Apoio à Administração Pública no Brasil

Ministério do Planejamento, Orçamento e Gestão

Secretaria de Gestão Pública

Departamento de Inovação e Melhoria da Gestão

Gerência do Programa GesPública

PROJETO DE DESENVOLVIMENTO DO GUIA DE ORIENTAÇÃO PARA O GERENCIAMENTO DE RISCOS

PRODUTO VII

GUIA DE ORIENTAÇÃO PARA O GERENCIAMENTO DE RISCOS

VERSÃO 1.0 FINAL

Brasília, 01 de Março de 2013

Consultoria Contratada: SEDNA PARTNERS

VERSÃO 1.0 – FINAL

Guia de Orientação para o Gerenciamento de Riscos

Versão V1.0 FINAL

01 de Março de 2013

Embaixada Britânica Brasília
IFCI Instituto para o Fortalecimento das Capacidades Institucionais
SEGEP Secretaria de Gestão Pública
Ministério do Planejamento
Governo Federal Brasil País rico é país sem pobreza

HISTÓRICO DE VERSÕES

Versão	Autor	Data	Comentários
V1.0	Pedro C Ribeiro/Geraldo L. Marques	01/03/2013	Versão final

HISTÓRICO DE DISTRIBUIÇÃO

Versão	Distribuído por:	Data	Lista de Distribuição	Ação requerida
V1.0 Final	Pedro C. Ribeiro/ Geraldo L. Marques	01.03.2013	Bruno Palvarini Francisco J.Pompeu Campos	Aprovação

ÍNDICE

1.0 Histórico do GesPública

HÁ 21 ANOS A ADMINISTRAÇÃO PÚBLICA INVESTE NO FOMENTO DA SUA GESTÃO

O investimento sistemático em métodos e instrumentos que promovessem a maior qualidade dos processos e atividades no âmbito da gestão pública tem como marco significativo a criação do Programa Brasileiro da Qualidade e Produtividade - PBQP, por meio do Decreto nº 99.675, de 07 de novembro de 1990, que contemplou um subcomitê setorial para promover a implementação de programas de qualidade e produtividade na administração pública federal. O PBQP foi uma estratégia adotada pelo Governo Federal para estimular novas técnicas de produção, gestão e mudanças organizacionais no setor empresarial brasileiro e, assim, dar, às empresas, condições de concorrência, em um cenário de abertura dos mercados nacionais que havia sido promovida pelo Governo Collor.

O Subcomitê Setorial da Administração Publica foi coordenado pela extinta Secretaria de Administração Federal da Presidência da República e congregou representantes de todos os órgãos e entidades do Poder Executivo. Naquela época, houve o investimento na absorção dos conceitos e técnicas da Gestão pela Qualidade Total (Total Quality Management – TQM), com realização de diversas missões ao exterior para a internalização dos conceitos de Deming e outros especialistas na área, especialmente ao Japão e aos Estados Unidos da América.

Em 1995, por força do Decreto s/nº, de 9 de novembro de 1995, o PBQP foi reformulado e o Subcomitê Setorial da Administração Pública transformado em Programa da Qualidade e Participação1 na Administração Pública - QPAP. Coube à Câmara de Reforma do Estado do Conselho de Governo a responsabilidade pela formulação de suas diretrizes e o então recém-criado e já extinto Ministério da Administração Federal e Reforma do Estado - MARE ficou responsável pela implementação das ações do Programa (conforme art. 5º do Decreto).

O QPAP2 foi criado no escopo do Plano Diretor da Reforma do Aparelho do Estado, elaborado pelo MARE, como estratégia de promoção da modernização da gestão pública, com o objetivo de introduzir novos conceitos e técnicas de gestão pública, baseados no desempenho, na redução ao mínimo dos erros, e na participação dos servidores na definição dos processos de trabalho. Com a reformulação do Programa, sua abordagem, antes centrada na promoção das metodologias de TQM, evoluiu para a promoção da qualidade no sistema de gestão institucional, a partir da adoção dos

[1] O art. 5º do Decreto denomina o Programa como de Qualidade e Produtividade, mas o nome, efetivamente, utilizado foi Programa da Qualidade e Participação na Administração Pública – QPAP, conforme consta do Plano Diretor da Reforma do Estado.

[2] O QPAP foi elaborado pelo Ministério da Administração Federal e da Reforma do Estado e, depois de ampla discussão, aprovado pela Câmara da Reforma do Estado em sua reunião de 21 de setembro de 1995.

critérios de excelência da gestão pública, preconizados pela Fundação Nacional da Qualidade - FNQ3, com adaptações para aplicação na realidade pública.

Em 1997, o QPAP lançou o primeiro instrumento de avaliação da gestão pública, elaborado a partir dos critérios do PNQ, que serviu de base para o Prêmio de Qualidade do Governo Federal - PQGF, lançado em 1998 e hoje denominado Prêmio Nacional da Gestão Pública.

Após essa data, o instrumento sofreu diversas alterações e foi utilizado na efetivação de 12 ciclos anuais até o ano de 2010. Nesses doze anos, 685 órgãos e entidades públicas participaram dos ciclos de premiação, sendo que, delas, 132 foram reconhecidas ou premiadas pela qualidade e excelência dos seus métodos de gestão.

Em 2005, o QPAP foi reestruturado com o objetivo de ampliar sua abrangência de atuação; fortalecer a seu potencial de mobilização intra e extra governo e refinar suas metodologias e ferramentas. O Decreto nº 5.378, de 23 de fevereiro de 2005, criou o Programa Nacional de Gestão Pública e Desburocratização – Gespública, resultado da fusão do QPAP com o Programa Nacional de Desburocratização. Sua finalidade consiste em melhorar a qualidade dos serviços públicos prestados aos cidadãos e para o aumento da competitividade do país. .

Nessa fase, o Gespública constituiu e fortaleceu a Rede Nacional de Gestão Pública (RNGP), arranjo composto por órgãos, entidades, servidores públicos e integrantes da sociedade civil, que, nem janeiro de 2012, totalizou 1868 organizações e 1538 voluntários participantes. A Rede oferece cursos de capacitação em gestão, especialmente nos instrumentos que compõem o Programa.

O Gespública é um programa de melhoria e inovação administrativa, tendo desenvolvido e aperfeiçoado diversas tecnologias de gestão, adaptadas ao contexto e à identidade dos órgãos e entidades públicos, que são disponibilizadas à sua rede de participantes, tais como Carta de Serviços4, Gestão de Processos5, Instrumento Padrão de Pesquisa de Satisfação - IPPS6 e Indicadores de Desempenho7.

Embora com nomes diferentes e com redirecionamentos, o Gespública, em seus 21 anos de existência, consolida-se como um programa estratégico, capaz de gerar valor público para a Administração e para a Sociedade, por meio da promoção e da articulação do

---

3 Naquela época a FNQ denominava-se Fundação para o Prêmio Nacional da Qualidade – FPNQ.

4 Documento que estabelece o compromisso dos órgãos e entidades públicos de observar padrões de qualidade, eficiência e eficácia na execução de suas atividades, perante os seus públicos alvos e à sociedade em geral.

5 Instrumento para identificar, desenhar, executar, documentar, medir, monitorar, controlar e melhorar processos de trabalho voltados para a geração de valor público.

6 Metodologia de pesquisa de opinião padronizada que investiga o nível de satisfação dos usuários de um serviço público, desenvolvida para se adequar a qualquer organização pública prestadora de serviços diretos ao cidadão.

7 Referencial metodológico que permite às organizações públicas definirem e mensurarem seu desempenho, assumindo-se este como um decisivo passo para a gestão do desempenho, possibilitando sua pactuação, avaliação e divulgação em momentos posteriores.

conhecimento em gestão e do incentivo ao investimento contínuo na capacidade de governança das organizações e na entrega de serviços de qualidade aos cidadãos e ao mercado.

2.0 Introdução ao Guia

Os níveis de riscos, em todas as categorias - ambientais, sociais, econômicos, geopolíticos e tecnológicos, vêm aumentando globalmente.

Esta nova realidade vem exigindo cada vez mais das organizações a capacidade de lidar com altos graus de riscos em seus Planos Estratégicos, Programas, Projetos e Processos Finalísticos, tanto no setor público quanto no setor privado.

Diante desta realidade é fundamental a utilização de processos eficazes para o gerenciamento de riscos que permitam seu tratamento e a prevenção de crises.

Este Guia de Orientação para Gerenciamento de Riscos (Guia) tem como objetivos principais apoiar o Modelo de Excelência do Sistema de Gestão Pública no que tange ao tema de gerenciamento de riscos e prover uma introdução ao tema gerenciamento de riscos.

A estrutura do Guia baseou-se no documento “The Orange Book Management of Risk - Principles and Concepts“ (Gerenciamento de Riscos – Princípios e Conceitos) produzido e publicado pelo HM Treasury do Governo Britânico (Orange Book). O Orange Book foi amplamente utilizado como a principal referência do Programa de Gerenciamento de Riscos do Governo do Reino Unido, iniciado em 2001.

Os conceitos e princípios contidos neste Guia foram extraídos diretamente do Orange Book, a partir de trabalho desenvolvido pela Secretaria de Gestão Pública (SEGEP) do Ministério do Planejamento, Orçamento e Gestão em cooperação com o Ministério das Relações Exteriores do Reino Unido.

O Orange Book tem como vantagens, além de ser compatível com padrões internacionais de gerenciamento de riscos, apresentar uma introdução ao tema gerenciamento de riscos, tratando de uma forma abrangente e simples, um tema complexo como o gerenciamento de riscos nas organizações.

Isto é essencial na introdução de um processo de gerenciamento de riscos em uma organização, uma vez que, dentro de qualquer organização existem diversos níveis de maturidade com relação ao gerenciamento de riscos.

