

# GERENCIAMENTO DE RISCOS EM PROJETOS: UMA COMPARAÇÃO ENTRE O PMBOK E A ISO-31000

*Maildo Barros da Silva<sup>1</sup> e Fco.Rodrigo P. Cavalcanti<sup>2</sup>*

<sup>1</sup> Universidade de Fortaleza (UNIFOR), Fortaleza-CE, Brasil  
phone: +55(85) 96193248, email: maibarsilva@hotmail.com

<sup>2</sup> Universidade Federal do Ceará (UFC), Fortaleza-CE, Brasil  
phone: +55(85) 3666 9470, email: rodrigo@gtel.com.br

## Resumo

Este artigo tem o intuito de avaliar as similaridades e/ou diferenças na abordagem do Gerenciamento de Riscos dada pelo Guia do Conjunto de Conhecimentos em Gerenciamento de Projetos (PMBOK)[2] e a nova norma ISO31000 [1]. Esta avaliação consiste, principalmente, em análise e comparação entre ferramentas e técnicas empregadas em cada fase do gerenciamento de riscos. O artigo não se propõe a explicar detalhadamente os processos e procedimentos de gestão de riscos propriamente ditos, mas sim comparar a estrutura desse gerenciamento nestes dois documentos de boas práticas.

## 1. INTRODUÇÃO

O gerenciamento de riscos em geral, aplicado a projetos em particular, é um grupo de processos preconizado para as organizações modernas como forma de aumentar a probabilidade de sucesso em seus objetivos estratégicos, encorajar um gerenciamento proativo, minimizar perdas, realizar a prevenção de danos e acidentes, prover uma operação eficiente ou definir sua estratégia de planejamento. O PMBOK[2] é um guia de boas práticas para gerenciamento de projetos editado pelo PMI (Project Management Institute), cujo objetivo é organizar os processos de gestão de um projeto de forma que sejam aplicados durante as fases de seu ciclo de vida (Iniciação, Planejamento, Execução, Monitoramento e Controle e Encerramento).

Para o gerente de projetos que segue o PMBOK, o gerenciamento de riscos é uma das 9 áreas de conhecimento que devem ser aplicadas para atingir o sucesso em um projeto. A definição do guia PMBOK[2] para o gerenciamento de riscos é: "O gerenciamento de riscos em projetos tem como objetivo definir processos para a identificação, análise, respostas, monitoramento e controle e planejamento do gerenciamento de riscos em projetos". O objetivo de tal gerenciamento por sua vez é definido como sendo "aumentar a probabilidade e o impacto dos eventos positivos e diminuir a probabilidade e o impacto dos eventos negativos ao projeto". Em cada área de conhecimento, o PMBOK utiliza informações de entrada, ferramentas e saídas como forma de implementar os seus processos.

A norma ISO 31000[1] é editada pela ISO (International Standards Organization) e difere de várias outras normas ISO, não é certificável. Diferente do tratamento dado no PMBOK, a ISO 31000 estabelece princípios para o tratamento de riscos em geral, e não apenas no contexto de projetos. Ela vem de encontro ao entendimento de que todas as atividades em uma organização possuem riscos, e que todos estes riscos devem

ser identificados, analisados e quantificados para poderem ser modificados, segundo o critério de tratamento de riscos. A seguir abordaremos separadamente o gerenciamento de riscos do PMBOK e da ISO 31000.

## 2. O GERENCIAMENTO DE RISCOS PMBOK

A abordagem adotada pelo PMBOK para gerenciamento de um projeto inicia-se e fundamenta-se principalmente na definição dada para projetos, que é: "Um projeto é um esforço temporário empreendido para criar um produto, serviço ou resultado exclusivo". O PMBOK define que o gerenciamento de riscos inclui os processos que tratam da realização, análise, resposta, monitoramento e controle e planejamento de riscos em um projeto, tendo como objetivo principal aumentar a probabilidade e o impacto dos eventos positivos e diminuir a probabilidade e impacto dos eventos negativos ao projeto. Um fator importante a ser considerado é que todas as áreas de conhecimento utilizadas pelo PMBOK para o gerenciamento de projetos são integradas, donde resulta que as necessidades e objetivos dos projetos ficam mais claramente definidos, o que já auxilia o processo da identificação dos riscos do projeto.

