Revista Boletim do Gerenciamento

Site: www.nppg.org.br/revistas/boletimdogerenciamento

Gerenciamento de Riscos: Uma Comparação entre o Guia PMBOK 6ª Edição e a ISO 31000:2018

FONTE Eduardo Côrtes da

Pós-graduando em Gestão e Gerenciamento de Projetos, NPPG/POLI - UFRJ

Informações do Artigo

Histórico:
Recebimento: 06 Dez 2018
Revisão: 07 Dez 2018
Aprovação: 11 Dez 2018

Palavras-chave:
Gerenciamento de Riscos
PMBOK
ISO31000

Resumo:

Este artigo visa identificar as similaridades e diferenças da sexta edição do Guia do Conhecimento em Gerenciamento de Projetos (Guia PMBOK, PMI, 2017) e a Norma ABNT ISO 31000:2018 (ABNT, 2018) na abordagem do gerenciamento de riscos. Baseada principalmente nas informações dos dois documentos. Primeiro será realizada uma leitura dos documentos, após isso será feita uma comparação indicando as similaridades e diferenças entre eles. Listando as similaridades, que são superiores em números, e as diferenças, aponta-se sugestões para trabalhos futuros.

1. Introdução

Todos os projetos possuem riscos, lidar com eles é um dever da organização que deseja ser bem-sucedida em seus projetos, para isso um gerenciamento de riscos bem estruturado é fundamental.

De forma abrangente, o gerenciamento de riscos se baseia num grupo de processos que tem por objetivo aumentar as chances de sucesso do projeto. Riscos podem ser algo desejado ou evitado, mas nossas percepções em relação ao termo tendem a ser sempre negativas [1]. Os riscos negativos (ameaças) devem ser prevenidos ou mitigados, já os riscos positivos (oportunidades) devem ser aproveitados ao máximo.

David Hillson [2] diz que o gerenciamento de riscos não é uma tarefa difícil, ele simplesmente nos oferece uma forma estruturada para pensarmos sobre o risco e como lidar com eles intuitivamente.

Seguindo este pensamento, após a leitura e resumo das informações destes documentos, este artigo visa analisar comparativamente dois conjuntos de boas práticas já bem consolidados na abordagem do gerenciamento de riscos, a sexta edição do Guia do Conhecimento em Gerenciamento de Projetos, o Guia PMBOK, de 2017, e a última versão da ISO31000 de 2018. Citando cada um dos seus processos e abordagens para depois comparar suas similaridades e diferenças.

2. Gestão de Riscos segundo o PMI

O Guia do Conhecimento em Gerenciamento de Projetos (Guia PMBOK), editado pelo *Project Management Institute* (PMI), é um guia de boas práticas para o gerenciamento de projetos. Este artigo se baseia na versão mais recente desse guia, a sexta edição lançada no ano de 2017.

O PMI [3] trata os riscos em dois níveis: o risco individual do projeto e o risco geral do projeto. O primeiro é relacionado com os riscos que atingem um ou mais objetivos do projeto, podendo gerar um efeito positivo (oportunidade) ou negativo (ameaça). Já o risco geral do projeto é dado como a incerteza do projeto como um todo, decorrente de todas as fontes de incerteza, incluindo os riscos individuais.

Dentro do PMBOK, o gerenciamento de riscos tem por objetivo explorar os riscos positivos aproveitando as oportunidades e, ao mesmo tempo, evitar ou reduzir os riscos negativos, ou seja, as ameaças.

Os riscos podem surgir a qualquer momento na vida de um projeto, desta forma, o seu gerenciamento deve ocorrer de forma iterativa, sendo seu foco a garantia de que todos os riscos sejam considerados. [3]

Como definido pelo PMI [3], projeto é um esforço temporário empreendido para criar um produto, serviço ou resultado único. Sendo assim, convém que os processos de gerenciamento de riscos sejam ajustados conforme as características do projeto. Pode-se citar:

1. Porte do projeto;
2. Complexidade do projeto;
3. Importância do projeto.

2.1 Os Processos do PMBOK

O PMI [3] define sete processos para o gerenciamento dos riscos, sendo eles:

1. Planejar o gerenciamento dos riscos;
2. Identificar os riscos;
3. Realizar a análise qualitativa dos riscos;
4. Realizar a análise quantitativa dos riscos;
5. Planejar as respostas aos riscos;
6. Implementar respostas aos riscos;
7. Monitorar os riscos.

