Guia de Gestão de Riscos do Ministério da Economia

Comitê de Gestão de Riscos, Transparência, Controle e Integridade – CRTCI
Grupo de Trabalho em Gestão de Riscos

Integra
PROGRAMA DE INTEGRAÇÃO, GOVERNANÇA E ESTRATÉGIA

SECRETARIA DE GESTÃO CORPORATIVA
SECRETARIA EXECUTIVA
MINISTÉRIO DA ECONOMIA

PÁTRIA AMADA BRASIL
GOVERNO FEDERAL

Guia de Gestão de Riscos do Ministério da Economia

Comitê de Gestão de Riscos, Transparência, Controle e Integridade – CRTCI

Grupo de Trabalho em Gestão de Riscos

Ministro de Estado da Economia

Paulo Guedes

Secretário-Executivo

Marcelo Guaranys

Chefe da Assessoria Especial de Controle Interno

Francisco Eduardo de Holanda Bessa

Comitê de Gestão de Riscos, Transparência, Controle e Integridade – CRTCI

Francisco Eduardo de Holanda Bessa

Coordenador de Gestão de Riscos e Integridade

Thiago Mendes Rodrigues

Gabinete do Ministro da Economia – GME

Secretaria Executiva

- Assessoria Especial de Controle Interno – AECI
- Comissão de Ética – CE/ME
- Corregedoria – COGER
- Ouvidoria – OUV
- Secretaria de Gestão Corporativa – SGC

Procuradoria-Geral da Fazenda Nacional –PGFN

Secretaria Especial de Comércio Exterior e Assuntos Internacionais – SECINT

- Secretaria-Executiva da Câmara de Comércio Exterior – SE-CAMEX
- Secretaria de Assuntos Econômicos Internacionais – SAIN
- Secretaria de Comércio Exterior – SECEX

Secretaria Especial de Desburocratização, Gestão e Governo Digital – SEDGG

- Secretaria de Gestão – SEGES
- Secretaria de Governo Digital – SGD
- Secretaria de Gestão e Desempenho de Pessoal – SGP

Secretaria Especial de Desestatização, Desinvestimento e Mercados – SEDDM

- Secretaria de Coordenação e Governança das Empresas Estatais – SEST
- Secretaria de Coordenação e Governança do Patrimônio da União – SPU

Secretaria Especial de Fazenda – FAZENDA

- Departamento de Gestão de Fundos – DEF
- Secretaria de Política Econômica – SPE
- Secretaria de Avaliação, Planejamento, Energia e Loteria – SECAP
- Secretaria do Tesouro Nacional – STN
- Secretaria de Orçamento Federal – SOF

Secretaria Especial de Produtividade, Emprego e Competitividade – SEPEC

- Secretaria de Desenvolvimento da Infraestrutura – SDI
- Secretaria de Desenvolvimento da Industria, Comércio, Serviços e Inovação – SDIC
- Secretaria de Advocacia da Concorrência e Competitividade – SEAE
- Secretaria de Políticas Públicas para o Emprego – SPPE

Secretaria Especial do Programa de Parcerias de Investimentos – SEPPI

Secretaria Especial de Previdência e Trabalho – SEPRT

- Secretaria de Previdência – SPREV
- Secretaria do Trabalho – STRAB

Unidade LGPD

Secretaria Especial da Receita Federal do Brasil – SERFB

Conselho Administrativo de Recursos Fiscais – CARF

Conselho de Recursos do Sistema Financeiro Nacional – CRSFN

Conselho de Recursos do Sistema Nacional de Seguros Privados, Previdência Privada Aberta e de Capitalização – CRSNSP

Comissão de Valores Mobiliários – CVM

Fundação Escola Nacional de Administração Pública – ENAP

Fundação Jorge Durat Figueiredo de Segurança e Medicina do Trabalho – FUNDACENTRO

Fundação de Previdência Complementar do Servidor Público Federal do Poder Executivo – FUNPRESP–EXE