A Figura 1 mostra a visão geral do gerenciamento de riscos do projeto, segundo o PMBOK.

### 2.1 Os Processos do Gerenciamento de Riscos

- Planejar o gerenciamento de riscos - O processo de definição de como conduzir as atividades de gerenciamento de riscos de um projeto.
- Identificar os riscos - O processo de determinação dos riscos que podem afetar o projeto e de documentação de suas características.
- Realizar a análise qualitativa dos riscos - O processo de priorização dos riscos para análise ou ação adicional através da avaliação e combinação da sua probabilidade de ocorrência e impacto.
- Realizar análise quantitativa dos riscos - O processo de analisar numericamente o efeito dos riscos identificados, nos objetivos gerais do projeto.
- Planejar as respostas aos riscos - O processo de desenvolvimento de opções e ações para aumentar as oportunidades e reduzir as ameaças aos objetivos do projeto.
- Monitorar e controlar os riscos - O processo de implementação de planos de respostas aos riscos, acompanhamento dos riscos identificados, monitoramento dos riscos residuais, identificação de novos riscos e avaliação da eficácia dos processos de tratamento dos riscos durante todo projeto.

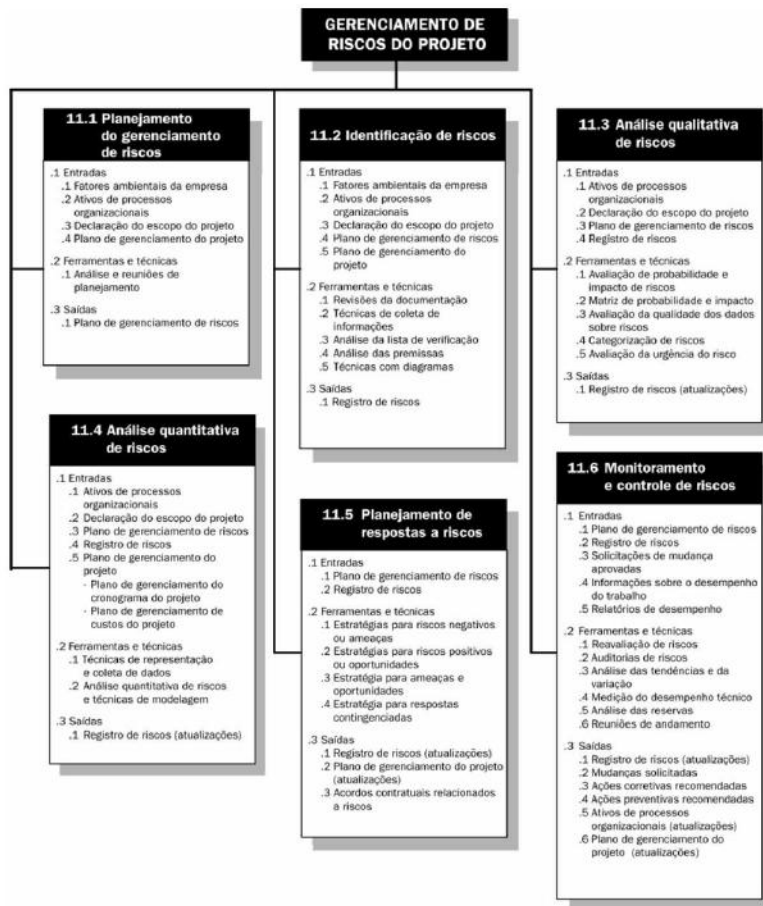


Figura 1: Visão geral do gerenciamento de riscos do projeto.

## 2.2 Entradas dos Processos

As entradas mais comuns dos processos de gerenciamento de risco, conforme denominado pelo PMBOK, são:

- Fatores ambientais da empresa;
- Ativos de processos organizacionais;
- Declaração de escopo do projeto;
- Plano de gerenciamento de projetos.

Por fim, cada saída vai agregar como entrada do processo seguinte ou no mínimo servir para a atualização dos documentos de entrada.