2.1.1 Planejar o Gerenciamento dos Riscos

Este é o processo onde se define como serão conduzidas as atividades do gerenciamento de riscos do projeto. Deve-se garantir que o grau, tipo e visibilidade do gerenciamento de riscos sejam proporcionais aos riscos e à importância do projeto.

Como entradas deste processo, temos: termo de abertura do projeto, plano de gerenciamento do projeto, registro das partes interessadas, fatores ambientais e os ativos organizacionais (dentre eles a política da organização quanto aos riscos, definições de conceitos e papéis e responsabilidades).

Utiliza-se como ferramentas a opinião especializada, análise de dados e reuniões.

E como saída, temos o plano de gerenciamento de riscos. [3]

2.1.2 Identificar os Riscos

A Identificação dos riscos é o processo que identifica os riscos individuais e as fontes do risco geral do projeto, além da documentação de suas características. Tais informações são relevantes para que a equipe possa responder de forma apropriada os riscos identificados. Esse processo deve ser realizado ao longo de todo o projeto.

As entradas desse processo são: o plano de gerenciamento do projeto (que inclui o plano de gerenciamento dos requisitos, plano de gerenciamento do cronograma, plano de gerenciamento de custos, dentre outros), documentos do projeto (registro de premissas, estimativas de custos, estimativas de duração, entre outros), acordos e documentação caso o projeto exija aquisições externas, fatores ambientais (banco de dados de riscos, resultados de *benchmarking*, estudos de projetos semelhantes, dentre outros) e ativos de processos organizacionais (arquivos do projeto, especificações de riscos, dentre outros).

Como ferramentas utiliza-se a opinião especializada (expertise de pessoas ou

grupos), coleta de dados (brainstormings, listas de verificações, entrevistas etc.), análise de dados (premissas e restrições, análise SWOT, análise de dados, dentre outros), habilidades interpessoais de facilitação, listas de alertas de riscos e realização de reuniões.

E como saídas temos o registro de riscos (lista de riscos identificados, responsáveis pelos riscos, respostas aos riscos etc.), relatórios de riscos que apresentam informações sobre o risco geral e os ricos individuais, como última saída temos a atualização de documentos do projeto (registros de premissas, registro de questões, lições aprendidas, dentre outros). [3]

2.1.3 Realizar a Análise Qualitativa dos Riscos

Este é o processo onde se prioriza os riscos individuais do projeto para serem analisados ou para tomada de ação futura. Esta priorização é realizada com base na avaliação de probabilidade e impacto, assim pode-se concentrar os esforços nos riscos de alta prioridade. Este processo deve ser realizado ao longo de todo o projeto.

Como entradas deste processo temos: o plano de gerenciamento do projeto (que inclui o plano de gerenciamento dos riscos), documentos do projeto (registro de premissas, registro de riscos, registro das partes interessadas etc.), fatores ambientais (estudos de projetos semelhantes no setor, banco de dados de riscos etc.) e os ativos de processos organizacionais como informações de projetos semelhantes.

Utiliza-se como ferramentas a opinião especializada, coleta e análise de danos (avaliações de probabilidade e impacto dos riscos, avaliações de outros parâmetros dos riscos, dentre outros), facilitação como habilidade interpessoal, categorização dos riscos, representação dos dados (matriz de probabilidade e impacto, gráficos hierárquicos, por exemplo) e realização de reuniões especializadas.

A saída deste processo é a atualização nos documentos do projeto, como o registro de premissas, registro das questões, registro dos riscos e relatório dos riscos. [3]

2.1.4 Realizar a Análise Quantitativa dos Riscos

Este é o processo que analisa de forma numérica o efeito da combinação de riscos individuais. Ele quantifica a exposição do projeto ao risco geral e pode fornecer apoio e informações no planejamento das respostas aos riscos. A análise quantitativa é um processo que não é necessário em todos os projetos, mas caso seja usada deve ser realizada ao longo de todo o projeto.

As entradas desse processo são: o plano de gerenciamento do projeto (plano de gerenciamento de riscos, linha de base do escopo, do cronograma e dos custos, dentre outros), documentos do projeto (registro de premissas, bases de estimativas, estimativas de custos, estimativas de duração etc.), fatores ambientais da empresa e ativos de processos organizacionais.