Fundação Instituto Brasileiro de Geografia e Estatística – IBGE

Fundação Instituto de Pesquisa Econômica Aplicada – IPEA

Instituto Nacional de Metrologia, Qualidade e Tecnologia – INMETRO

Instituto Nacional de Propriedade Industrial – INPI

Instituto Nacional de Seguro Social – INSS

Superintendência Nacional de Previdência Complementar – PREVIC

Superintendência da Zona Franca de Manaus – SUFRAMA

Superintendência de Seguros Privados – SUSEP

Responsável pela Implementação da LGPD – Lei Geral de Proteção de Dados Pessoais

Grupo de Trabalho em Gestão de Riscos

Coordenadores:

Ana Maria Brandão Cavalcanti – AECI

Carlos Alberto de Camargo Spina – *AECI*

Membros:

Adriana Paiva – Inmetro

Anderson Melchiades – SOF

André Costa Barros – PGFN

Cesar Almeida de Meneses Silva – STN

Etienne Arruda – SEPEC

Francisco Olímpio Corrêa Neto – AECI

Gustavo Lucas – SEPRT

Hélio Fernandes – SEPRT

Hélio Francisco Matos Miranda – Previc

Iamakauê de Almeida – STN

Iuri Cassemiro – SEPEC

João Carneiro – SPU

José A. Filho – PGFN

Marco Aurelio Aires Barreto Ferreira – AECI

Marcos da Costa Avelar – SOF

Marne S. Melo – Inmetro

VERSÕES		
Versão	**Data**	**Principais mudanças realizadas**
1.0	29 ago. 2019	–
2.0	4 fev. 2021	Inclusão dos benefícios da Gestão de Riscos
		Inclusão da Legislação Aplicável
		Inclusão da Metodologia de Gestão de Riscos adotada pelo ME
		Atualização do Referencial Teórico
		Atualização do Glossário

Sumário

1. Introdução

O Guia de Gestão de Riscos do Ministério da Economia (ME), aprovado pela Resolução CRTCI nº 5, de 2019, busca promover a cultura da gestão de riscos em todos os seus órgãos e entidades vinculadas, a fim de alcançar a gradual convergência de métodos, resultados e comunicação.

O esforço de integração e convergência interna do ME quanto à gestão de riscos envolve a compreensão das diferentes culturas, desafios, contextos e níveis de maturidade de seus órgãos e entidades.

De forma a estruturar esse esforço, o modelo de governança adotado pelo ME contempla um processo contínuo, desenhado para identificar, responder e monitorar eventos que possam constranger os objetivos definidos, sob liderança da Assessoria Especial de Controle Interno (AECI), com auxílio do Comitê de Gestão de Riscos, Transparência, Controle e Integridade (CRTCI), que é um órgão de natureza consultiva e deliberativa em apoio ao Comitê Ministerial de Governança (CMG).

Riscos são o efeito da incerteza nos objetivos, conforme definido naa Política de Gestão de Riscos do ME (Resolução CRTCI nº 2, de 2019). Podem surgir da condição natural dos cenários econômico, político, social ou organizacional, e podem se apresentar como ameaças, à medida em que dificultem o alcance dos objetivos, ou como oportunidades, quando indicarem eventos que contribuam ao sucesso.

Nesse sentido, a gestão de riscos é o conjunto de princípios, estruturas, alçadas, processos e atividades coordenados para dirigir e controlar uma organização no que se refere a risco.

Por sua vez, a Política de Gestão de Riscos do ME estabelece princípios, diretrizes e responsabilidades, e serve de base à elaboração do presente Guia, que tem o objetivo de orientar as unidades ministeriais, facultando a utilização de outras metodologias.

Ou seja, respeita-se o grau de maturidade de cada unidade ministerial, e se recomenda a utilização do presente Guia para a implantação da gestão de riscos nas unidades que necessitarem eventualmente de maior apoio ao cumprimento da missão institucional.

2. Sobre a Gestão de Riscos

2.1 Considerações Preliminares

As organizações públicas ou privadas devem procurar entender quais são os riscos associados às suas operações, processos e atividades, no intuito de tratar potenciais prejuízos, e, por conseguinte, implantar as melhorias necessárias ao aprimoramento do sistema de gestão de riscos.