### 2.2.1 Ferramentas e técnicas

O PMBOK é bem claro ao definir suas ferramentas e mais ainda em detalhar as técnicas utilizadas durante todo o processo de gerenciamento de riscos, tais como:

- Análise e reuniões de planejamento;
- Revisões da documentação;
- Técnicas de coleta de informações, tais como: Brainstorming; Técnicas Delphi; Entrevistas; Identificação de causa-raiz; Análise de SOWT;
- Análise da lista de verificação;
- Análise das premissas;
- Técnicas com diagramas - Diagramas de causa e efeito;

Diagramas de sistemas ou fluxograma; Diagramas de influência;

- Avaliação de probabilidade e impacto;
- Matriz de probabilidade e impacto;
- Categorização dos riscos;
- Avaliação da urgência;
- Técnicas de representação e coleta de dados (Distribuição de probabilidades; Opiniões de especialistas);
- Análise quantitativa de riscos tais como: técnicas de modelagem; Análise de Valor monetário esperado; Análise da árvore de decisão e simulação Monte Carlo.

### 2.2.2 Saídas

Os produtos destas entradas com aplicação das ferramentas e técnicas citadas resultam principalmente nos principais produtos ou saídas dos processos que compõem o gerenciamento de riscos PMBOK:

- Plano de Gerenciamento de Riscos;
- Registros dos Riscos;
- As atualizações do plano de gerenciamento do projeto.

## 3. O GERENCIAMENTO DOS RISCOS NA ISO31000

A norma ISO31000 se propõe a descrever a sistemática e lógica no processo de gerenciamento de riscos, propondo que o

gerenciamento de riscos pode ser aplicado em todos os níveis de uma organização, seja para atividades de rotina ou projetos. A ISO31000 cita como chave do processo o termo “establishing the context”, que na realidade é entender os objetivos estratégicos da organização, o ambiente proposto para estes objetivos e quais os critérios que serão adotados para os riscos. Nesse sentido, a ISO 31000 tem uma abrangência e aplicabilidade potencialmente maior que o conteúdo equivalente proposto no PMBOK. A Figura 2 ilustra o arcabouço de gestão de risco proposto na ISO31000.

A ISO31000 adota em sua abordagem para o gerenciamento de riscos a seguinte concepção:

- Princípios
- Estrutura para o Gerenciamento de Riscos
- Processos para o Gerenciamento de Riscos

### 3.1 Princípios para o Gerenciamento de Riscos

Os princípios vão definir o contexto interno e externo que a organização vai dar para o gerenciamento dos riscos. Os princípios descritos na ISO31000 são :

- criar valor para os objetivos da organização;
- ser parte integrante de todo processo organizacional;
- fazer parte das decisões;
- explicitar as incertezas;
- prover a sistemática, estrutura e agilidade na abordagem do gerenciamento de riscos, contribuindo de forma eficiente e consistente;
- basear-se nas melhores informações;
- alinhar a organização ao contexto externo e interno;
- fatores culturais e humanos são levados em conta;
- processos transparentes e que incluam todas as pessoas interessadas;
- respostas a mudanças acontecem de forma dinâmica e interativa;
- prover a organização com ferramentas apropriadas continuamente.

### 3.2 Estrutura do Gerenciamento de Risco

#### Comunicação e Consulta

- Implantação do Comitê: Nesta fase é definida a política para gerenciamento dos riscos; deve-se alinhar a política com a cultura da organização; determinar os indicadores; alinhar os objetivos e estratégias organizacionais; comunicar a todos os interessados os benefícios da gestão dos riscos.
- Desenho da Estrutura de Gerenciamento de Riscos: entender a organização e o contexto em que ela está inserida; além disso: integrar os processos organizacionais; realizar pesquisas; estabelecer os mecanismos de comunicação internos e externos.
- Implementação do Gerenciamento de Riscos: definir a estratégia e tempo para implantação da estrutura; aplicabilidade da política de gerenciamento de riscos e dos processos organizacionais; os cumprimentos legais e regulamentações requeridas.
- Monitoramento e Revisão Medir: nessa etapa mede-se o desempenho do processo de gestão de riscos através de indicadores com periodicidade apropriada; além disso: acompanha periodicamente os desvios no plano de gerenciamento de riscos; os riscos e o progresso do plano de

gerenciamento de riscos.