3.0 A importância do Gerenciamento de Riscos

Organizações existem para atingir propósitos que resultam em entregas de serviços ou produtos. Qualquer que seja este propósito, esta entrega de serviços e o atingimento dos seus objetivos estão cercados por incertezas que podem gerar ameaças ao sucesso ou oportunidade de melhoria, e devem ser gerenciadas de forma estruturada.

Riscos, quando não gerenciados adequadamente, ameaçam o atingimento dos objetivos, o cumprimento dos prazos, o controle dos custos e da qualidade de um programa, projeto ou entrega de serviços aos cidadãos.

Assim sendo, o gerenciamento de riscos é fundamental para o sucesso no cumprimento da missão da organização pública em entregar serviços de qualidade para o cidadão.

O gerenciamento de riscos pode ajudar as organizações a melhorar a eficiência, eficácia e efetividade de diversas formas, como por exemplo:

- melhoria na entrega de serviços ao cidadão;
- melhor utilização de recursos;
- melhor planejamento e melhor gerenciamento de programas e projetos.

Tanto cidadãos quanto a sociedade perdem tempo e dinheiro, se programas de governo e serviços públicos associados não são entregues de forma adequada e em tempo hábil.

O bom gerenciamento de riscos contribui também para aumentar a confiança do cidadão: (a) na capacidade do Governo de entregar os serviços prometidos; (b) no sistema de governança; e (c) na utilização adequada dos recursos públicos.

A reputação das organizações governamentais nas diversas esferas sofre quando seus programas, projetos e serviços não atendem às expectativas de seus públicos alvos.

Um relatório do “Cabinet Office” do Governo do Reino Unido exemplifica esta preocupação por ocasião da criação do Programa de Gerenciamento de Riscos do Governo Britânico, quando determina que os objetivos do programa devem gerar:

- menos surpresas para os cidadãos e para o próprio Governo;
- menor custo resultante de falhas em antecipar riscos;
- melhor clareza de responsabilidades pelo gerenciamento dos riscos no Governo.

Em resumo, um bom gerenciamento de riscos resulta em:

- melhor chance de entrega de serviços no prazo, no custo e na qualidade esperada;
- redução de surpresas, crises e “apagar incêndios”;
- aumento de chances de sucesso de Programas e Projetos governamentais;
- maior transparência.

4.0 Objetivos do Guia

O Guia tem como objetivos apoiar o Modelo de Excelência do Sistema de Gestão Pública no que tange ao gerenciamento de riscos e prover uma introdução ao tema gerenciamento de riscos no setor público, abordando os pontos essenciais e as etapas que devem ser levadas em consideração no gerenciamento de riscos.

Este Guia não é uma norma ou manual detalhado de como gerenciar riscos em um órgão/entidade específica de governo.

Este Guia não é um padrão, norma ou manual detalhado de como gerenciar os riscos em uma unidade específica do governo. O seu objetivo é simplesmente elencar os fundamentos e as etapas que devem ser levadas em consideração para o gerenciamento de riscos, assim como prover um direcionamento que auxilie os membros da Rede GesPública a identificar e abordar este tema nas situações específicas da sua organização quando da utilização do Modelo de Excelência do Sistema de Gestão Pública.

Cada organização deve utilizar os seus padrões específicos, normas ou procedimentos e técnicas – opcionais ou mandatórias ao seu tipo de atividade - que tratem em detalhe os elementos constantes neste Guia.

Podemos citar como exemplos, normas relativas à segurança ocupacional, riscos ambientais, resoluções que dispõem sobre o gerenciamento do risco de crédito e seguros, e normas internacionais como a ISO 31000, ISO 9001, OHSAS 18.0001 e ISO 14000.

Além da conformidade com os padrões específicos, é importante a organização adotar um processo estruturado de gerenciamento de riscos e demonstrar que os riscos estão sendo gerenciados pela organização de modo a apoiar a entrega dos seus objetivos.

As orientações contidas neste Guia devem ser adaptadas à realidade de cada organização. Conforme indicado no item 9.0 Contexto do Gerenciamento de Riscos, as organizações devem possuir ou desenvolver uma estrutura mínima de governança que apoie seu processo de gerenciamento de riscos.

O Guia foi desenvolvido com base no “Orange Book”, sendo compatível com as práticas de gerenciamento de riscos elencadas na maioria das normas e padrões internacionais.

5.0 Públicos Alvos

Este Guia tem os seguintes públicos alvos:

1 Aqueles que participam da Rede GesPública ou estejam adotando o Modelo de Excelência;

2 Aqueles iniciantes em gerenciamento de riscos que podem utilizá-lo como um documento introdutório;

3 Aqueles que estejam envolvidos na avaliação de riscos de seus programas, projetos, processos finalísticos, auditoria interna de riscos, participando em comitês ou em reuniões para revisão e avaliação de riscos e que necessitem de um documento que contenha os elementos essenciais geralmente abordados no gerenciamento de riscos;

4 As lideranças das organizações que podem utilizá-lo como apoio para introduzir, de uma forma simples e eficaz, o gerenciamento de riscos na sua organização.

Este Guia pode ser utilizado das seguintes formas:

1 Como apoio ao entendimento da terminologia, papéis e responsabilidades referentes a riscos contidos no Modelo de Excelência do Sistema de Gestão Pública;

2 Em conjunto com padrões, normas ou procedimentos específicos que ofereçam maior detalhamento sobre os princípios e conceitos contidos neste Guia.

Este Guia não substitui Normas Regulamentadoras, Decretos, Resoluções, Procedimentos, Políticas, Instruções ou Leis específicas relativas ao gerenciamento de riscos em vigor ou em processo de introdução.

6.0 Definição de Risco

Podemos considerar riscos como eventos ou condições incertas, que caso ocorram, podem gerar impactos negativos (ameaças) ou positivos (oportunidades) nos objetivos (por exemplo: objetivos de prazo, custo, qualidade, escopo e imagem) de programas, projetos ou serviços a serem entregues à sociedade.

Alinhado com esta definição, a ISO 31000 define risco como sendo “o efeito da incerteza nos objetivos” (Norma ABNT ISO 31000:2009).

Um risco pode ser expresso pela combinação percebida da sua probabilidade de ocorrência e do(s) impacto(s) resultante(s) da(s) ameaça(s) ou oportunidade(s).

Toda atividade humana inclui riscos. Sendo assim, toda organização tem que gerenciar os riscos de modo a contê-los em níveis aceitáveis pela organização.

O gerenciamento de riscos consiste na aplicação de princípios e processos para identificação e avaliação de riscos ao planejamento, à implementação e ao controle das respostas aos riscos. Caso os riscos não sejam adequadamente gerenciados, a organização acaba tomando riscos que não foram analisados adequadamente e, portanto, desconhece.

Como indicado no item 8.0 – Contexto do Gerenciamento de Riscos, o gerenciamento de riscos deve adotar uma abordagem que contenha os seguintes elementos:

1. Alinhamento com o Sistema de Governança da Organização;
2. Definição de processo, métodos e técnicas a serem utilizados;
3. Papéis e responsabilidades;
4. Formulários e modelos a serem utilizados;
5. Definição de níveis de tolerância, alçada e de aprovação de riscos;
6. Recursos a serem utilizados no gerenciamento de riscos.

7.0 A Hierarquia de Riscos

Riscos devem ser gerenciados em três níveis: estratégico, de programas e de projetos e atividades (ver Fig. 1). A organização deve ser capaz de gerenciar riscos nos três níveis.

Nível Estratégico

É neste nível onde se dá o contrato político do Governo com a sociedade e é estabelecida a coerência do seu programa de Governo. Decisões neste nível envolvem a formulação dos objetivos estratégicos e as prioridades para a alocação de recursos públicos em alinhamento com as políticas públicas.

Nível Programa

Neste nível encontram-se as decisões de implementação e gerenciamento de programas temáticos previstos no nível estratégico, através dos quais são executadas as politicas e as ações prioritárias de Governo.

Nível Projetos e Atividades

Neste nível encontram-se os projetos que contribuirão para o atingimento dos objetivos dos Programas, e as atividades relativas aos processos finalísticos.

As lideranças em todos os níveis da organização devem estar conscientes, capacitadas e motivadas com relação à relevância do gerenciamento de riscos nos três níveis, que são interdependentes.

Fig. 1 Hierarquia de Riscos: Adaptado de The Orange Book – HM Treasury, 2004

O direcionamento para o gerenciamento de riscos é dado pelo topo da organização, mas deve ser gerenciado nos três níveis de forma integrada. O gerenciamento de riscos deve ser incorporado aos processos, atividades e rotinas das organizações governamentais.

A organização como um todo precisa ter meios de assegurar que o gerenciamento de riscos esteja acontecendo de forma apropriada em cada nível, de acordo com os planos de gerenciamento de riscos definidos para as mesmas. A gerência, em cada nível, precisa ser capacitada com as competências necessárias e processos definidos para o gerenciamento de riscos em alinhamento com o Guia.

8.0 O Contexto do Gerenciamento de Riscos

O gerenciamento de riscos não ocorre no vácuo. Toda organização encontra-se em um ambiente que determina a natureza e o contexto dos riscos a serem gerenciados.

8.1 O Contexto Interno

O gerenciamento de riscos precisa levar em consideração a organização na qual está inserido, incluindo o sistema de governança, políticas, objetivos, estrutura organizacional, recursos (humanos, materiais e financeiros), conhecimento, sistemas de informação, processo decisório, valores, partes interessadas, cultura organizacional, normas, modelos e diretrizes da organização.

Deve haver uma total aderência entre o processo de gerenciamento de riscos e o sistema de governança da organização.