O gerenciamento de riscos é o processo conduzido pela alta administração e pelos demais servidores e colaboradores em que são estabelecidas as estratégias de prevenção e controle de riscos que possam impactar os objetivos da organização.

Ou conforme define a Política de Gestão de Riscos do ME (art. 4º, III): é a 'aplicação sistemática de políticas, procedimentos e práticas de gestão de riscos, para identificar, analisar, avaliar, tratar, comunicar e monitorar potenciais eventos ou situações de risco, bem como fornecer segurança razoável no alcance dos objetivos relacionados a processos, projetos e demais objetos avaliados.'

A função dos controles é dar tratamento à probabilidade ou ao impacto da materialização de um risco em relação a um objetivo fixado. É para responder aos riscos que são avaliados e estabelecidos controles.

Desse modo, a atenção volta-se primeiramente à identificação dos riscos que possam impactar os objetivos da organização e à avaliação da forma como os gestores atuam para minimizar esses riscos, por meio de controles internos e de outras respostas. Evolui-se assim da gestão centrada em controles funcionais à promoção de uma cultura de risco, em que todos os colaboradores tornam-se responsáveis pela gestão de risco e adquirem consciência dos objetivos dos controles.

Considerando a heterogeneidade de contextos entre os órgãos e entidades do ME, o processo de gestão de riscos pode ser personalizado, quando for o caso, para abranger de forma mais adequada situações específicas.

O sistema Ágatha foi desenvolvido para facilitar o processo de gestão de riscos em órgãos ou entidades que desejam implantá-lo ou que o consideram como o sistema mais adequado à sua realidade organizacional.

2.2 Os Benefícios da Gestão de Riscos

A gestão de riscos implementada de forma adequada e contínua traz mais segurança para que a alta administração tome decisões consistentes. Para isso, é preciso levar em consideração a possibilidade de ocorrência tanto de riscos quanto de oportunidades.

Entre outros aspectos, e complementarmente à governança, cabe reforçar que a cultura contribui na formação da base ao gerenciamento de riscos: a governança define o tom, reforça a importância e estabelece as responsabilidades pelo Gerenciamento de Riscos; e a cultura, por sua vez, refere-se aos valores éticos, aos comportamentos desejados e à disseminação da gestão de

riscos como parte do processo de tomada de decisão em todos os níveis.

Assim, de forma geral, compreende-se que gerenciar riscos contribui para assegurar a comunicação eficaz, melhorando as bases ao direcionamento estratégico e à tomada de decisões, bem como para o cumprimento das leis e regulamentos, e à mitigação de possíveis riscos que possam prejudicar o cumprimento dos objetivos e a reputação da organização.

O desenvolvimento de um ambiente ético, com a definição de papéis e responsabilidades, associado ao processo de Gestão de Riscos, é fundamental para se ter uma adequada avaliação, direcionamento e monitoramento da gestão, com vistas à condução eficiente das políticas públicas.

Uma gestão de riscos eficiente contribui para a entrega de serviços dentro do prazo e com a qualidade esperada, e sem desperdício de recursos. Também minimiza a ocorrência de imprevistos para o Governo no momento de implementar suas políticas públicas. Neste sentido, evitam-se crises e contratempos, e há maior previsibilidade dos resultados esperados.

Ao gerir seus riscos, a organização pública deve definir e comunicar as alçadas e responsabilidades de cada agente, notadamente a fim de promover o adequado accountability. O objetivo é fornecer maior transparência na gestão dos bens públicos em prol do cidadão. Uma boa gestão de riscos possibilita identificar oportunidades de melhoria (inclusive a redução e otimização de controles já existentes), bem como gerar ganhos de produtividade.

Complementarmente, ao tratar dos nos riscos à integridade, a gestão de riscos promove melhorias no ambiente ético, pois trata de questões fundamentalmente relacionadas aos valores da instituição e ao cumprimento das leis e regulamentos, de modo a prevenir diversos desvios, entre eles o de corrupção. A Resolução CRTCI nº 7, de 2019, trata especificamente desse temário.