As ferramentas utilizadas são a opinião especializada, coleta e análise de dados, representações da incerteza (representação em probabilidade quando a duração, escopo, custo ou requisitos são incertos).

A saída deste processo é a atualização nos documentos do projeto, como a avaliação ao risco geral do projeto, análise probabilística detalhada e lista de priorização dos riscos individuais. [3]

2.1.5 Planejar as Respostas aos Riscos

Este processo visa desenvolver alternativas, estratégias e ações para lidar com o risco geral e os ricos individuais do projeto. Ele identifica de forma apropriada qual abordagem utilizar para o risco geral e os ricos individuais. É um processo que deve ocorrer ao longo de todo o projeto.

Como entradas deste processo temos: plano de gerenciamento do projeto (plano de gerenciamento dos recursos, dos riscos, linha

de base dos custos etc.), documentos do projeto (registro de lições aprendidas, cronograma do projeto, registros dos riscos, dentre outros), fatores ambientais e ativos organizacionais

As ferramentas utilizadas são: opinião especializada, coleta de dados, facilitação como habilidade interpessoal, estratégias para ameaças (escalar, prevenir, transferir, mitigar ou aceitar o risco), estratégias para oportunidades (escalar, explorar, compartilhar, melhorar e aceitar as oportunidades), estratégias de resposta de contingências (plano de respostas que é utilizado somente quando condições predefinidas ocorrem), estratégias para o risco geral do projeto (prevenir, explorar, transferir, compartilhar, mitigar, melhorar ou aceitar), a análise de dados e a tomada de decisão.

E como saídas temos solicitações de mudanças (mudanças nas linhas de base de custo, cronograma ou outros componentes), atualizações no plano de gerenciamento do projeto (atualizar o plano de gerenciamento do cronograma, dos custos, da qualidade, dos recursos etc.) e atualizações de documentos como registro de premissas, registro de riscos e atribuições da equipe. [3]

2.1.6 Implementar Respostas aos Riscos

Este foi um processo adicionado nesta 6ª edição do Guia PMBoK [3], ele visa garantir que as respostas acordadas aos riscos sejam implementadas conforme o planejamento, tendo como objetivo minimizar as ameaças individuais e maximizar as oportunidades do projeto ao longo de todo o projeto. As entradas deste processo são o plano de gerenciamento do projeto, documentos do projeto (registros de lições aprendidas, registros de riscos, relatórios de riscos etc.) e ativos de processos organizacionais.

As ferramentas utilizadas são a opinião especializada, influência como habilidade interpessoal e sistema de informações de gerenciamento de projetos (*softwares* de cronograma, recursos e custos)

E como saídas temos as solicitações de mudanças (na linha de base dos custos, cronogramas e outros) e atualizações de documentos do projeto (registro de questões, registro de lições aprendidas, registros de riscos etc.). [3]

2.1.7 Monitorar os Riscos

Este processo tem por objetivo monitorar a implementação das respostas aos riscos, acompanhamento dos riscos já identificados, identificação de novos riscos e a avaliação do processo de riscos ao longo de todo o projeto. Com este processo, decisões podem ser tomadas com informações atualizadas sobre o risco geral e os riscos individuais do projeto.

Como entradas deste processo temos: o plano de gerenciamento do projeto, documentos do projeto (registro de questões, registro de lições aprendidas, registros dos riscos etc.), dados de desempenho do trabalho (informações sobre o *status* do projeto) e relatórios de desempenho do trabalho (informações de medições do projeto).

As ferramentas utilizadas nesse processo são: análise de dados (análise do desempenho técnico, análise de reservas, dentre outros), auditorias para verificar a eficácia do processo de gerenciamento dos riscos e reuniões para revisões de riscos.

E suas saídas são: informações sobre o desempenho do trabalho, solicitações de mudanças (mudanças na linha de base de custos, cronogramas e outros), atualizações no plano de gerenciamento do projeto, atualizações de documentos (registros de premissas, de lições aprendidas, dos riscos, dentre outros) e atualizações nos ativos de processos organizacionais (modelos de planos de gerenciamento dos riscos, registros e relatórios dos riscos, estrutura analítica dos riscos etc.). [3]

3. Gestão De Riscos Segundo a ABNT

A ISO 31000[4] é um guia que fornece princípios e processos para o gerenciamento

de riscos. Editada pelo *International Organization for Standardization*, sua última revisão foi finalizada neste ano de 2018 pelo comitê técnico ISO/TC 262. No Brasil, a ISO 31000 é publicada pela ABNT. Diferente de outras normas ISO, a ISO 31000 não é certificável.