O Modelo de Excelência define que o “Sistema de Governança aborda as práticas de gestão adotadas pela alta direção no cumprimento da finalidade do órgão/entidade, de forma a gerar valor para a sociedade, observando os valores e fundamentos da administração pública, especialmente os princípios da supremacia do interesse público, da articulação federativa e descentralização das políticas públicas, da participação e controle social”.

Não existe uma maneira única de implementar um processo de gerenciamento de riscos. Os elementos abaixo estão entre os que devem ser definidos:

- política de gerenciamento de riscos ou alinhamento com uma política existente;
- processo específico para o gerenciamento de riscos alinhado com o sistema de governança;
- níveis de tolerância a riscos;
- papéis e responsabilidades e níveis de autoridade e de aprovação dentro do processo de gerenciamento de riscos;
- estrutura organizacional e recursos dedicados ao gerenciamento de riscos;
- documentos e relatórios a serem produzidos, distribuídos, utilizados, mantidos e armazenados;
- normas regulamentadoras, decretos, resoluções, procedimentos, politicas, instruções ou leis específicas em vigor ou em processo de introdução relacionadas a riscos a serem utilizadas;
- ciclos de revisão, auditorias e aprovação;
- fóruns de decisão e alçadas sobre riscos;
- sistemas de suporte necessários;
- plano de capacitação das pessoas; e
- procedimentos e critérios de avaliação e melhoria contínua do processo de gerenciamento de riscos.

8.2 O Contexto Externo

O contexto externo é o ambiente no qual a organização busca atingir seus objetivos. Inclui desde interdependências com outras organizações, dentro ou fora do governo, que formam sua cadeia de valor (Organização Estendida), assim como o macro ambiente externo que inclui economia, política, legislação, tanto nacional quanto internacional.

8.2.1 A Organização Estendida

Nenhuma organização opera de forma independente, mas tem inúmeras interdependências com outras organizações, dentro ou fora do governo. Estas organizações compõem o que chamamos de “organização estendida” e as suas interdependências impactam o gerenciamento de riscos através da geração de riscos de interdependência que devem ser gerenciados.

O impacto recíproco da ação de uma organização nas demais organizações deve ser sempre avaliado. Por exemplo, se um órgão do governo responsável por prover serviços de apoio de Tecnologia da Informação tem incertezas sobre cortes em seu orçamento, esta situação gera um risco para outros órgãos do governo que planejam utilizar tais serviços para atingir os objetivos de seus programas, projetos ou processos finalísticos.

As organizações governamentais têm interdependências com outras organizações sobre as quais não possui controle direto. Assim sendo, a entrega de seus programas, projetos, processos e serviços dependem de outras organizações ou impactam as entregas e o atingimento de metas de outras organizações.

Vários órgãos do Governo têm relacionamentos cruzados dentro da estrutura do Estado. Por isso é essencial o alinhamento entre estas organizações com o objetivo de facilitar uma abordagem de gerenciamento de riscos que permita às partes atingir e/ou ajustarem os seus objetivos. Organizações têm também interdependências com fornecedores, financiadores de projetos e terceiros de maneira geral, inclusive para entrega de serviços, integrantes da cadeia de valor do setor público.

Por exemplo, Governos utilizam contratos de terceirização de serviços com empresas privadas para atendimento aos cidadãos em diversas áreas.

Qualquer que seja a natureza das relações de riscos entre as organizações participantes desta cadeia de valor de serviços governamentais, há necessidade de se assegurar que o risco está sendo gerenciado em todos os níveis (integração vertical) e em toda a cadeia de valor (integração horizontal).

8.2.2 O Macro Ambiente

Além das fronteiras da organização estendida – cadeia de valor – existem outros fatores que contribuem para formar o ambiente e gerar cenários nos quais os riscos devem ser gerenciados.

Estes fatores geralmente classificados como “riscos externos” podem gerar riscos que não são diretamente controlados, ou podem restringir a forma como tomamos ou tratamos os riscos. Os mesmos estão associados ao ambiente político, econômico, social, tecnológico e ambiental no nível internacional, nacional, regional ou local no qual a organização está inserida.

Fazem parte deste ambiente, a legislação nacional e internacional, organismos reguladores tais como a ANAC e ANATEL, o Congresso Nacional (Senado e Câmara dos Deputados), Assembleias Legislativas na esfera Estadual e Câmaras de Vereadores na esfera Municipal), a economia nacional e internacional, órgãos de auditoria e controle externo, a sociedade civil (cidadãos, empresas, mídia, organizações não governamentais), o Ministério Público e os demais agentes econômicos e políticos do país.

Um aspecto particular do macro ambiente de riscos nas organizações governamentais é a própria estrutura organizacional do governo. Em princípio, as organizações do governo existem para entregar as politicas e metas definidas pelo governo. Assim sendo, para o sucesso de um processo de gerenciamento de riscos, é muito importante que as decisões de prioridades e politicas de governo, estejam alinhadas e levem em consideração boas práticas de gerenciamento de riscos.

Em particular, a legislação, aí incluídas as normas e os regulamentos, tem impacto no contexto e consequentemente nos riscos. É importante para uma organização identificar quais são as exigências da legislação, como por exemplo, legislação ambiental, para que sejam devidamente levadas em consideração no gerenciamento de riscos pois preveem prazos para obtenção da licença ambiental.

Um aspecto importante com relação a riscos do macro ambiente é que uma organização não pode ter controle total sobre riscos associados a eventos - como uma catástrofe natural – que impactam a entrega dos seus serviços. No entanto, a organização sempre pode desenvolver planos de contingência para assegurar da melhor maneira possível a entrega destes serviços, caso o evento ocorra.

9.0 O Modelo de Gerenciamento de Riscos

O modelo adotado neste Guia é baseado no Modelo de Gerenciamento de Riscos “Risk Management Model” contido no “Orange Book” do Governo Britânico.

Este modelo permite visualizar, de uma forma simplificada, o gerenciamento de riscos como um conjunto de elementos inter-relacionados que precisam ser considerados para que o gerenciamento de riscos aconteça de forma adequada.

O modelo é composto de quatro elementos, conforme a figura 2 abaixo:

9.1 Processo de Gerenciamento de Riscos: O processo de gerenciamento de riscos consiste no conjunto de atividades inter-relacionadas, necessárias para o gerenciamento de riscos. O gerenciamento de riscos consiste na aplicação de princípios e processos para identificação e avaliação de riscos, planejamento, implementação e controle das respostas aos riscos.

O processo de gerenciamento de riscos está inserido e precisa levar em consideração a organização na qual faz parte, incluindo: governança, politicas, objetivos, estrutura organizacional, recursos (humanos, materiais e financeiros), conhecimento, sistemas de informação e processo decisório, valores, partes interessadas, cultura organizacional, normas, modelos e diretrizes da organização.

Estabelecimento do Contexto do Gerenciamento de Riscos:
Sendo parte integrante dos processos da organização, é importante que o processo de gerenciamento de riscos envolva a definição dos seguintes elementos:

- especificação do processo de gerenciamento de riscos a ser adotado;
- alinhamento do processo com o Sistema de Governança da Organização;
- identificação das partes interessadas;
- comunicação às partes interessadas sobre o processo de gerenciamento de riscos adotado;
- definição de papéis e responsabilidades pelo gerenciamento de riscos;
- definição de metodologias e normas específicas a serem utilizadas;
- relatórios, modelos e formulários a serem utilizados;
- ciclos de avaliação e revisão;
- plano de comunicação de riscos entre níveis hierárquicos (vide item 7.0 Hierarquia de Riscos);
- categorias de riscos a serem utilizadas;
- níveis de riscos considerados inaceitáveis;
- alinhamento com outros processos gerenciais e sistemas de gestão existentes; e
- demais elementos considerados no item 8.1 Contexto Interno.

9.2 - Organização Estendida: Nenhuma organização opera de forma independente – ela tem inúmeras interdependências com outras organizações dentro e fora do âmbito do governo que devem ser levados em consideração (ver 8.2.1 Organização Estendida)

9.3- O Macro Ambiente de Riscos: Além das fronteiras da organização estendida existem outros fatores que contribuem para formar o ambiente (ou cenários) nos quais os riscos devem ser gerenciados. Estes fatores podem gerar riscos que não são diretamente controlados ou podem restringir a forma como podemos tomar ou tratar riscos. Estão relacionados ao ambiente social, político, técnico, tecnológico, econômico e ambiental no nível internacional, nacional, regional ou local no qual a organização está inserida. (ver 8.2.2 Macro Ambiente)

9.4- Comunicação e Aprendizado Contínuo

Consiste no processo que uma organização executa para fornecer, obter e compartilhar informações necessárias para dialogar com as partes interessadas e aprender com o gerenciamento de riscos (ver item 11.0 Comunicação e Aprendizado).

A comunicação não é um estágio separado do gerenciamento de riscos, mas permeia todo o processo de gerenciamento de riscos. Um processo de gerenciamento de riscos depende de participação e a participação depende de comunicação.