2.3 Legislação Aplicável

O Decreto-lei nº 200, de 1967, definiu a necessidade de gerir riscos na administração pública, e já em seu art. 14 destacava: "O trabalho administrativo será racionalizado mediante simplificação de processos e supressão de controles que se evidenciarem como puramente formais ou cujo custo seja evidentemente superior ao risco.

A Instrução Normativa Conjunta MP/CGU nº 01, de 2016, prevê em seu art.1º: "os órgãos e entidades do Poder Executivo Federal deverão adotar medidas para a sistematização de práticas relacionadas à **gestão de riscos, aos controles internos e à governança**."

O Decreto nº 9.203, de 2017, estabeleceu a política de governança da administração pública direta, indireta, autárquica e fundacional. Seu art. 17 esclarece:

- *A alta administração das organizações da administração pública federal direta, autárquica e fundacional deverá estabelecer, manter, monitorar e aprimorar sistema de gestão de riscos e controles internos com vistas à identificação, à avaliação, ao tratamento, ao monitoramento e à análise crítica de riscos que possam impactar a implementação da estratégia e a consecução dos objetivos da organização no*

cumprimento da sua missão institucional, observados os seguintes princípios:

I. implementação e aplicação de forma sistemática, estruturada, oportuna e documentada, subordinada ao interesse público;

II. integração da gestão de riscos ao processo de planejamento estratégico e aos seus desdobramentos, às atividades, aos processos de trabalho e aos projetos em todos os níveis da organização, relevantes para a execução da estratégia e o alcance dos objetivos institucionais;

III. estabelecimento de controles internos proporcionais aos riscos, de maneira a considerar suas causas, fontes, consequências e impactos, observada a relação custo-benefício; e

IV. utilização dos resultados da gestão de riscos para apoio à melhoria contínua do desempenho e dos processos de gerenciamento de risco, controle e governança.

3. Implantando a Gestão de Riscos

3.1. Princípios da Gestão de Riscos

A Política de Gestão de Riscos do ME especifica que são princípios da gestão de riscos:

i. agregação e proteção do valor público gerado;

ii. promoção do uso eficiente e integrado dos recursos disponíveis, sejam financeiros, humanos, materiais ou tecnológicos;

iii. abordagem explícita da incerteza e de sua natureza;

iv. comprometimento da alta administração, liderança de todos os níveis de gestão e engajamento de todo o corpo funcional;

v. transparência;

vi. uso efetivo das melhores informações disponíveis;

vii. sinergia e apoio da tecnologia da informação;

viii. consideração dos fatores culturais, humanos e sociais;

ix. dinamismo, iteração e capacidade de reagir a mudanças; e

x. melhoria institucional contínua.

3.2. Metodologia de Gestão de Riscos adotada pelo ME

3.2.1 Objetos prioritários – Uma visão conceitual

Todo ato de agir ou de se omitir traz consigo algum risco. Logo, são quase inesgotáveis as oportunidades de análise de risco sobre esses atos. Alguns desses atos ocorrem de forma

isolada e a grande maioria possui baixo impacto para a organização como um todo. Em geral, até em função de sua baixa complexidade, esses atos menos importantes são tratados nas relações internas da organização, quem geralmente concentrará sua atenção para aqueles atos que podem lhe provocar maiores danos (riscos negativos) ou que podem lhe abrir boas oportunidades (riscos positivos), e esses atos precisam estar necessariamente alinhados ao planejamento estratégico da organização e à sua cadeia de valor.

O Planejamento Estratégico e a Cadeia de Valor do ME estão definidos em seu Programa de Integração, Governança e Estratégia, conhecido como Integra (https://www.gov.br/economia/pt-br/acesso-a-informacao/acoes-e-programas/integra). E vale ressaltar que o planejamento estratégico do ME também se integra ao Plano Plurianual (PPA) vigente e com outros planos transversais do Governo.