Segundo Tranchard [5], a ISO 31000:2018 fornece um guia claro, curto e conciso que ajudará as organizações a usar os princípios do gerenciamento de riscos para melhorar o planejamento e tomar melhores decisões. Em comparação com a versão anterior da norma de 2009, as principais mudanças foram:

- Revisão nos princípios do gerenciamento de riscos;
- Foco na liderança, que deve garantir a integração do gerenciamento de riscos em todas as atividades da organização;
- Grande ênfase na natureza iterativa do gerenciamento de riscos;
- Maior foco na manutenção de um ambiente aberto, que troque *feedback* regularmente com o ambiente externo.

A ISO 31000:2018[4] define que risco é o efeito da incerteza nos objetivos, podendo ser positivo, negativo ou ambos e pode abordar, criar ou resultar em oportunidades e ameaças, e que a gestão de riscos é um conjunto de atividades coordenadas para dirigir e controlar uma organização no que se refere a riscos, sendo seu propósito a criação e proteção de valor.

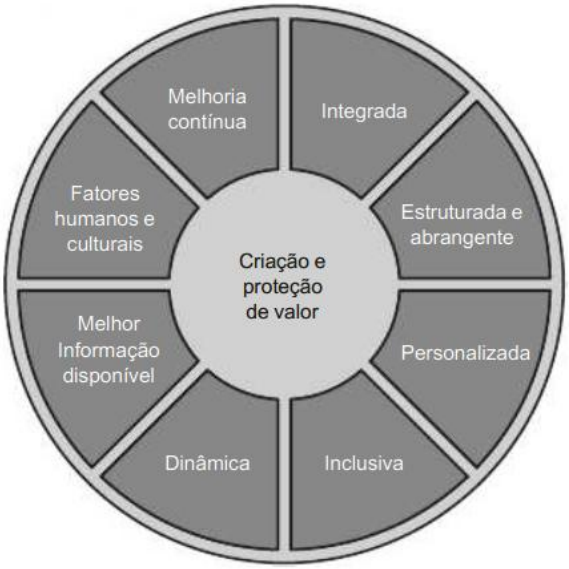
A norma explicita que organizações de todos os tamanhos e tipos sofrem influências de fatores externos e internos que tornam seus objetivos incertos de serem alcançados.

Para a ABNT [4], o gerenciamento dos riscos, deve se basear nos princípios, estrutura e processos.

3.1 Princípios

A ISO 31000 [4] define que os princípios (Figura 1) são uma base para o gerenciamento de riscos e que devem ser considerados quando se estabelece uma estrutura de gerenciamento de riscos na organização.

Figura 1 – Princípios da norma ABNT ISO 31000



Fonte: ABNT (2018) [4]

Seus princípios, vistos na Figura 1, podem ser resumidos em:

1. A gestão de riscos deve ser parte integrante de todas as atividades organizacionais;
2. Abordagens estruturadas e abrangentes contribuem para resultados consistentes;
3. Estrutura e processos devem ser personalizados em proporção aos contextos externos e internos da organização;
4. O envolvimento das partes interessadas possibilita conhecimento e novos pontos de vistas a serem considerados, o que resulta numa maior conscientização;
5. Riscos podem surgir, mudar ou desaparecer a qualquer momento. A gestão de riscos deve antecipar, reconhecer e dar respostas a estas mudanças de maneira apropriada;
6. As entradas para a gestão de riscos são baseadas em informações passadas e atuais, além de expectativas futuras. A gestão de

riscos deve considerar as limitações e incertezas destas informações;

7. O comportamento humano e a cultura da organização influenciam diretamente, em todos os estágios e níveis, na gestão de riscos;