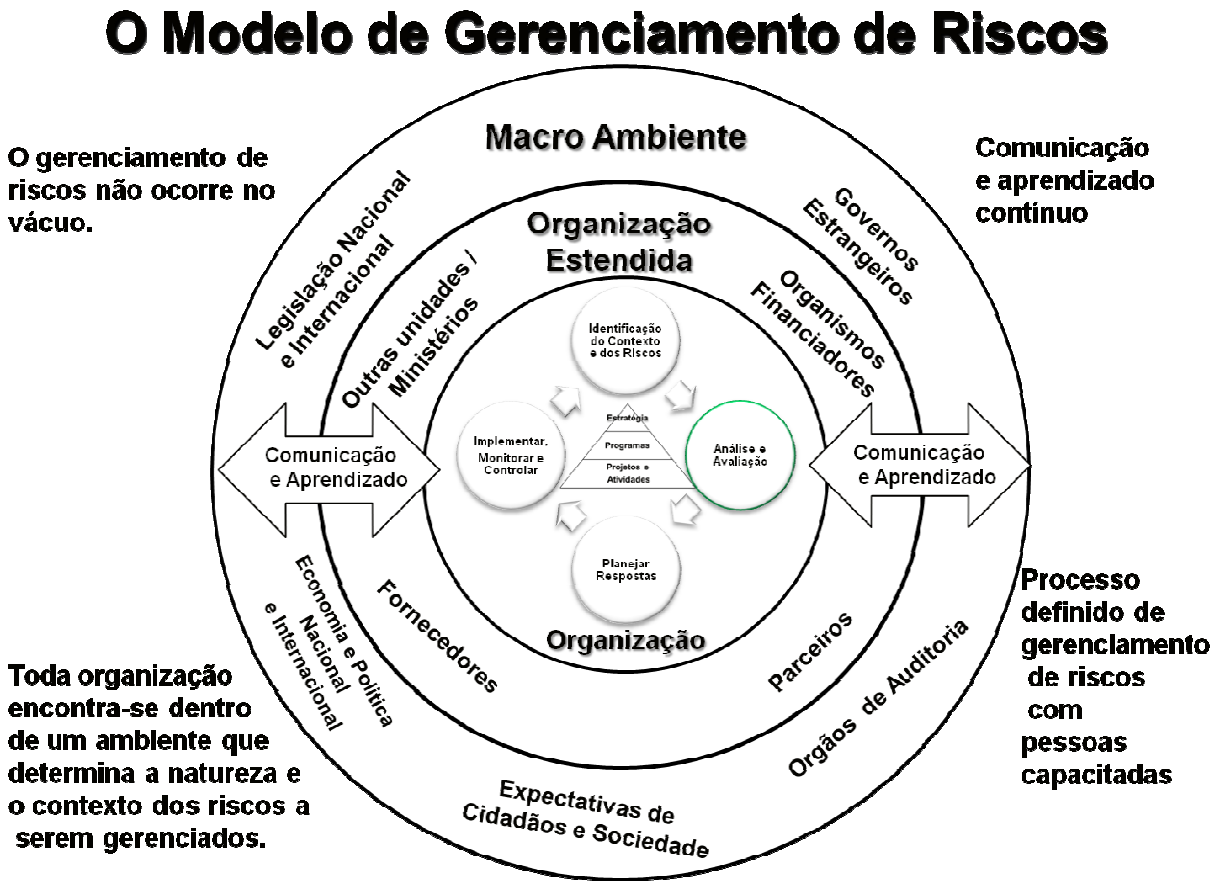


Fig. 2 Modelo de Gerenciamento de Riscos; Adaptado do Risk Management Model do Orange Book. do HM Treasury do Reino Unido

10.0 O Processo de Gerenciamento de Riscos

O processo de gerenciamento de riscos consiste no conjunto de etapas e atividades relacionadas, necessárias para realizar o gerenciamento de riscos.

O processo gerenciamento de riscos é composto de quatro etapas:

1 - Identificação de Riscos;

2 - Análise e Avaliação de Riscos;

3 – Planejamento das Respostas aos Riscos;

4 - Implementação, Monitoramento e Controle de Riscos.

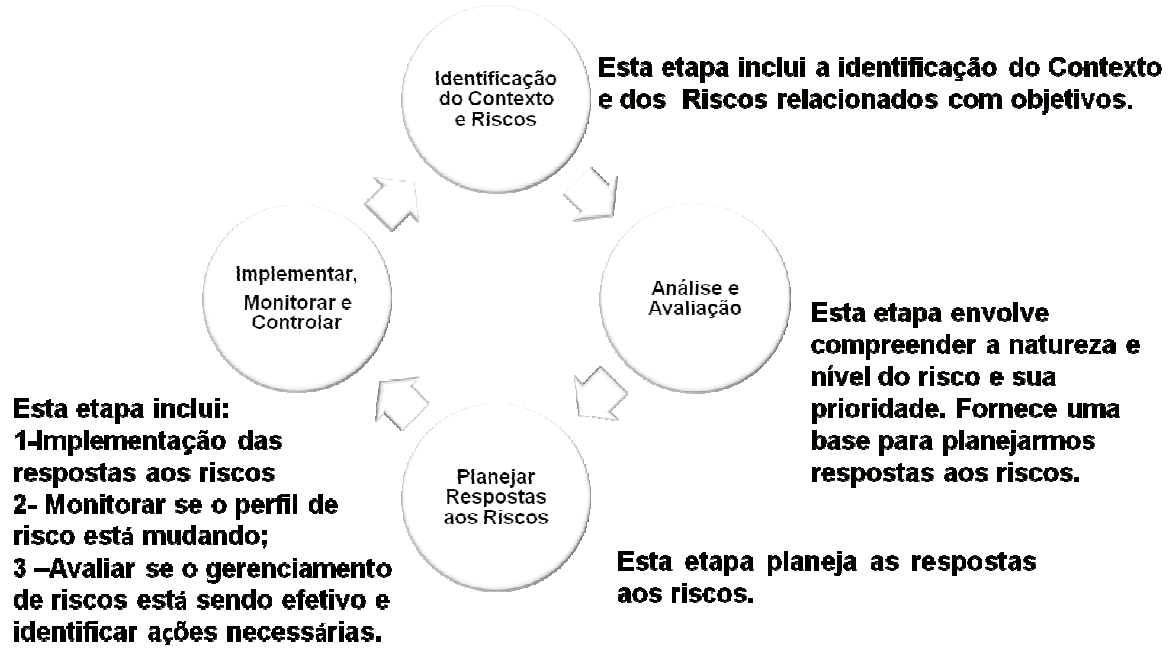
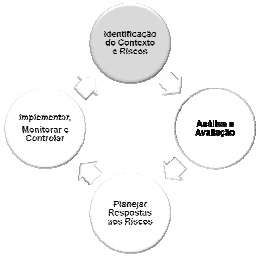


Fig. 3 Processo de Gerenciamento de Riscos; Adaptado do Risk Management Model do Orange Book.

10.1 IDENTIFICAÇÃO DE RISCOS



Para que riscos possam ser gerenciados, a organização precisa em primeiro lugar identificá-los e documentá-los.

A identificação trata da definição dos eventos de riscos que podem afetar o programa, projeto ou processo finalístico e a documentação de suas características.

A identificação de riscos possui dois componentes, a saber:

10.1.1. Componentes da Identificação de Riscos

10.1.1.1. Identificação do Contexto de Riscos

A Identificação do Contexto de Riscos tem como resultado (a) o alinhamento do processo a ser adotado com os elementos descritos no item 9.1; (b) a definição da estratégia de gerenciamento de riscos específica para os programas, projetos ou processos finalísticos, que incluirá elementos tais como**:**

- Definição da equipe responsável pelo gerenciamento de riscos;
- Definição de papéis e responsabilidades pelo gerenciamento de riscos;
- Definição de partes interessadas envolvidas e plano de comunicação;
- Definição de metodologias e normas específicas a serem utilizadas;
- Relatórios, modelos e formulários a serem utilizados;
- Ciclo de acompanhamento e revisão para o programa, projetos ou atividades especificas;
- Definição de ferramentas (ex: matriz probabilidade e impacto) a serem utilizadas;
- Plano de Comunicação e alinhamento entre níveis hierárquicos;
- Categorias de riscos a serem utilizadas (ver item 10.1.2);
- Níveis de riscos considerados inaceitáveis para o programa, projeto ou processo específico;
- Alinhamento com outros processos gerenciais e os sistemas de gestão existentes.

10.1.1.2 Identificação de Riscos:

A identificação de riscos não é um evento pontual. Ela deve ocorrer ao longo da vida do programa, projeto ou processo finalístico de duas formas:

> **Identificação inicial de Riscos:** Quando é efetuada pela primeira vez, ocorre para uma organização que ainda não tenha identificado os riscos de uma forma estruturada ou relativa a um novo projeto ou processo;
>
> **Identificação contínua de Riscos:** Necessária para a identificação de novos riscos ou riscos que não são mais relevantes para a organização. A identificação contínua de riscos deve ser uma rotina do gerenciamento de riscos da organização.

O Gerenciamento de Riscos está relacionado aos objetivos da organização.

Um princípio importante do gerenciamento de riscos é que a identificação de riscos deve estar relacionada continuamente com objetivos. Riscos só podem ser identificados e priorizados com relação a estes objetivos. Assim sendo, uma declaração de riscos deve incluir: evento de risco, causa(s) e impacto(s) no(s) objetivo(s).

EXEMPLO:

Objetivo: Você (Departamento Z) é responsável por entregar um determinado serviço ou projeto na data Y (objetivo de prazo) que depende de informações ou materiais a serem fornecidos pelo Departamento X.

Evento de Risco: Departamento X pode entregar ou não a tempo as informações necessárias para o seu projeto.

Causa do Risco: Devido a incertezas relacionadas à aprovação, o Departamento X pode não ter os recursos necessários, liberados a tempo para esta entrega.

Impacto do Risco: Atraso na entrega do seu serviço ou projeto na data Y.

10.1.2 Abordagens para Identificação

Duas abordagens que podem ser utilizadas são:

1. **Equipe de Identificação de Riscos:** uma equipe é designada pela administração como responsável pela identificação de riscos. Esta equipe conduz uma série de entrevistas e oficinas para identificação de riscos;

2. **Auto avaliação:** nesta abordagem cada nível da organização é convocado a rever seus programas, projetos e processos finalísticos para identificar os riscos associados. Podem ser designadas áreas específicas para apoiar a etapa de identificação através de reuniões e oficinas estruturadas.