3.2.2 Mapa Estratégico e Carteira de Projetos

Fonte: https://www.gov.br/economia/pt-br/acesso-a-informacao/acoes-e-programas/integra/arquivos/mapaestrategico.pdf/@@download/file/2.pdf

O mapa estratégico é uma representação gráfica da estratégia que o ME resolveu adotar, com anuência de seu Comitê Ministerial de Governança. Ele traz o conjunto de Objetivos Estratégicos assumidos pelo ME, distribuídos em eixos de atuação.

A esses objetivos estratégicos são vinculados indicadores de desempenho e de referência, sobre os quais são estabelecidas metas anuais a serem alcançadas. E, para alcançar essas metas, o ME mantém, desenvolve ou aperfeiçoa processos internos, vinculados à sua Cadeia de Valor, como será visto em seguida; ou desenvolve Projetos Estratégicos Ministeriais – PEM, que serão desdobrados em projetos setoriais no âmbito das Secretarias Especiais ou da Secretaria Executiva. E é sobre os projetos setoriais que se desenvolve a gestão de riscos em projetos, que servirá para direcionar a execução do projeto para o alcance de seu objetivo específico. Uma vez cumprido o objetivo do projeto, não há mais que se falar em riscos de projeto. Caso os resultados esperados não sejam alcançados, outro projeto pode ser eventualmente criado para uma nova tentativa de alcance de resultados.

Fonte: https://www.gov.br/economia/pt-br/acesso-a-informacao/acoes-e-programas/integra/arquivos/cadeiadevalorintegrada.pdf/@@download/file/cadeiadevalorintegrada.pdf

A Cadeia de Valor do ME também é uma representação gráfica que busca demonstrar o que faz a pasta para gerar valor para a sociedade. Se o Mapa Estratégico é desdobrado em Projetos Estratégicos Ministeriais, a Cadeia de Valor se desdobra em Macroprocessos, que também são aglutinados em eixos estratégicos que levarão a dois principais ganhos para a sociedade: o crescimento econômico e a geração de mais e melhores empregos.

Os macroprocessos são desdobrados em processos pelas Secretarias Especiais e pela Secretaria Executiva e é sobre os processos que se estabelece a gestão de riscos em processos que, apesar de ter fundamentos semelhantes aos dos riscos de projetos, são mais significativos, com maior exigência de controle pois, diferente dos projetos, os processos não são temporários e monocíclicos. Os processos são perenes e se repetem em ciclos sucessivos, orientados no tempo ou por evento. Se um risco negativo se materializa em um projeto, em geral não resta muito o que se fazer, senão contingenciá-lo para que haja o menor prejuízo possível para o objetivo a ser alcançado.

Mas, quando se trata de um processo, além de contingenciar um risco negativo que se materialize, é possível aperfeiçoar o processo para que esse risco não se materialize novamente em um ciclo futuro. Caso se trate de um risco positivo, é possível aperfeiçoar o processo para que a organização se beneficie da oportunidade proporcionada. Faz sentido, portanto, desenvolver tratamentos para os riscos considerados acima do limite prudencial da instituição, buscando aumento de eficiência e eficácia. Em projetos, por sua natureza temporária, os mecanismos de

controle são mais precários, posto que eles se encerrarão quando a etapa do projeto a que ele se refere for concluída.

3.2.3 Priorização dos Objetos para a Gestão de Riscos

Mesmo que qualquer ato de ação ou de omissão possa ser objeto para a gestão de riscos, tipicamente uma organização priorizará a gestão de riscos sobre projetos e processos. Assim, a primeira etapa para a definição de objetos para a gestão de riscos deve ser o mapeamento de iniciativas que tenham relevância nos resultados compromissados pelo ME, classificando-os como "projeto", "processo" ou "outras ações", quando não for um projeto ou um processo.(Ex.: A edição de uma portaria que define os feriados anuais no âmbito do ministério, não precisa ser necessariamente estruturada como um projeto, mas pode ser relevante para os resultados a serem alcançados pela pasta).

Como quem define os projetos e os processos estratégicos são as unidades setoriais do ME (PGFN, Secretarias Especiais e Secretaria Executiva), cabe a elas comporem seus próprios portfólios para a análise de priorização. Não é viável, dado o tamanho do ME, estabelecer prioridades para objetos de unidades setoriais distintas. Então, se as prioridades serão setorizadas, é razoável que os parâmetros para essa priorização também sejam setorizados. Mas não é razoável que essa priorização seja sub setorizada.