8. A gestão de riscos deve ser melhorada continuamente por meio do aprendizado e experiência (ABNT, 2018) [4].

3.2 Estrutura

A estrutura da gestão de riscos tem como propósito apoiar a organização na integração da gestão (Figura 2). A eficácia da gestão de riscos está diretamente ligada à esta integração na governança e demais atividades, incluindo as tomadas de decisão, e para isto, o apoio de todas as partes interessadas, incluindo a alta direção, é fundamental. [4]

Figura 2 – Estrutura da norma ABNT ISO 31000

Fonte: ABNT (2018) [4]

3.2.1 Liderança e Comprometimento

É dever da alta direção e dos órgãos de supervisão, caso existam, assegurar que a gestão de riscos esteja totalmente integrada nas atividades da organização e que exponham comprometimento personalizando e implementando a estrutura, assegurando recursos para a gestão de riscos, atribuindo autoridade e responsabilidade dentro da organização.

Tais atitudes ajudarão no alinhamento da gestão de riscos com os objetivos estratégicos, na comunicação do valor da gestão de riscos, na promoção do monitoramento sistemático dos riscos, no desenvolvimento de critérios para assumir, ou não, determinados riscos e assegurar que a estrutura de gestão de riscos seja apropriada no contexto da organização [4].

3.2.2 Integração

A estrutura de uma organização tem relação com seu propósito e metas e a integração da gestão de riscos é apoiada por esta estrutura, tendo que os riscos serem gerenciados em toda sua cadeia. Assim, todos na estrutura da organização têm o dever de gerenciar os riscos.

Dentro da organização, a governança é que tem o papel de orientar o rumo que a organização vai tomar, as regras, processos e práticas utilizadas. Quem determina a responsabilidade e os papéis de cada um no gerenciamento de riscos é a governança.

O ato de integrar a gestão de riscos em uma organização deve ser algo dinâmico e iterativo, além de ser personalizado para as necessidades e cultura da empresa. É necessário fazer da gestão de riscos parte integrante do propósito organizacional [4].

3.2.3 Concepção

Ao criar a estrutura para gerenciar riscos, a organização deve estar atenta a alguns fatores externos e internos.

Para os fatores externos pode-se citar, dentre outros: fatores políticos, culturais, financeiros e tecnológicos, direcionadores que afetem os objetivos, valores, necessidades e expectativas, além dos compromissos contratuais.

Já para os fatores internos pode-se citar, dentre outros: visão, missão e valores, a governança e a estrutura da organização, as

estratégias, objetivos e políticas, a cultura da organização e as normas, diretrizes e modelos adotados.

É dever da alta direção demonstrar seu comprometimento com a gestão de riscos através de uma política, declaração ou qualquer outra forma que transmita de maneira clara os objetivos com a gestão de riscos.

Outro papel da alta direção é atribuir autoridade, responsabilidade e responsabilizações para os papéis pertinentes à gestão de riscos. Tal comunicação deve ocorrer em todos os níveis da organização. Além disso, deve-se garantir a alocação de recursos apropriados, sejam pessoas, processos ou métodos, para a gestão de riscos.

E, por último, a organização deve estabelecer uma abordagem para a comunicação e consulta. Por comunicação, entende-se o compartilhamento de informação com o público-alvo. Já por consulta, entende-se o *feedback* dos participantes. As informações resultantes da comunicação e consulta devem ser utilizadas de forma apropriada, sendo elas coletada, sintetizada e compartilhada. [4]

3.2.4 Implementação

A implementação da gestão de riscos em uma organização deve ser realizada de forma apropriada, desenvolvendo-se um plano que inclua prazos e recursos, com a identificação de quem ou como irá tomar certa decisão, com a modificação de processos caso haja necessidade e com a garantia de que as mudanças realizadas para a adequação à gestão de riscos sejam compreendidas de forma clara por todos os envolvidos. [4]

3.2.5 Avaliação

Para garantir a eficácia da estrutura de gestão de riscos, a organização deve mensurar periodicamente tal estrutura com base nos objetivos traçados e determinar se ela permanece adequada para apoiar o alcance destes objetivos. [4]