Um ponto forte desta segunda abordagem é que ajuda a desenvolver a responsabilidade das áreas em relação aos riscos.

Cabe salientar que estas abordagens não são mutuamente excludentes, e uma combinação de abordagens é sempre desejável.

Para que possamos gerenciar riscos, primeiro temos que identificá-los. A classificação dos riscos em categorias auxilia a organizar a etapa de identificação.

10.1.3 Categoria de Riscos

A classificação de riscos em categorias auxilia a etapa de identificação dos riscos e verificar se algum tipo de risco relevante não foi considerado, e também a garantir que sejam considerados tipos de riscos com que a organização pode se deparar. Não há uma classificação de riscos que seja consensual, exaustiva e aplicável a todas as organizações. A classificação deve ser desenvolvida de acordo com as características de cada organização, contemplando as particularidades do seu setor de atuação. Por exemplo: riscos relacionados a variações cambiais podem ser cruciais para uma determinada organização do setor financeiro e podem não ser tão relevantes para determinada organização que não possui atividades diretamente ligadas ao câmbio.

As tabelas a seguir, adaptadas do Orange Book, apresentam um sumário das categorias de riscos mais comuns. É importante salientar que cada organização deve considerar os riscos que são aplicáveis à sua realidade específica, e algumas organizações podem identificar outras categorias aplicáveis de acordo com a natureza da sua organização.

Em termos gerais podemos classificar com base na origem dos eventos (externos ou internos).

- **Riscos Externos:** são os riscos associados ao ambiente onde a organização opera. Em geral, a organização não tem controle direto sobre estes eventos, mas mesmo assim ações podem ser tomadas quando necessário. Por exemplo: Não podemos controlar a incidência de raios, mas podemos instalar para-raios.

- **Riscos Internos:** são os riscos associados à própria estrutura da organização, seus processos, governança, quadro de pessoal, recursos ou ambiente de tecnologia. A organização pode e deve agir diretamente de forma proativa.

Riscos Externos e Internos podem resultar em:

Falha na entrega de Programas e Projetos: Riscos que podem resultar em falha na entrega do programa ou projeto no escopo, prazo, custo e qualidade especificados;

Falha no produto/serviço: Riscos que podem resultar na falha na entrega do serviço para o usuário/cidadão nos termos e condições esperadas/contratadas.

RISCOS EXTERNOS

Políticos (Nacional e Internacional) ex.: mudança de governo; mudança no cenário político; decisões sobre políticas interministeriais; mudanças na máquina do governo; terrorismo etc.

Econômico/Financeiros (Nacional e Internacional) ex.: inflação; variação cambial afetando custos nas transações internacionais; taxa de juros; efeitos da economia global na economia brasileira; ações da concorrência internacional, etc.

Socioculturais ex**.: m**udanças demográficas afetando a demanda por serviços; mobilidade de classes sociais; mudança de expectativa dos cidadãos e da sociedade devido à globalização; conflitos sociais etc.

Tecnológicos ex.: tecnologias emergentes; Internet; obsolescência dos sistemas atuais; mudança na competitividade estrutural com base no uso de novas tecnologias; oportunidades advindas de avanços tecnológicos; etc.

Legal/Regulatório ex.: novas leis ou mudanças de marcos regulatórios em termos de qualidade, segurança, meio ambiente, saúde, trabalhista; etc.

Ambiental ex.: desastres naturais, ecológicos, climáticos (enchentes, deslizamentos, secas, etc...) etc.

RISCOS INTERNOS

Recursos Financeiros ex.: incerteza em relação às fontes de financiamento e orçamento.

Recursos Humanos ex.: relacionados à disponibilidade, contratação ou capacitação das equipes.

Processos Internos ex.: relacionados à falta de definição de processos críticos específicos assim como de papéis e responsabilidades, autoridade para aprovação.

Sistemas de Informação ex.: relacionados à adequação de sistemas de informação.

Parceiros/Fornecedores ex.: forma contratual e definição de papéis e responsabilidades, capacitação de fornecedores, processo de seleção.

Outros Riscos Outros riscos específicos da organização que não se enquadram nas categorias acima.

10.1.4 Ferramentas para a Identificação de Riscos

É importante utilizar ferramentas adequadas para coleta de dados e informações que possibilitem a identificação de riscos. Isto é definido como parte da estratégia de gerenciamento de riscos a ser adotada pela organização.

Dentre as ferramentas mais utilizadas, podemos incluir:

Brainstorming: Obtenção de uma lista dos riscos a partir de uma reunião com equipe multidisciplinar representando setores e competências diferentes da organização, com o apoio de um facilitador, com objetivo de identificar riscos .

Entrevistas: Entrevistar as partes interessadas e os especialistas com o objetivo de identificar riscos.

Análise de Listas de Verificação de Riscos: Verificar as listas de riscos previamente identificadas pela organização sobre processos ou programas similares. Utiliza lições aprendidas e informações já catalogadas pela organização.

Cada organização deve determinar quais ferramentas, opcionais ou mandatórias, são as mais adequadas à sua realidade. É importante salientar que as oportunidades geradas pela incerteza (riscos positivos) também devem ser identificadas.

Após o término da etapa de identificação, os riscos identificados devem ser atribuídos a uma pessoa ou entidade, designada “proprietária do risco”, que deve ser responsável por assegurar que os riscos sejam gerenciados e monitorados adequadamente e para isso deve ter a autoridade necessária e suficiente.

No Brasil a NORMA ABNT NBR ISO 31010:2012 descreve em detalhe os tipos de ferramentas e atributos para seleção de ferramentas mais adequadas.

10.1.5 Documentação da Etapa de Identificação de Riscos

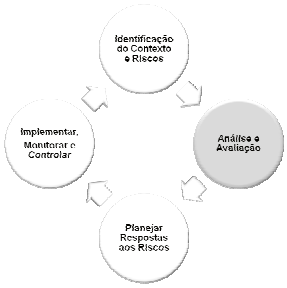
Os riscos identificados devem ser registrados em documento específico (Registro de Riscos) que poderá conter atributos como:

- Número de Identificação atribuído ao risco
- Categoria de Risco
- Data da Identificação
- Nome/Área/Contato de quem identificou o risco
- Descrição do Risco
- Evento de Risco
- Causa(s) do Risco
- Impacto(s) do Risco
- Proprietário do Risco

Os formulários específicos a serem utilizados, forma de arquivamento, aprovação e retenção, níveis de reporte e aprovação requeridos devem ser definidos pela estratégia de gerenciamento de riscos alinhada com o sistema de governança como indicado no item 10.1.1.

Após devidamente identificados e documentados, os riscos serão avaliados na etapa 10.2 ANÁLISE E AVALIAÇÃO DE RISCOS.

10.2 ANÁLISE E AVALIAÇÃO DE RISCOS



Uma vez identificados os riscos, é importante compreender e determinar o nível de cada risco.

O nível de um risco pode ser determinado pela combinação das suas consequências para a organização (impacto) e a chance de ocorrência (probabilidade).

A análise dos riscos possibilita a sua avaliação e fornece uma base para a etapa de planejamento de respostas aos riscos.

É importante assegurar a adoção de um método que considere tanto a probabilidade quanto o impacto de cada risco identificado.

Devemos também documentar a etapa de análise e avaliação dos riscos de forma que facilite a priorização dos mesmos.

Alguns riscos são mais fáceis de serem analisados e avaliados numericamente, particularmente riscos econômico-financeiros, mas outros riscos, por exemplo, riscos que podem ocasionar impactos de imagem, são mais subjetivos. Nesse caso, a análise e a avaliação de riscos passam a ser mais arte do que ciência.

A análise e avaliação de riscos, sempre que possível, devem ser baseadas em evidências objetivas, considerando as perspectivas das partes interessadas impactadas pelo risco, e fundamentadas em uma etapa de identificação bem realizada.

A análise do risco leva em consideração a probabilidade do risco específico ocorrer e o seu impacto sobre um ou mais objetivos do programa, projeto ou processo finalístico.

10.2.1 Ferramentas para a Análise e Avaliação de Riscos

Uma das ferramentas para análise e avaliação de riscos é a Matriz de Probabilidade e Impacto que pode ser utilizada para posicionar e avaliar as combinações de probabilidade e impacto. A utilização de uma escala alto/médio/baixo para probabilidade e impacto pode ser suficiente, o que resulta em uma matriz 3 x 3 conforme indicado na Figura 4 abaixo.

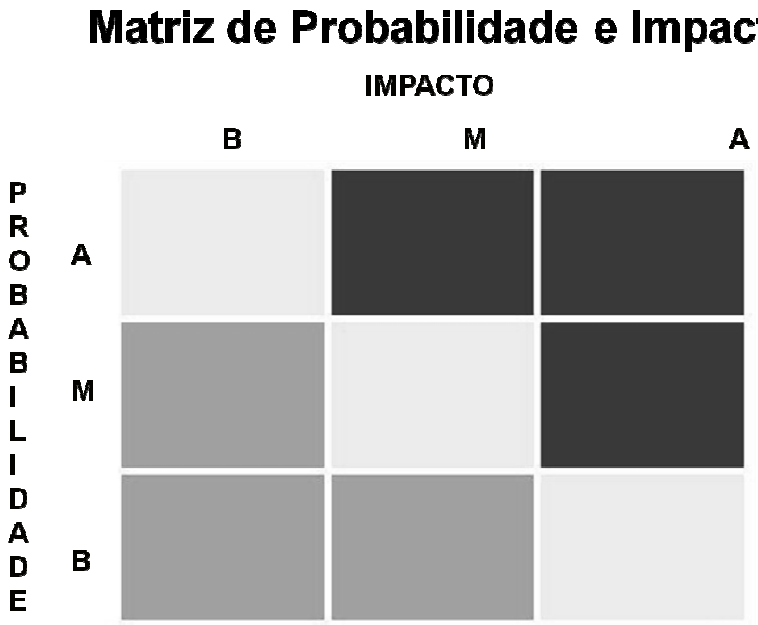


Fig. 4 Matriz de Probabilidade Impacto; Adaptado do Risk Management Model do Orange Book.