- Revisão Contínua: baseada nos resultados dos monitoramentos e nas revisões; decisões que devem ser tomadas para manter a política e o planejamento.

Pode-se fazer um paralelo desta estrutura com o PDCA (plan/do/control/action)[2].

### 3.3 Processos de Gerenciamento de Riscos

Os processos de gerenciamento de riscos devem ser parte integrante da estrutura de gerenciamento da organização e devem ser parte também da sua cultura e práticas.

#### 3.3.1 Comunicação e Consulta

Processo contínuo e interativo de uma organização para fornecer, compartilhar ou obter informações, com relação ao gerenciamento de riscos. O processo de comunicação e consulta eficiente, tanto para contexto interno como externo, deve ser a base das decisões do que deve ser feito, quais as razões e que ações devem ser tomadas.

#### 3.3.2 Estabelecer o contexto

Definir os parâmetros externos e internos a serem levados em conta pelo gerenciamento de riscos, e estabelecimento de escopo e dos critérios de riscos a ser adotados para a política do sistema de gestão.

#### 3.3.3 Avaliação do Risco

No processo para avaliação do risco, estão presentes todos os processos para identificação, análise e valorização dos riscos.

- Identificação dos Riscos: A organização deve identificar as fontes, o impacto e os eventos de gatilho dos riscos.
- Análise: envolve o entendimento do risco, provendo ações para avaliar quantitativamente as decisões; e ainda as definições de quais riscos devem ser tratados e sua prioridade, as estratégias e métodos.
- Valorização dos Riscos: consiste em comparar o nível da gravidade dos riscos encontrados na fase de análise com o critério estabelecido no contexto considerado. Decisões devem ser tomadas considerando a tolerância a riscos admitida pela organização.

#### 3.3.4 Tratamento de Riscos

Processo para modificar os riscos, através de ações que serão tomadas para aumentar a probabilidade e impacto dos riscos positivos e/ou ações que serão tomadas para minimizar a probabilidade e impacto dos riscos negativos. É no tratamento que serão tomadas as ações para prevenir, transferir, mitigar os riscos negativos ou para os riscos positivos explorar, compartilhar e melhorar ou ainda até definir as ações para os riscos que serão aceitos.

#### 3.3.5 Monitoramento e Controle

É neste processo que são feitas as verificações, supervisão e observações críticas ou a identificação de situação, executadas de forma contínua, para com isto identificar mudanças dentro dos parâmetros de riscos assumidos e aplicar as ações de controles definidas para modificar a probabilidade e impacto associados com os riscos.

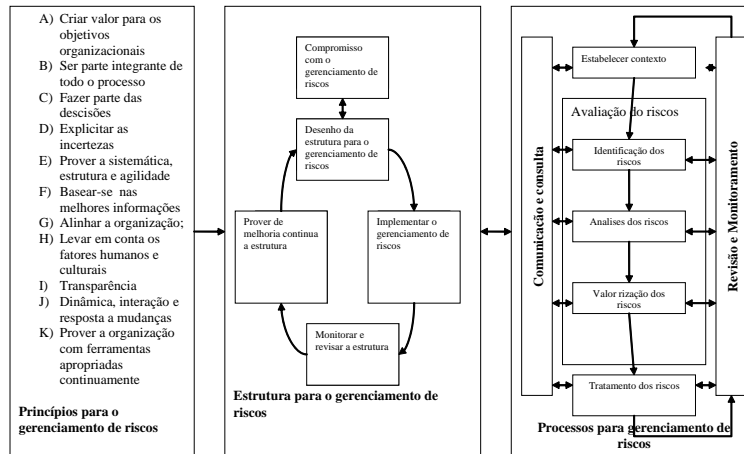


Figura 2: Relação entre o Princípio do Gerenciamento de Riscos, sua estrutura e processos.