É oportuno que cada Secretaria Especial, a Secretaria Executiva e a PGFN possuam uma unidade central que reúna todo o portfólio de objetos relevantes para o resultado da unidade e sobre ele adotar um critério racional de priorização. Não cabe às Secretarias singulares, tampouco a suas subsecretarias e coordenações estabelecer portfólio próprio para priorização. Esclareça-se que essa regra se aplica ao portfólio de objetos que devem ser monitorados em nível ministerial, ou seja um portfólio estratégico.

Em nível setorial, a Secretaria Executiva, as Secretarias Especiais e a PGFN devem ter total liberdade para tratar daquilo que interessa apenas àquela unidade: iniciativas, projetos e processos internos, não vinculados ao Integra. Nessa perspectiva, as Secretarias Especiais e suas secretarias singulares têm autonomia para definir os respectivos objetos prioritários. Ou seja, cumpre-se com o determinado nas resoluções nº 2 e nº 7 do CRTCI.

3.2.4 Plano de Priorização de Objetos para a Gestão de Riscos

Uma vez que a unidade setorial tenha definido seu portfólio de objetos relevantes para os resultados almejados pelo Ministério e os tenha classificado por projeto, processo ou iniciativa, sobre esse portfólio ela aplicará um conjunto de parâmetros que a permitirá, de forma justificada, escolher quais objetos serão alvo da análise de riscos e avaliação de apetite a riscos.

A unidade setorial tem autonomia para definir seus critérios, mas é importante que esses critérios sejam comunicados à alta administração (Comitê Ministerial de Governança – CMG), para que ela ratifique aquele plano de priorização de objetos.

Aprovados pela alta administração (CMG), os objetos do portfólio serão analisados, um a um, à luz desses critérios, gerando a relação de processos a serem avaliados pela unidade.

Os objetos escolhidos irão compor o Plano de Priorização de Objetos para a Gestão de Riscos, até que esse processo tenha que acontecer novamente. E todos os documentos gerados ao longo do processo de escolha desses objetos prioritários devem ser mantidos em guarda para eventual futura auditoria.

A título de exemplo, imagine que uma unidade setorial do ME, ao levantar seu portfólio de objetos, identificou quatro projetos, quatro processos e duas iniciativas, totalizando dez objetos. Ela também validou no CMG cinco parâmetros para priorização dos objetos: grau de impacto do objeto na Estratégia Setorial (Peso 2); grau de impacto do objeto no Orçamento Setorial (Peso 2); Maturidade Operacional do Objeto (Peso 1); Objeto de Análise por TCU ou CGU (Peso 3); e objeto pactuado com outro *stakeholder* (Peso 2). Então, a autoridade máxima da unidade setorial, após consultar suas áreas técnicas, definiu notas de 1 a 5 para cada parâmetro de cada objeto, obtendo uma média ponderada para cada objeto analisado, conforme a figura a seguir:

Objeto ⬇	Parâmetro ➡	Impacto na Estratégia Setorial	Impacto no Orçamento Setorial	Maturidade Operacional	Objeto de Análise por TCU ou CGU	Pactuado por outro stakeholder	Média Ponderada
	Peso ➡	2	2	1	3	2	
Objeto 1	Projeto	1	3	3	3	2	2,4
Objeto 2	Processo	1	1	2	3	3	2,1
Objeto 3	Processo	3	3	2	1	1	1,9
Objeto 4	Processo	3	2	1	1	2	1,8
Objeto 5	Projeto	3	1	3	2	1	1,9
Objeto 6	Projeto	2	1	2	2	1	1,6
Objeto 7	Projeto	2	2	2	2	2	2,0
Objeto 8	Iniciativa	1	1	1	1	3	1,4
Objeto 9	Processo	2	1	3	3	5	2,8
Objeto 10	Iniciativa	3	3	2	2	1	2,2

