo de gestão de riscos e controles internos nas entidades sem fins lucrativos como uma ferramenta para redução de custos. In: CONGRESSO BRASILEIRO DE CUSTOS-ABC. **Anais**. 2006.
- BERGAMINI JUNIOR, S.. Controles internos como um instrumento de governança corporativa. **Revista do BNDES**, v.12, n.24, p.149- 188, 2005.
- BERMÚDEZ, I. G.; RANGEL, L. J. A.. **V Diseño de un modelo de gestión integral del riesgo, basado en la norma ISO 31000:2018 en la clínica Girón ESE**. Monografía (Especialização em Gestão de Qualidade e saúde) - Universidade de Santander, Bucaramanga, 2019.
- CARVALHO, F. C. V. S.. **Fiabilidade na avaliação de risco: estudo comparativo de métodos semi-quantitativos de avaliação de risco em contexto ocupacional**. Tese (Doutorado em motricidade humana na especialidade em ergonomia) - Universidade de Lisboa, Lisboa, 2013.
- COOPER, D. F.; GREY, S.; RAYMOND, G.; WALKER, P.. **Project risk management guidelines: managing risk in large projects and complex procurements**. John Wiley & Sons, Inc., 2005.
- CORRÊA, R. G. F.. **Gestão integrada de riscos no agronegócio: um modelo para sistemas integrados de produção agropecuária**. Tese (Doutorado em Engenharia de produção) - Universidade Federal do Rio grande do Sul, Porto Alegre, 2019.
- CRUZ, C. O.; RODOVALHO, E. C.. Application of ISO 31000 standard on tailings dam safety. **REM-International Engineering Journal**, v.72, n.1, p.47-54, 2019. DOI: <https://doi.org/10.1590/0370-44672018720123>
- DEWI, L.; KITRI, M. L.. Operational Risk Analysis in Department of Enterprise Risk Management of PT. XYZ Based on ISO 31000: 2018 Framework. In: MANAGEMENT, BUSINESS AND ECONOMIC CONFERENCE (AMBEC 2019). **Annual**. Atlantis Press, p.33-38, 2020. DOI: <https://doi.org/10.2991/aebmr.k.200415.007>
- DUARTE JUNIOR, A. M.. Risco: definições, tipos, medição e recomendações para seu gerenciamento. LEMGRUBER, E. C. et al. **Gestão de riscos e derivativos: aplicação no Brasil**. São Paulo: Atlas, 2001.
- DUARTE, H. O.; DROGUETT, E. A. L.. Análise Quantitativa de Risco de uma unidade de recuperação de enxofre em uma refinaria de petróleo. **Revista Gestão da Produção Operações e Sistemas**, n.2, p.23, 2012. DOI: <https://doi.org/10.15675/gepros.v0i2.756>
- FERNANDES, F. C.; BEVETTI, J. E.. Gestão de risco em micro e pequenas empresas: uma pesquisa na região sul do Brasil. In: ENCONTRO DE ESTUDOS EM EMPREENDEDORISMO E GESTÃO DE PEQUENAS EMPRESAS (EGEPE), 8. **Anais**. Goiânia, 2014.
- FISCHHOFF, B.; WATSON, S. R.; HOPE, C.. Defining risk. **Policy sciences**, v.17, n.2, p.123-139, 1984.
- FONSECA, R. C. V.. **Metodologia do trabalho científico**. Curitiba: IESDE Brasil S.A., 2012.
- HOLLÓS, A. C.; PEDERSOLI JUNIOR, J. L.. Gerenciamento de riscos: uma abordagem interdisciplinar. **Ponto de Acesso**, v.3, n.1, p.72-81, 2009. DOI: <http://dx.doi.org/10.9771/1981-6766rpa.v3i1.3314>
- HOLTON, G. A.. Defining risk. **Financial Analysts Journal**, v.60, n.6, p.19-25, 2004. DOI: <https://doi.org/10.2469/faj.v60.n6.2669>

IBA. Instituto Brasileiro de Atuária. **O Atuário**. Rio de Janeiro: IBA, 2020.

KLIEMANN NETO, K. J. F.; SOUZA, S. J.; CARMON, M. U. C.; MARQUERON, C.; RANGEL, A. D.; ABENSUR, O. E.. **A Gestão de Riscos como Ferramenta para Aumento da Competitividade das Empresas**. 2018.

LALONDE, C.; BOIRAL, O.. Gerenciamento de riscos através da ISO 31000: Uma análise crítica. **Gerenciamento de riscos**, v.14, n.4, p.272-300, 2012.

LEOPOLDINO, C. B.. **Avaliação de Riscos em Desenvolvimento de Software**. Dissertação (Mestrado em Administração de Empresas) - Universidade Federal do Rio Grande do Sul, Porto Alegre, 2004.

LIEBER, R. R.; ROMANO-LIEBER, N. S.. O conceito de risco: Janus reinventado. In: **Saúde e ambiente sustentável: estreitando nós**. Rio de Janeiro: FIOCRUZ, 2002.

MACHADO, A. C.. **Controladoria e Gerenciamento de riscos**. Monografia (Especialização em Controladoria e Auditoria) - AVM Faculdade Integrada, Rio de Janeiro, 2015.