#### 4. AS FERRAMENTAS E TÉCNICAS UTILIZADAS NO GERENCIAMENTO DOS RISCOS

Diferentemente do PMBOK a ISO31000 não define no seu texto as ferramentas e técnicas utilizadas para identificação dos riscos. Para especificar as ferramentas de tratamento de riscos, foi publicada a norma complementar ISO31010[4] que detalha as técnicas que devem ser utilizadas. Nesta norma a ISO classifica as ferramentas e técnicas quanto à sua aplicabilidade em cada fase, definindo também uma classificação destas ferramentas quanto a alguns atributos, tais como: grau de incerteza, complexidade e se a mesma pode prover uma saída quantitativa. De maneira similar, o PMI editou recentemente um padrão complementar intitulado "Practice Standard for Project Risk Management"[3] que aprofunda a discussão sobre o capítulo de gestão de riscos do PMBOK, com uma ênfase particular no detalhamento e classificação das ferramentas de análise de riscos. Na próxima seção é feita uma discussão mais detida sobre esse tópico com uma apresentação de uma tabela comparativa.

#### 5. DIFERENÇAS E SIMILARIDADES

Ao ler os dois documentos citados, observa-se mais similaridades do que diferenças. A principal similaridade se dá no objetivo que é comum, ou seja, prover a organização da capacidade de agir de forma a se beneficiar dos riscos positivos e se proteger de riscos negativos de forma a minimizar impactos.

Como grande diferença, temos a proposta de aplicação dos dois documentos: o PMBOK entende sua aplicação para projetos, enquanto que a ISO31000 prega a aplicação do gerenciamento de riscos tanto em atividades de rotina como em projetos. Este fato é entendido na forma que o PMBOK utiliza o gerenciamento de risco como conhecimento a ser aplicado em um projeto, e a ISO entende o gerenciamento como filosofia a ser aplicada na estrutura organizacional.

Na estruturação dos processos, a diferença está nos agrupamentos, já que a ISO trata 5(cinco) grupos de processos e o PMBOK utiliza 6(seis) grupos, mas o que se observa é que se trata somente de um agrupamento diferente e os processos das duas abordagens são essencialmente os mesmos. Este agrupamento se dá principalmente no Processo de Análises

de Risco na ISO31000 que trata as análises qualitativa, semi-qualitativa e quantitativa como fazendo parte de um único processo.

Os dois documentos utilizam o ciclo do PDCA(Plan/Do/Control/Action) para estabelecer a relação entre os componentes da estrutura do gerenciamento de riscos e manter o processo em constante evolução.

Um fator de relevância nesta análise é que o gerenciamento de risco em projeto faz parte de um grupo de processos, e por isto é beneficiado pela integração dos vários processos, e esta integração serve de suporte para o gerenciamento do risco. É esta integração entre os objetivos de escopo, tempo, qualidade e custo que auxilia ao gerente de projeto na análise e identificação dos riscos. Outra diferença que pode ser notada é que o PMBOK apresenta ferramentas que diferem da norma ISO em alguns casos. A Tabela 1 comparativa a seguir mostra que as ferramentas que são indicadas pelo PMBOK, na sua grande maioria, também são consideradas pela ISO como de forte aplicabilidade, mas o reverso nem sempre é verdadeiro.

#### 6. CONCLUSÕES

A ISO 31000 vem confirmar que metodologias adotadas pelo PMBOK são reconhecidamente boas práticas para o gerenciamento de risco. A aplicação do gerenciamento de riscos utilizada pelos Gerentes de Projetos pode ser também considerada como dentro dos padrões ISO, já que os processos e estruturas do gerenciamento dos riscos são em grande parte semelhantes. A semelhança entre as duas normas capacita as organizações, que já utilizam em seus projetos as orientações do PMBOK, a obter uma maior facilidade no caso de utilizar a ISO 31000 como metodologia de gerenciamento de riscos em suas outras atividades, pelo fato da transmissão das experiências das pessoas e nos documentos existentes sobre gerenciamento de riscos já implantados. Assim, o uso de uma das metodologias para gerenciamento dos riscos apresentadas, seja PMBOK ou ISO 31000, deve ser suficiente para o atendimento dos objetivos estratégicos das empresas, quanto ao tratamento de riscos na gestão de seus projetos. Se o objetivo é ampliar a gestão de riscos para operações e produção, a norma ISO31000 e sua norma complementar so-

Tabela 1: Ferramentas e Técnicas e suas aplicabilidades nas fases do Processo de Gerenciamento de Riscos.