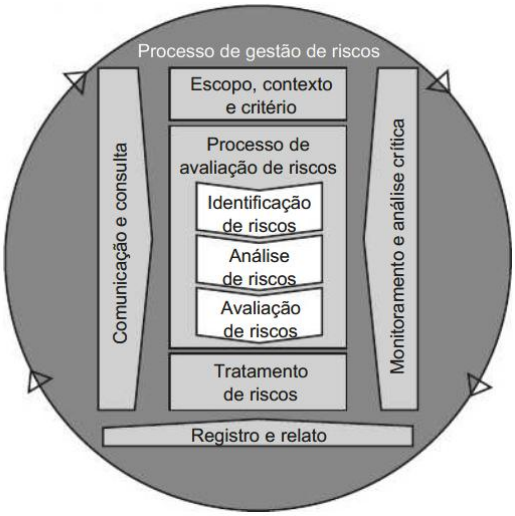
3.2.6 Melhoria

A melhoria na estrutura de gerenciamento de riscos deve ser contínua para abranger mudanças externas e internas e assim agregar valor à organização, melhorando continuamente a adequação e suficiência da estrutura e a forma de como os processos são integrados. [4]

3.3 Processos

Os processos de gestão de riscos da NBR ISO 31000:2018 [4] (Figura 3), assim como citado pela própria norma, devem ser partes integrantes da gestão e da tomada de decisão, sendo integrados nas operações e processos da organização.

Figura 3 – Processos da norma ABNT ISO 31000



Fonte: ABNT (2018)[4]

Os processos devem ser personalizados para que se adequem ao contexto da organização, tanto interno como externo, além de se considerar a natureza dinâmica do comportamento humano e a cultura organizacional. [4]

Os processos da norma, como vistos na Figura 3 são:

1. Comunicação e consulta;

2. Escopo, contexto e critérios;
3. Processos de avaliação de riscos;
4. Tratamento dos riscos;
5. Monitoramento e análise crítica;
6. Registro e relato.

3.3.1 Comunicação e consulta

Este processo tem como propósito o auxílio das partes interessadas na compreensão do risco, na tomada de decisões e nas razões pelas quais certas ações são executadas.

A comunicação tem por objetivo a conscientização e entendimento do risco, já a consulta envolve obter o retorno e informações pertinentes das partes interessadas.

Este processo visa a troca de informações executada de maneira correta, reunião de diferentes áreas de especialização no processo de gestão de riscos, assegurar que pontos de vistas diferentes sejam considerados, fornecimento de informações suficientes para a supervisão dos riscos e tomada de decisão e construção de um senso de inclusão e propriedade entre as partes afetadas pelo risco. [4]

3.3.2 Escopo, contexto e critério

Este processo tem como propósito a personalização do processo de gestão de riscos, ajudando na eficácia do processo de avaliação dos riscos e nas respostas apropriadas aos riscos. [4]

3.3.2.1 Definição do Escopo

É dever da organização definir o escopo de suas atividades de gestão de riscos. A clareza deste escopo e do alinhamento com os objetivos organizacionais é fundamental.

Alguns pontos devem ser abordados, como os objetivos e decisões a serem tomadas, os resultados esperados, ferramentas e técnicas para a avaliação dos riscos, recursos requeridos, responsabilidades, registros a serem mantidos, relacionamentos com outros processos e atividades, dentre outros. [4]

3.3.2.2 Contexto externo e interno

O contexto do processo de gestão de riscos deve ser estabelecido a partir da compreensão dos ambientes externos e internos que a organização opera. Esta compreensão é deveras importante, pois a gestão de riscos ocorre no contexto dos objetivos e atividades da organização. Também vale ressaltar que no que tange o contexto interno, fatores organizacionais podem ser uma fonte de risco.

O estabelecimento destes contextos internos e externos do processo de gestão de riscos deve considerar os fatores mencionados na estrutura da gestão, sendo neste artigo o item 3.2.3. Concepção. [4]

3.3.2.3 Definição dos critérios de risco

A organização deve especificar a quantidade e o tipo de riscos que pode ou não assumir, estabelecer critérios para avaliar a significância do risco e apoiar os processos de tomada de decisão. Os critérios dos riscos devem refletir os valores, objetivos e recursos da organização e ser consistentes com as políticas e declarações sobre gestão de riscos.