O que é considerado impacto “alto/médio/baixo” varia de acordo com o programa, projeto ou processo específico sendo avaliado conforme definido no item 10.1.1. Os riscos identificados na etapa anterior de Identificação de Riscos podem ser então posicionados na matriz de acordo com a avaliação realizada de probabilidade de ocorrência e impacto.

Por exemplo, se tivermos três riscos identificados (riscos (1) (2) e (3)) e avaliados em termos de probabilidade e impacto, poderíamos posicioná-los na matriz e obter um sumário do Perfil de Riscos como indicado na Fig. 5. Escalas mais detalhadas podem ser consideradas apropriadas ou serem requeridas por norma ou regulamentação específica. Não existe um padrão absoluto para a escala da matriz de probabilidade e impacto. A organização deve chegar a um consenso sobre o nível de análise que ela considera adequado para as suas circunstâncias específicas. Esta decisão é tomada durante a etapa de Identificação de Contexto item 10.1.1.

Os riscos podem diferir também em nível de urgência. Isto irá variar com relação ao tempo de antecedência com que precisam ser tratados e também ao tempo necessário para respostas. Dois riscos de mesma probabilidade e impacto podem ter níveis de urgência de tratamento diferentes. Uma escala complementar para o nível de urgência pode ser criada para auxiliar a análise levando este fato em consideração.

A Matriz de Probabilidade e Impacto também pode ser utilizada para demonstrar visualmente os níveis de tolerância da organização a riscos, utilizando para isto o conceito de apetite de risco descrito a seguir.

10.2.2 Apetite de Riscos

Apetite de riscos é a quantidade de risco julgada aceitável pela organização. Representa o montante de riscos que uma organização está preparada para aceitar, tolerar ou estar exposta.

O conceito de “apetite de risco” é fundamental para o gerenciamento eficaz de riscos. Deve ser considerado pela organização antes da decisão sobre como os riscos serão tratados, sendo também útil para estabelecer as alçadas de riscos.

Um risco que é considerado aceitável no nível estratégico pode não ser considerado aceitável no nível de programa, projeto ou processo específico. O nível de exposição que é considerado aceitável pode ser definido em termos de impacto tolerável e frequência tolerável deste impacto. Níveis de tolerância podem ser estabelecidos e comunicados, reduzindo as chances de surpresas.

Podemos definir o nível de riscos que a organização está disposta a tolerar para um determinado programa, projeto ou processo finalístico, utilizando o conceito de **tolerância a riscos,** ou nível de exposição que, se excedido, deverá ser reportado e uma ação específica deve ser tomada.

O nível de tolerância a riscos pode ser expresso pela **linha de tolerância a riscos** indicada no sumário do perfil de risco. Riscos que aparecem acima da linha não podem ser aceitos sem que sejam autorizados por nível de autoridade superior.

Na Fig. 5, os riscos (1) e (2) estão situados numa área acima do nível de riscos tolerados pela organização, demarcados pela linha pontilhada (linha de tolerância a riscos), exigindo que sejam reportados e que autorizações e ações específicas devam ser demandadas.

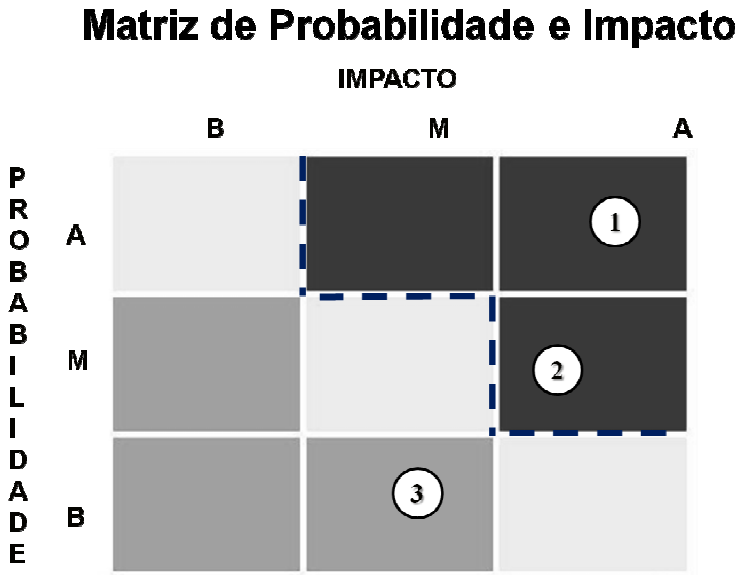


Fig.5 – Matriz de Probabilidade e Impacto com Riscos e Limites de Tolerância

O apetite de risco pode ser expresso por um conjunto de limites devidamente autorizados pela Alta Administração, que comunica a cada nível da organização os limites de risco que a organização pode tomar, seja uma ameaça e o custo de controlá-la, ou uma oportunidade e o custo de explorá-la.

O apetite de risco poderá ser traduzido para o nível específico de programas, projetos e processos finalísticos, nos mesmos termos utilizados para avaliar os riscos.

O conceito de apetite de riscos é útil tanto com relação a ameaças quanto a oportunidades.

O apetite de risco de uma organização não é necessariamente estático. A Alta Administração pode ajustar a qualquer tempo o montante de riscos que a organização deseja tomar, baseado na análise e na avaliação contínua de riscos no nível estratégico.

Apetite de Risco, Hierarquia de Riscos e Delegação de Apetite de Risco

Apetite de Nível Estratégico: é o apetite de risco total de uma organização julgado apropriado e tolerável. É acordado no nível da Alta Administração que deve fixar os limites toleráveis de exposição e limitar as fronteiras de risco aceitável. Isto deve ser feito pelo menos para os riscos que devem ser reportados ou escalados para discussão e decisão da Alta Administração, como, por exemplo, os riscos 1 e 2 da Fig. 5.

Realizando esta análise, é possível à Alta Administração considerar visões setoriais sobre os riscos que podem ser tomados.

Delegação de Apetite de Risco: O apetite de risco definido no nível estratégico pode ser utilizado como ponto de partida para o desdobramento dos níveis de tolerância nos demais níveis da organização. Isto facilita o desdobramento de apetite de risco para tomada de decisão e "empodera" as pessoas para inovar dentro das suas delegações de riscos.

Como descrito acima, o conceito de apetite de riscos é útil tanto com relação a ameaças quanto a oportunidades.

Em caso de ameaças, o conceito de apetite de riscos indica o nível de exposição considerado tolerável e justificável caso a ameaça ocorra.

Em caso de oportunidades, o conceito de apetite de riscos indica o quanto a organização está preparada para perdas potenciais na busca dos benefícios das oportunidades. É importante comparar o valor dos benefícios potenciais com as perdas que poderão ocorrer.

Deve ser observado que alguns riscos são inevitáveis e talvez não estejam dentro da alçada de uma organização gerenciá-lo completamente em um nível tolerável. Por exemplo: muitas organizações têm que aceitar que existem riscos oriundos de atividades terroristas que a organização não pode controlar. Nesses casos, a organização precisa desenvolver planos de contingência, como exemplo na programação de grandes eventos esportivos internacionais.

Apetite de Risco, Governança e Estratégia de Gerenciamento de Riscos

A aplicação do apetite de risco delegado exige que os níveis de autoridade, de reporte, assim como a comunicação, estejam bem claros e definidos como parte da governança e da estratégia de gerenciamento de riscos indicados nos itens 8.1 e 9.1. e 10.1.1.

É possível estabelecer pontos de controle (gatilhos) a partir dos quais os riscos devem ser registrados e reportados para o próximo nível gerencial, quando se aproximam ou se ultrapassam níveis de riscos especificados como, por exemplo, o risco de um projeto que tenha impacto em um programa estratégico do governo.

A delegação de apetite de risco ocorre no nível estratégico da organização que define o apetite de risco e comunica os limites de tolerância de riscos. O nível de programas, projetos e atividades, avalia e desenvolve um plano de respostas a riscos, reportando os riscos "fora dos níveis de tolerância". O nível estratégico concorda ou não com as respostas incluindo reavaliação do limite de tolerância e apetite de riscos.

10.2.3. Risco Inerente e Risco Residual

O risco inerente é a exposição proveniente de um risco específico antes que qualquer ação seja tomada para gerenciá-lo e o risco residual é a exposição remanescente de um risco específico após uma ação ser tomada para gerenciá-lo, assumindo que esta ação seja efetiva.

Quando um risco for identificado e analisado, deve ser sempre considerado o risco inerente e não o risco residual. Se isto não for realizado, a organização não vai saber qual será a sua exposição ao risco, se a ação de controle falhar. O conhecimento sobre o risco inerente também permite avaliar se ele está dentro do apetite de risco da organização e se não precisam ser gastos recursos para controlar estes riscos. Esta necessidade de se conhecer o risco inerente e o risco residual indica que a avaliação do risco é uma etapa do processo de gerenciamento de riscos que não pode ser separada da etapa de planejamento de respostas a riscos.

O risco residual deve ser monitorado, pois a ação de controle pode necessitar de ajustes. Esta análise do risco residual é necessária para a avaliação da efetividade das ações de controle propostas durante a etapa de implementação, monitoramento e controle.

A definição de métodos de análises a serem utilizados, inclusive métodos quantitativos específicos como a análise de Monte Carlo, na etapa de análise e avaliação de riscos, será determinada pelas características da organização, pela natureza dos riscos e pela estratégia de gerenciamento de riscos indicada no item 10.1.1.