MATIAS JUNIOR, R.. Análise quantitativa de risco baseada no método de Monte Carlo: abordagem PMBOK. In: CONGRESSO BRASILEIRO DE GERENCIAMENTO DE PROJETOS, 1. **Anais**. Florianópolis, 2006.

NASCIMENTO, R. R.; SOUSA JÚNIOR, A. B.. Auditoria, controle interno e gestão de risco: importantes aliados na tomada de decisão. **Entrepreneurship**, v.4, n.2, p.1-12, 2020. DOI: <https://doi.org/10.6008/CBPC2595-4318.2020.002.0001>

NÓBREGA, N. C. M.. **Um estudo teórico da avaliação de riscos em projetos de investimento em organizações**. Monografia (Engenharia de Produção) - Universidade Federal de Juiz de Fora, Juiz de Fora, 2007.

OLECHOWSKI, A.; OEHMEN, J.; SEERING, W.; BEN-DAYA, M.. The professionalization of risk management: What role can the ISO 31000 risk management principles play?. **International Journal of Project Management**, v.34, n.8, p.1568-1578, 2016. DOI: <https://doi.org/10.1016/j.ijproman.2016.08.002>

OLIVEIRA, M. F.. **Metodologia científica: um manual para a realização de pesquisas em Administração**. Catalão: Universidade Federal de Goiás, 2011.

OLIVEIRA, U. R.; MARINS, F. A. S.; ROCHA, H. M.; SALOMON, V. A. P.. The ISO 31000 standard in supply chain risk management. **Journal of Cleaner Production**, v.151, p.616-633, 2017. DOI: <https://doi.org/10.1016/j.jclepro.2017.03.054>

PALMA, M. A. M.; ANDRADE, J. L. P.; PEDRO, J. S.. Gestão de riscos em projeto: contornando incertezas para viabilizar a implantação de nova tecnologia em uma indústria

petrolífera de E&P. **Gestão e Projetos: GeP**, v.2, n.2, p.102-122, 2011. DOI: <http://doi.org.10.5585/gep.v2i2.43>

PAULO, W. D. L.; FERNANDES, F. C.; RODRIGUES, L. G. B.; EIDIT, J.. Riscos e controles internos: uma metodologia de mensuração dos níveis de controle de riscos empresariais. **Revista Contabilidade & Finanças**, v.18, n.43, p.49-60, 2007. DOI: <https://doi.org/10.1590/S1519-70772007000100005>

PENHA, J. C.; PARISI, C.. Um caminho para integrar a gestão de riscos à controladoria. In: ANAIS DO CONGRESSO BRASILEIRO DE CUSTOS-ABC. **Anais**. 2005.

RABECHINI JUNIOR, R.; CARVALHO, M. M.. Relacionamento entre gerenciamento de risco e sucesso de projetos. **Production**, v.23, n.3, p.570-581, 2013. DOI: <https://doi.org/10.1590/S0103-65132012005000091>

RELIM, T. E.; OLIVEIRA, E. C.; MARIANO, A. M.; GRUBISIC, V. V. F.. Capital econômico para risco de crédito: gestão de riscos do processo de cálculo por meio da aplicação da norma abnt iso 31000 e da matriz GUT. **Brazilian Journal of Development**, v.6, n.5, p.25369-25384, 2020. DOI: <https://doi.org/10.34117/bjdv6n5-115>

RENN, O.. Concepts of risk: a classification. In: KRIMSKY, S.; GOLDING, D.. **Social Theories of Risk**. Westport: Praeger, 1992.

RODRIGUES, W. C.. **Metodologia científica**. Paracambi: Faetec/IST, 2007.

ROSA, G. M.; TOLEDO, J. C.. Gestão de riscos e a norma ISO 31000: importância e impasses rumo a um consenso. In: CONGRESSO BRASILEIRO DE ENGENHARIA DE PRODUÇÃO, 5. **Anais**. 2015.

SANTOS, M. M.. **O Controle interno e a gestão de risco nas empresas da área metropolitana do Porto**. Tese Doutorado) - Instituto Superior de Contabilidade e Administração do Porto, Porto, 2013.

SILVA, C. E. S. D.; MELLO, C. H. P.; SIQUEIRA, N. F. G.; GODOY, H. A.; SALGADO, E. G.. Aplicação do gerenciamento de riscos no processo de desenvolvimento de produtos nas empresas de autopeças. **Production**, v.20, n.2, p.200-213, 2010. DOI: <https://doi.org/10.1590/S0103-65132010005000023>

WESTERMAN, G.; HUNTER, R.. **O risco de Ti convertendo ameaças aos negócios em vantagem competitiva**. São Paulo: M. Books do Brasil, 2008.

ZACARI, R. X.. **Gerenciamento de riscos no varejo omnichannel**. Monografia (Bacharelado em Engenharia de Produção) – Escola Politécnica da Universidade de São Paulo, São Paulo, 2018.

ZONATTO, V. C. S.; BEUREN, I. M.. Categorias de riscos evidenciadas nos relatórios da administração de empresas brasileiras com ADRs. **RBGN: Revista Brasileira de Gestão de Negócios**, v.12, n.35, p.141-155, 2010.