Mesmo que seja conveniente que os critérios de riscos sejam estabelecidos no início do processo de avaliação de ricos, este é um processo dinâmico e iterativo e deve ser continuamente analisado criticamente e alterado quando necessário. [4]

3.3.3 Processos de avaliação de riscos

Este é o processo de identificação, análise e avaliação de riscos. O processo de avaliação de riscos deve ser conduzido de forma iterativa, sistemática e colaborativa com base nos conhecimentos e pontos de vista das partes interessadas. [4]

3.3.3.1 Identificação de riscos

A identificação dos riscos tem por objetivo encontrar, reconhecer e descrever riscos positivos ou negativos. Alguns fatores devem ser considerados, dentre eles: mudanças no contexto interno e externo, indicadores de riscos emergentes, consequências e impactos nos objetivos e fatores temporais. [4]

3.3.3.2 Análise de Riscos

A análise de risco objetiva a compreensão do risco e suas características. Deve-se levar em consideração detalhes das incertezas, fontes de risco, consequências, probabilidade, eventos, cenários, controles e sua eficácia.

A Análise de riscos pode ser qualitativa, quantitativa ou uma combinação das duas formas.[4]

3.3.3.3 Avaliação de Riscos

A avaliação dos riscos compara os resultados da análise de riscos com os critérios que foram estabelecidos, assim, chegando a conclusão de como agir com o risco em questão. Podem-se considerar outras opções de tratamento, realizar análises adicionais, reconsiderar os objetivos ou até mesmo não fazer nada. [4]

3.3.4 Tratamento de Riscos

O propósito deste processo é selecionar e implementar uma ou mais opções para abordar os riscos.

O processo de tratamento de riscos deve realizar, de forma iterativa, a formulação de opções para o tratamento do risco, planejamento e implementação do tratamento, a avaliação da eficácia do tratamento aplicado, a decisão se o risco remanescente é aceitável e se não for, o tratamento adicional a este risco. [4]

3.3.5 Monitoramento e Análise Crítica

Este processo tem por objetivo melhorar a qualidade e eficácia da concepção, implementação e resultados da gestão de riscos. Deve existir um monitoramento contínuo e análise periódica do processo de gestão de riscos, além de que o monitoramento e análise crítica devem ocorrer em todos os estágios do processo. [4]

3.3.6 Registro e Relato

O processo de registro e relato visa a documentação de todos os processos da gestão de riscos, com o objetivo de comunicar as atividades de gestão de riscos em toda a organização, fornecer informações para a tomada de decisão e melhorar as atividades de gestão de riscos. A criação, retenção e manuseio das informações devem levar em consideração a sensibilidade da informação. [4]

4. Similaridades e Diferenças

De acordo com Gabriel, Matos e Kovaleski [6], ao realizar esta mesma comparação, mas com a versão de 2009 da ISO 31000 e com a 4ª edição do Guia PMBOK, de 2004, os dois documentos apresentam mais similaridades do que diferenças.

Tabela 1 – Diferenças e similaridades na abordagem do gerenciamento de risco

ITEM	PMI	ABNT
Processos aplicados aos projetos	✓	✓
Processos aplicados às demais atividades	X	✓
Trata de ferramentas a serem utilizadas	✓	X
Processos devem ser iterativos, repetitivos	✓	✓
Baseado no ciclo PDCA	✓	✓
Os processos devem ser personalizados	✓	✓

Fonte: Autor, 2018.

A Tabela 1 ilustra as diferenças e similaridades na abordagem do gerenciamento de risco entre as versões atuais. Uma das maiores diferenças entre as duas abordagens está na aplicação do conjunto de processos do gerenciamento de risco. Enquanto o PMI oferece uma abordagem em que processos de gerenciamento de riscos devem ser aplicados em projetos, a ISO 31000 diz que suas aplicações cabem a qualquer atividade.

A ISO 31000 não trata diretamente sobre ferramentas a serem utilizadas nos processos de avaliação dos riscos, sendo essa uma grande diferença com o Guia PMBOK, para isto existe a norma complementar ISO 31010 [7] cuja última versão foi publicada em novembro de 2009 e aqui no Brasil, em 2012 pela ABNT.

Atualmente, a ISO 31010 encontra-se sob revisão, segundo Epelbaum[8] esta nova versão vem para se alinhar com a revisão da ISO 31000.

Outra diferença que pode ser citada é a respeito da quantidade de processos. A 6ª edição do Guia PMBOK [3] apresenta sete processos, enquanto a ISO 31000:2018[4] apresenta seis processos. Quando se trata da comparação com as versões anteriores destes documentos, o número de processos se equiparava em seis. Essa diferença, porém, se trata apenas do agrupamento dos processos, pois as definições dos processos são bem semelhantes [6].