Os resultados da etapa de análise e avaliação de riscos permitem criar perfis de riscos dos programas, projetos e processos finalísticos da organização, os quais:

1. Facilitam a identificação da prioridade de riscos (em particular identifica os mais importantes riscos com os quais a alta administração deve se preocupar);
2. Capturam as razões pelas quais as decisões tomadas sobre o que é exposição tolerável e não tolerável;
3. Permitem àqueles envolvidos no gerenciamento de riscos uma visualização de perfis de riscos e como essas áreas e responsabilidades estão relacionadas;
4. Facilitam a reavaliação e monitoramento dos riscos;
5. Fornecem uma base de decisão para a etapa de Planejamento de Respostas aos Riscos.

Uma vez que riscos tenham sido avaliados, os riscos prioritários da organização emergirão. Quanto menos aceitável a exposição relativa a um risco, maior a prioridade que deve ser dada ao seu gerenciamento. Os riscos de maior prioridade devem receber atenção especial do nível mais alto da organização, e devem, consequentemente, serem considerados regularmente pela Alta Administração.

10.2.4 Documentação da Etapa de Análise e Avaliação de Riscos

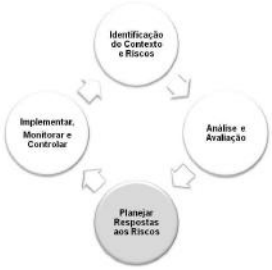
Os resultados da etapa de análise e avaliação de riscos devem ser registrados em documento específico (Registro de Riscos) e documentados de maneira que registre as etapas do processo e complemente as informações inseridas como resultado da etapa anterior Identificação de Riscos que elementos como:

- Probabilidade do Evento de Risco / Descrição da Probabilidade
- Impacto do Evento de Risco / Descrição do Impacto
- Nível de Risco (Combinação Probabilidade e Impacto)
- Matriz de Probabilidade e Impacto
- Perfil Sumário de Riscos
- Quantificação do impacto dos riscos em termos monetários
- Data da Análise
- Lista de Riscos para Análise Adicional e Acompanhamento
- Nível de Urgência dos Riscos

Os formulários específicos a serem utilizados, a forma de arquivamento, de aprovação e retenção, os níveis de reporte e aprovação requeridos devem ser definidos pela estratégia de gerenciamento de riscos alinhada com o sistema de governança conforme indicado nos itens 10.1.1.

Após devidamente analisados e avaliados, os riscos serão considerados na etapa 10.3 PLANEJAMENTO DE RESPOSTAS AOS RISCOS.

10.3 Planejamento de Respostas a Riscos



Esta etapa inclui a formulação das respostas aos riscos de forma a aumentar as oportunidades e reduzir as ameaças aos objetivos do programa, projeto ou processo finalístico. As ações tomadas pela organização para tratar os riscos são ações de controle.

As respostas planejadas devem ser adequadas à relevância do risco, levando em consideração seus custos e benefícios, acordada com as partes interessadas e ter um responsável designado para a coordenação de sua implementação.

As respostas a riscos podem envolver um ou mais dos seguintes tipos:

- Aceitar (ou tolerar) o risco;
- Mitigar os riscos, isto é, tratá-los de forma a restringi-los a um nível aceitável reduzindo as chances de ocorrência (probabilidade) e/ou impacto do evento de riscos;
- Transferir o risco para terceiros;
- Eliminar o risco, alterando o plano ou processo ou terminar a atividade que deu origem ao risco.

Em todos estes casos, as oportunidades geradas pela incerteza devem ser consideradas.

O risco residual é a exposição remanescente de um risco específico após uma ação ser tomada para gerenciá-lo, assumindo que esta ação seja efetiva.

O risco residual deve ser aceitável e justificável, isto é, deve estar dentro do apetite de risco da organização.

10.3.1 Estratégias para Riscos

Existem várias estratégias ou combinação de estratégias que podemos adotar com relação a riscos:

MITIGAR

Um grande número de riscos será tratado desta forma. O propósito desta ação é que, mesmo continuando com a iniciativa que deu origem ao risco, a organização tome a ação de controle para conter o risco em um determinado nível. Implica a redução da probabilidade e/ou impacto de um evento de risco para dentro de limites aceitáveis.

TRANSFERIR

Para alguns riscos, a melhor resposta pode ser transferi-los para terceiros. Isto pode ser feito através de seguros ou contratualmente através de cláusulas específicas e garantias. Esta opção é particularmente útil para mitigar riscos financeiros ou riscos de ativos. A transferência de riscos também pode ser considerada para transferir o nível de exposição da organização ou porque outra organização do governo (pode ser do próprio Governo) é mais capaz de gerenciar o risco. É importante notar que alguns riscos não são totalmente transferíveis - em particular não é geralmente possível transferir risco de reputação e imagem, mesmo se a entrega dos serviços foi contratada para um terceiro. O relacionamento com o terceiro para o qual o risco foi transferido deve ser muito bem gerenciado para assegurar a transferência do risco.

ELIMINAR

Alguns riscos podem ser tratados somente pela alteração de objetivos via redução de escopo, alteração de requisitos e cronograma até término da atividade ou projeto. Deve observado que esta opção de término de atividades e projetos pode ser severamente limitada no governo quando comparado ao setor privado, por se tratarem de serviços essenciais para a sociedade. Por outro lado, certas atividades são conduzidas no setor público porque os riscos são tão grandes que não existe outra forma na qual os resultados que são necessários em termos de benefícios públicos possam ser atingidos. Esta opção pode ser particularmente adotada em projetos se se tornar claro que a relação custo/benefício coloca o projeto em nível de risco inaceitável.

ACEITAR

A exposição ao risco é tolerada sem que nenhuma ação específica seja tomada. Mesmo se o risco não for tolerável, a capacidade para fazer alguma coisa com relação ao risco pode ser limitada, ou o custo de tomar uma ação pode ser desproporcional ao benefício potencial gerado. Nesses casos, a resposta pode ser tolerar o nível de risco. Esta opção, é claro, pode ser suplementada por um plano de contingência para conter os impactos que adviriam caso a ameaça acorra.

PLANO DE CONTINGÊNCIA

O propósito desta ação é prover resposta de risco para uma ameaça, colocando-se em prática um plano de ação que visa reduzir o impacto da ameaça caso o risco ocorra.

RESPOSTAS PARA OPORTUNIDADES

Respostas para as oportunidades identificadas devem ser elaboradas. Esta opção não é uma alternativa para as opções acima. Ao invés disso, é uma opção que deve sempre ser considerada, mesmo quando o risco é tolerado, transferido ou mitigado. Existem dois aspectos a serem considerados. O primeiro é se, ao mesmo tempo em que se está mitigando ameaças, uma oportunidade aparece para explorar um impacto positivo. O segundo é se as circunstâncias ocorrem e, apesar de não gerar ameaças, oferecem oportunidades, como por exemplo, uma iniciativa de redução de custos em determinadas áreas do governo, liberando recursos que podem ser reinvestidos em outro setor.

RISCOS SECUNDÁRIOS

São riscos que surgem como resultados da implementação de respostas aos riscos.

10.3.2 Documentação da Etapa de Planejamento de Respostas aos Riscos

As respostas definidas para os riscos devem ser devidamente documentadas e submetidas à aprovação em documento específico (Registro de Riscos) que poderá conter, além das informações já inseridas como resultado das etapas anteriores, elementos como:

- Respostas selecionadas (Mitigar, Transferir, etc.)
- Ações específicas para implementar a estratégia de resposta definida
- Orçamento / Cronograma da Ação
- Data da Decisão
- Planos de Contingência Recomendados
- Riscos Residuais (após a ação)
- Riscos Secundários (gerados pelas respostas aos riscos)
- Responsável pela Implementação das Respostas
- Perfil de Risco visualizando ações planejadas - ver exemplo Fig. 6 (a) e (b)
- Aprovação das Ações Planejadas

Os formulários e componentes específicos a serem utilizados, assim como níveis de reporte e aprovação requeridos, a forma de arquivamento e o tempo de retenção são definidos pela estratégia de gerenciamento de riscos da organização alinhada com o sistema de governança como indicado no item 10.1.1.

OBJETIVO:		Participar de uma reunião em outra localidade (A viagem será de avião e não posso viajar no no dia anterior)						
RISCO #	DESCRIÇÃO DO RISCO	Risco Inerente		PLANO DE AÇÃO	Risco Residual		DATA	RESP
		IMPACTO	PROBABILIDADE		IMPACTO	PROBABILIDADE		
1	Perder o avião devido a transito	Alto	Alta	Acordar mais cedo Pegar um avião mais cedo	Alto	Baixa	10.8.13	Eu
2	O avião não sair devido ao mau tempo	Alto	Média	Preparar alternativa de reunião via tel/internet	Médio	Média	5.8.13	Sr. Z