<b>COMPARATIVO DAS FERRAMENTAS E TÉCNICAS PARA O GERENCIAMENTO DOS RISCOS ENTRE A NORMA PRÁTICA PARA GERENCIAMENTO DOS RISCOS - PMBOK E A ISO31010</b>						
Técnicas ISO	Identificação do Risco		Análises de Riscos	Avaliação do Risco	Tratamento do Risco	Revisão e Monitoramento
Técnicas PMBOK	Planejamento	Identificação	Análise Qualitativo	Análise Quantitativo	Planejamento de Resposta	Monitoramento e Controle
Análise e reuniões de Planejamento	PMBOK					
Análises das Premissas		PMBOK				
Análises da modo de Falha (FMEA)		PMBOK/ISO		PMBOK/ISO		
Análises das Forças		PMBOK			PMBOK	
Análise da Arvore de Decisão				PMBOK/ISO		
Análise da Identificação Causa-Raiz		PMBOK/ISO	PMBOK/ISO		PMBOK	
Análise de SWOT		PMBOK				
Análise do Cenário					PMBOK	
Análise das Reservas						PMBOK
Análises das Variações						PMBOK
Análises das Tendências						PMBOK
Análise da Gravata Borboleta(Bow Tie Analysis)				ISO	ISO	
Análises de Markov			ISO			
Árvore de Evento		ISO	ISO	ISO	ISO	
Brainstorming		PMBOK/ISO			PMBOK	
Bayes Net			ISO		ISO	
Curvas FN		ISO	ISO	ISO	ISO	
Check List		PMBOK/ISO			PMBOK	
Conhecimento da Indústria (Benchmarking)		PMBOK/ISO			PMBOK	
Corrente Crítica					PMBOK	PMBOK
Diagrama de Causa e Efeito(Ishikawa)		PMBOK/ISO	ISO			
Diagrama de Influência		PMBOK				
Diagrama de Sistemas ou Fluxogramas		PMBOK		PMBOK		
Estimativa da Reserva de Contingência					PMBOK	
Entrevistas		PMBOK/ISO			PMBOK	
Estrutura What - if?(Swift)		ISO	ISO	ISO	ISO	
Estrutura Analítica de Risco(EAR)		PMBOK				
Grupo Técnico		PMBOK			PMBOK	
HACCP Análises e Pontos de controle crítico		ISO				
HAZOP - Análise de Riscos e Perigo		ISO	ISO			
HRA(Human reliability assessment)		ISO	ISO	ISO	ISO	
Layer protection Analysis(LOPA)			ISO			
Lições Aprendidas		PMBOK	PMBOK	PMBOK	PMBOK	
Lista de Verificação		PMBOK				
Matriz de Probabilidade e Impacto		ISO	PMBOK/ISO			
Plano de Contingência					PMBOK	
Processo Analítico Hierárquico			PMBOK/ISO			
Questionário		PMBOK				
Revisão de Documentos		PMBOK/ISO				
Revisão da EAR		PMBOK				
Re Análise dos Riscos(PDCA)						PMBOK
Reuniões de Andamento						PMBOK
Sneak Circuit Analysis		ISO				
Simulação de Monte Carlo				PMBOK/ISO		
Técnica de Seleção de Multi Critérios					PMBOK	
Técnicas de estimativas			PMBOK/ISO			
Técnica de Delphi		PMBOK/ISO				
Valor Monetário Esperado (EMV)				PMBOK/ISO	PMBOK	

bre ferramentas de análise, a ISO31010, nos parecem mais recomendadas.

## REFERÊNCIAS

- [1] International Standard, “Risk Management - Principles and Guidelines,” *ISO31000*, Novembro. 2009.
- [2] Project Management Institute, Inc, “Guia do Conjunto de Conhecimentos em gerenciamento de Proje-

tos PMBOK,” in *Quarta Edição*, For Campus Boulevard, Newton Square, PA 19073-3299, 2004.

- [3] Project Management Institute, Inc, “PRACTICE STANDARD FOR PROJECT RISK MANAGEMENT,” in *Quarta Edição*, For Campus Boulevard, Newton Square, PA 19073-3299, 2004.
- [4] International Standard, “Risk assessment techniques,” *ISO31010*, Novembro. 2009.