Os dois documentos insistem que os processos de gerenciamento de riscos devem ser tratados de forma iterativa, ou seja, de forma repetitiva [9], visando sempre ter a melhor fonte de informação possível para a tomada de decisão, além de atualizações contínuas sobre os riscos já identificados ou novos.

Os processos dos dois documentos se baseiam no ciclo PDCA [10], método criado por Walter A. Shewhart e mais tarde consolidado por William Edwards Deming. Composto pelas fases *Plan* (Planejar), *Do* (Executar), *Check* (Verificar) e *Act* (Agir) o ciclo pode ser utilizado de forma iterativa visando a melhoria continua dos processos.

Outra similaridade entre as duas abordagens é na necessidade de ajuste da aplicação dos processos de gerenciamento de riscos. É preciso uma personalização para se adequar ao contexto da organização, complexidade, porte e importância do projeto, além de diversas outras características que podem influenciar a forma de gestão.

5. Considerações Finais

Observa-se um padrão nas duas abordagens, tanto em sua estrutura que se utiliza do PDCA quanto no restante de suas boas práticas, podendo ser citadas aqui a personalização dos processos de gerenciamento de riscos dependendo da organização e/ou projeto e a forma iterativa como os processos devem ser executados, sempre buscando novas fontes de risco, respostas e ações a serem tomadas.

Os dois documentos são ótimas referências na implantação do gerenciamento de riscos, ou em sua expansão caso já exista algum trabalho na área dentro da organização.

Como as duas abordagens têm uma grande tendência de trabalhar de forma semelhante, seria de extrema facilidade para uma organização que já utiliza uma delas, implementar a outra para algum outro projeto ou fim, caso seja de seu interesse.

Para trabalhos futuros, sugere-se a continuação desta comparação com as respectivas novas versões dos documentos, já que suas atualizações ocorrem de tempos em tempos. Também, pode-se sugerir a implementação, nesta análise, da futura versão da norma ISO 31010 que trata das ferramentas utilizadas na avaliação de riscos da norma ISO 31000. Outra sugestão é analisar um caso onde ocorreu a implementação da norma ABNT ISO 31000

ou o uso concomitante dela com as boas práticas definidas pelo PMI.

6. Referências

[1] JOIA, Luiz Antonio et al. Gerenciamento de Riscos em Projetos**.** Rio de Janeiro: Fundação Getúlio Vargas, 2013.

[2] HILLSON, David. Risk management isn't hard. Project Manager Today, Reino Unido, p.25-25, maio 2009

[3] PMI. Um Guia do Conhecimento em Gerenciamento de Projetos**:** Guia PMBOK. 6. ed. Newtown Square: Project Management Institute, 2017.

[4]. NBR ISO 31000: Gestão de Riscos - Diretrizes. Rio de Janeiro, 2018.

[5] TRANCHARD, Sandrine. The new ISO 31000 keeps risk management simple. 2018. Disponível em: <https://www.iso.org/news/ref2263.html>. Acesso em: 13 out. 2018.

[6] GABRIEL, Marcos; MATOS, Eloisa Aparecida Ávila de; KOVALESKI, João Luiz. Gerenciamento de Riscos em Projetos de Inovação Tecnológica: uma Análise Comparativa entre o PMBOK e a ISO 31000. In: CONGRESSO BRASILEIRO DE ENGENHARIA DE PRODUÇÃO, 1., 2011, Ponta Grossa. 2011.

[7] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS NBR ISO 31010: Gestão de Riscos – Técnicas para o processo de avaliação de riscos. Rio de Janeiro, 2012.

[8] EPELBAUM, Michel. MUDANÇAS NA ISO 31000 – GESTÃO DE RISCOS**.** 2018. Disponível em: <http://elluxconsultoria.com.br/iso-31000-gestao-riscos/>. Acesso em: 10 set. 2018.

[9] POLITO, André Guilherme. Michaelis moderno dicionário da língua portuguesa. São Paulo: Melhoramentos, 2004.

[10] ANDRADE, Fábio Felippe de. O método de melhorias PDCA. 2003. Tese de Mestrado. Universidade de São Paulo.