Fig.6 (a) – Plano de Ação

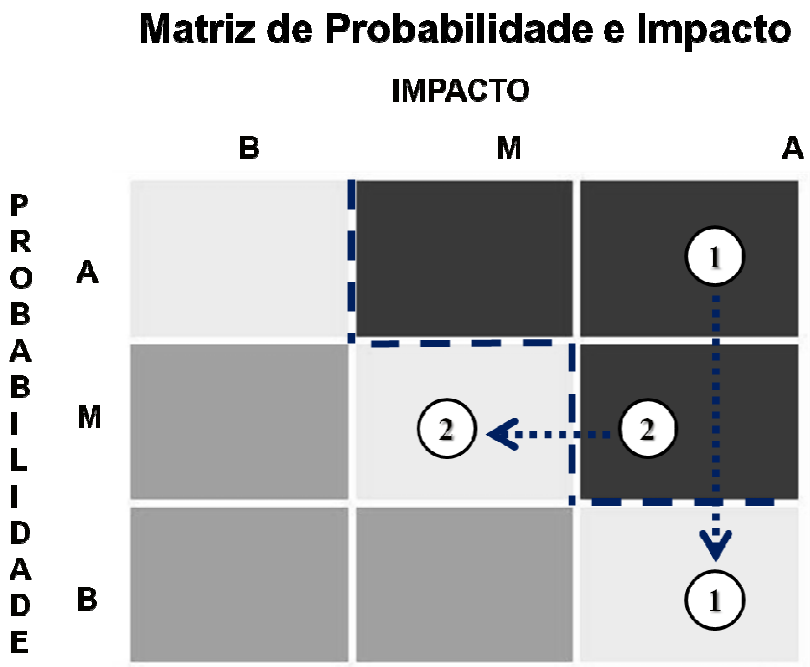
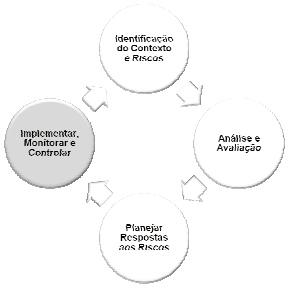


Fig.6(b) – Matriz de Probabilidade e Perfil de Risco e Linha de Tolerância

Após devidamente aprovadas as ações planejadas serão implementados na etapa **10.4 Implementação, Monitoramento e Controle de Riscos.**

10.4 Implementação, Monitoramento e Controle de Riscos



Esta etapa envolve:

1- Implementação das ações planejadas na etapa anterior;

2- Monitoramento e Controle de Riscos que inclui:

- Monitorar se o perfil de risco está mudando;
- Tomar as ações preventivas e corretivas necessárias;
- Garantir que o gerenciamento de riscos está sendo efetivo;
- Atualizar registros de riscos e documentos relacionados;
- Documentar lições aprendidas com plano de ação.

A implementação das ações planejadas será coordenada por responsável indicado na etapa anterior.

Nesta etapa, as atividades definidas pela estratégia de gerenciamento de riscos são implementadas visando identificar se riscos ainda existem, se novos riscos apareceram, se a probabilidade e/ou impacto dos riscos mudaram, reportar mudanças significativas que alteram o nível de riscos, e assegurar a eficácia do controle.

Avaliação Periódica dos Níveis de Riscos: Reuniões de Acompanhamento

Como riscos podem impactar objetivos e metas da organização, o gerenciamento de riscos deve ser um tópico integrante das reuniões relativas ao progresso de programas, projetos e processos finalísticos. Durante as reuniões de acompanhamento serão verificados elementos como: se novos riscos apareceram; se a probabilidade e/ou impacto dos riscos mudaram; reportar aos níveis adequados mudanças significativas que alteram o nível de riscos.

A frequência, a estrutura e os relatórios dessas reuniões devem ser realizados conforme especificado e aprovado na estratégia de gerenciamento de riscos da organização, alinhados com o sistema de governança do órgão e levando em consideração a natureza e nível dos riscos considerados no planejamento das respostas aos riscos. Por exemplo, programas de alto nível risco e orçamento talvez tenham que ser revistos com maior frequência e produzir relatórios específicos adicionais.

Os formulários e componentes específicos a serem utilizados, assim como níveis de reporte e aprovação requeridos, forma de arquivamento, e tempo de retenção são definidos pela estratégia de gerenciamento de riscos da organização alinhada com o sistema de governança como indicado nos itens 10.1.1

Avaliação Periódica do Processo de Gerenciamento de Riscos

O processo de gerenciamento de riscos deve ser submetido a revisões regulares alinhadas com o sistema de governança da organização, para assegurar que ele se mantém adequado e efetivo. A avaliação periódica dos processos de gerenciamento de riscos deve:

1. Assegurar que todos os aspectos de gerenciamento de riscos são revistos, pelo menos, uma vez por ano, ou a critério especificado pelo sistema de governança da organização;

2. Assegurar que os próprios riscos são sujeitos a revisão com uma frequência apropriada de acordo com processo definido pela estratégia de gerenciamento de riscos

3. Assegurar que a gerência responsável esteja participando da avaliação periódica dos riscos e que os níveis apropriados da administração estejam sendo alertados para riscos emergentes ou mudanças em riscos existentes fora dos níveis de tolerância .

Esta avaliação periódica deve ser validada por órgão independente.

A avaliação periódica do nível de riscos e a avaliação do processo de gerenciamento de riscos são distintas entre si, e um não substitui o outro.

Auditorias

Boas práticas de governança preveem que toda organização tenha sua própria auditoria interna. O trabalho da auditoria interna provê uma importante garantia independente e objetiva sobre a adequação do processo de gerenciamento de riscos, controle e governança.

A auditoria interna pode ser utilizada pela organização para auxiliar no desenvolvimento do seu processo de gerenciamento de riscos. A auditoria tem uma visão de todas as atividades relevantes que a organização executa. Entretanto, é importante salientar que a auditoria interna não é um substituto para a responsabilidade primária da administração por gerenciar os riscos sob sua responsabilidade associados ao atingimento de seus objetivos e metas.

Muitas organizações podem designar especialistas internos para auxiliar na estruturação e revisão do processo de gerenciamento de riscos.

É considerada uma boa prática que as organizações estabeleçam um Comitê de Auditoria e Riscos, que englobam as responsabilidades associadas de auditoria com foco no processo de gerenciamento de riscos.

Algumas responsabilidades do Comitê de Auditoria incluem:

- Garantir que riscos e mudanças em riscos estão sendo monitoradas e reportadas de acordo com processos definidos;

- Fornecer recomendações sobre o processo de gerenciamento de riscos, incluindo seu alinhamento com a governança;

Deve ser observado que o Comitê de Auditoria não é o proprietário dos riscos nem responsável pelo gerenciamento riscos e, como a auditoria interna, não é um substituto para o papel do administrador de gerenciar os riscos.

11.0 Comunicação e Aprendizado

A comunicação ágil e adequada entre as diversas partes interessadas e entidades do contexto externo e interno permite avaliações mais rápidas e objetivas a respeito dos riscos a que está exposta uma organização.

A comunicação não é um estágio separado, mas permeia todo o processo de gerenciamento de riscos. Um processo de gerenciamento de riscos depende de participação das partes interessadas e da comunicação de elementos como:

- A importância e a relevância de um gerenciamento efetivo de riscos;

- Uma linguagem comum e acessível para o tema riscos;

- Funções e responsabilidades claras com relação a riscos;

- O processo de gerenciamento de riscos.

Aspectos críticos do gerenciamento de riscos dependem de comunicação :

- Entendimento da definição de riscos;

- A identificação de novos riscos;

- A necessidade de controle das mudanças no nível de riscos;

- Entendimento dos riscos prioritários;

- Entendimento do nível de urgência em termos do tempo com que os riscos precisam ser tratados e do tempo necessário para respostas;

- A importância do contexto de organização estendida e a identificação cruzada de riscos;

- Captura e compartilhamento das lições aprendidas sem os quais a organização não aprende e tende a repetir os mesmos erros.

Um processo de gerenciamento de riscos, que utilize comunicação adequada, reduz as chances de que a Alta Administração só venha a saber de um risco depois que ele se transformou em crise.

GLOSSÁRIO

Apetite de Risco - Quantidade de riscos que uma organização esta preparada para aceitar, tolerar ou estar exposta em um dado ponto no tempo.

Avaliação de Risco - Processo de entendimento do impacto e probabilidade de ocorrência , assim como seu efeito combinado, de um evento de risco específico.

Comitê de Gestão de Riscos - Comitê estabelecido com autoridade para determinar ações relacionadas ao gerenciamento de riscos.

Exposição - Consequências para a organização, expressas em termos de combinação de probabilidade e impacto que podem ocorrer caso o risco específico ocorra.

Gerenciamento de Riscos - Processo que inclui, identificação e avaliação de riscos planejamento e implementação de ações de resposta, monitoramento e controle de riscos.

Estratégia de Riscos - A abordagem definida pela organização com relação ao gerenciamento de riscos. Deve ser documentada, alinhada com sistema de governança e disponibilizada na organização. Descreve elementos como: objetivos do gerenciamento de riscos, processo a ser adotado, os papéis e responsabilidades, as tolerâncias de riscos, a frequência das intervenções do gerenciamento de riscos, as ferramentas e técnicas que serão utilizadas, e os requerimentos de relatórios.

Perfil de Riscos - Avaliação documentada do conjunto de riscos da organização em um dado momento.

Risco - Incerteza quanto ao resultado de ação ou evento, seja positivo ou negativo. Evento incerto ou conjunto de eventos que, caso ocorram ocorrer, ocasionará efeito nos objetivos. Representado por uma combinação de probabilidade de ocorrência e impacto nos objetivos.

Risco Inerente - Exposição proveniente de um risco específico antes que qualquer ação seja tomada para gerenciá-lo.

Risco Residual - Exposição remanescente de um risco específico após uma ação ter sido tomada para gerenciá-lo, assumindo que a ação seja efetiva.

REFERÊNCIAS

Management of Risk - Principles and Concepts- The Orange Book - HM Treasury do HM Government, 2004

ABNT NBR ISO 31000:2009 Gestão de Risco – Princípios e Diretrizes – ABNT Associação Brasileira de Normas Técnicas -2011

MODELO DE EXCELÊNCIA DO SISTEMA DE GESTÃO PÚBLICA – Secretaria de Gestão Publica – Ministério do Planejamento, Orçamento e Gestão

Management of Risk: Guidance for Practitioners - Office of Government Commerce HM Government, 2010

Um Guia do Conhecimento em Gerenciamento de Projetos (Guia PMBOK) 4ª Edição Project Management Institute – 2008.