Fonte: Elaboração própria

A unidade setorial irá classificar os objetos a partir da média ponderada obtida e chegará a uma tabela como a mostrada abaixo, excluindo 60% dos objetos com menor média ponderada:

Objeto ⬇	Parâmetro ➡	Impacto na Estratégia Setorial	Impacto no Orçamento Setorial	Maturidade Operacional	Objeto de Análise por TCU ou CGU	Pactuado por outro stakeholder	Média Ponderada
	Peso ➡	2	2	1	3	2	
Objeto 9	Processo	2	1	3	3	5	2,8
Objeto 1	Projeto	1	3	3	3	2	2,4
Objeto 10	Iniciativa	3	3	2	2	1	2,2
Objeto 2	Processo	1	1	2	3	3	2,1
~~Objeto 7~~	~~Projeto~~	~~2~~	~~2~~	~~2~~	~~2~~	~~2~~	~~2,0~~
~~Objeto 3~~	~~Processo~~	~~3~~	~~3~~	~~2~~	~~1~~	~~1~~	~~1,9~~
~~Objeto 5~~	~~Projeto~~	~~3~~	~~1~~	~~3~~	~~2~~	~~1~~	~~1,9~~
~~Objeto 4~~	~~Processo~~	~~3~~	~~2~~	~~1~~	~~1~~	~~2~~	~~1,8~~
~~Objeto 6~~	~~Projeto~~	~~2~~	~~1~~	~~2~~	~~2~~	~~1~~	~~1,6~~
~~Objeto 8~~	~~Iniciativa~~	~~1~~	~~1~~	~~1~~	~~1~~	~~3~~	~~1,4~~

Fonte: Elaboração própria

A área tinha como objetivo selecionar dois projetos para passar pelo processo de gestão de riscos, compondo o Plano de Priorização de Objetos para a Gestão de Riscos do ME. Então, dos quatro objetos mais bem ranqueados, a autoridade máxima da unidade setorial precisaria escolher dois e, por critérios qualitativos, assertivos subjetivos e justificados, ela decidiu selecionar o objeto com maior média ponderada (Objeto 9) e objeto que ficou na terceira colocação do *ranking* (Objeto 10), em detrimento do segundo colocado (Objeto 1), pois o Objeto 10 tinha maior impacto sobre a estratégia setorial. E assim foram selecionados os dois objetos a serem submetidos ao processo de gestão de riscos.

Objeto ⬇	Parâmetro ➡	Impacto na Estratégia Setorial	Impacto no Orçamento Setorial	Maturidade Operacional	Objeto de Análise por TCU ou CGU	Pactuado por outro stakeholder	Média Ponderada
	Peso ➡	2	2	1	3	2	
Objeto 9	Processo	2	1	3	3	5	2,8
Objeto 10	Iniciativa	3	3	2	2	1	2,2
~~Objeto 1~~	~~Projeto~~	~~1~~	~~3~~	~~3~~	~~3~~	~~2~~	~~2,4~~
~~Objeto 2~~	~~Processo~~	~~1~~	~~1~~	~~2~~	~~3~~	~~3~~	~~2,1~~

Fonte: Elaboração própria

3.2.5 Detalhamento do Plano de Priorização de Objetos

Aqui o que se tem é uma lista de objetos que serão tratados no Plano de Priorização de Objetos para a Gestão de Riscos, com sua classificação quanto ao tipo: projeto, processo ou iniciativa. Caberá, então, à unidade setorial designar os responsáveis pelo detalhamento de cada objeto, que deverá trazer:

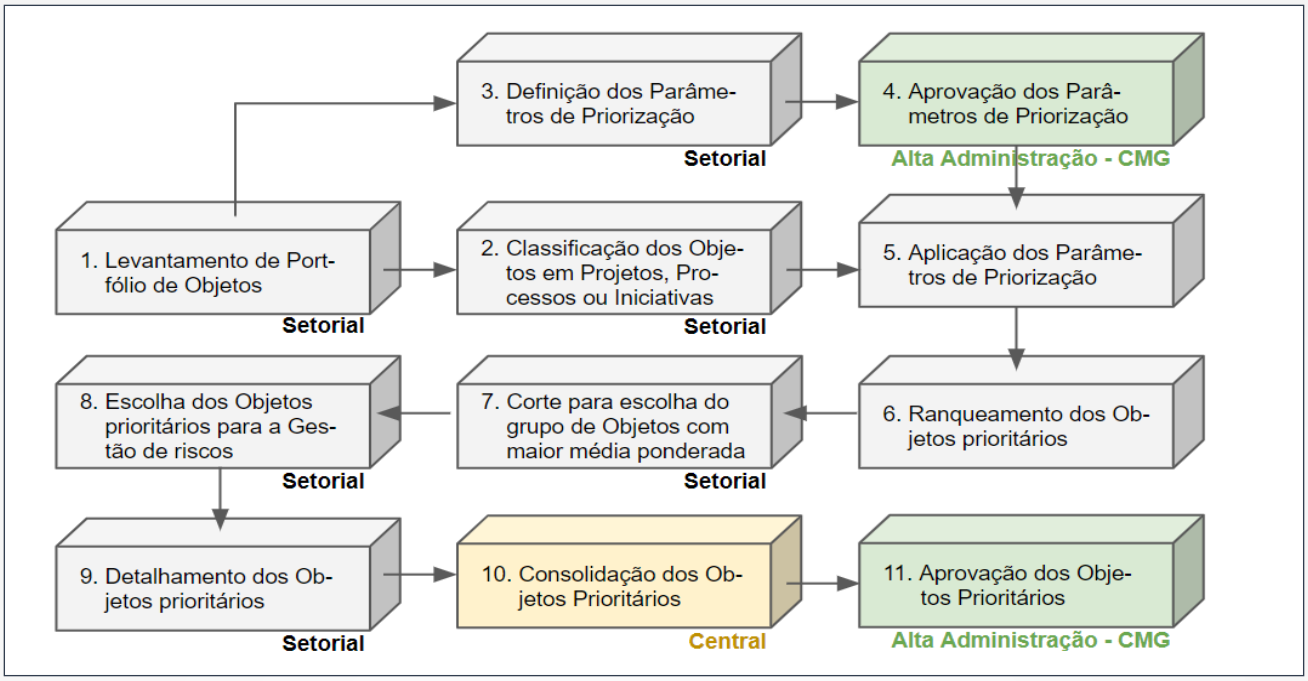
a) Breve descrição do objeto;
b) Como o objeto impacta o planejamento estratégico do Ministério;
c) Áreas do Ministério envolvidas na execução do objeto, com as suas devidas responsabilidades;
d) Cronograma com apontamento de prazos para o mapeamento do objeto; a análise de riscos do objeto; a definição da resposta aos riscos; a definição do plano de ações mitigadoras decorrentes da resposta ao risco; e a definição mecanismos de controle do risco, com eventuais medidas de contingência.

A figura abaixo representa como um objeto pode ser detalhado para compor o Plano de Priorização de Objetos para a Gestão de Riscos.

OBJETO 02		
Descrição:	O objeto.	
Impacto:	O objeto impacta na estratégia do Ministério quando.	
Áreas envolvidas:	a) A Subsecretaria XPTO é responsável por. b) A Coordenação XYZ é responsável por.	
Cronograma:	Mapeamento	31/01/2021
	Análise de riscos	28/02/2021
	Resposta aos riscos	15/03/2021
	Levantamento das ações mitigadoras	31/03/2021
	Definição dos mecanismos de controle	31/03/2021

Uma vez detalhado cada objeto, o Plano de Priorização de Objetos para a Gestão de Riscos deve ser levado pelas unidades setoriais ao conhecimento das unidades centrais responsáveis no ME, para análise crítica e possível revisão, bem como definição da estratégia de acompanhamento da execução do plano. Essas áreas centrais, então, levarão o plano consolidado para conhecimento e aprovação da alta administração (em reunião do CMG). Aprovado pelo CMG, o plano é levado para conhecimento dos órgãos de controle para que eles se manifestem sobre como querem acompanhar a execução do plano.

A figura a seguir demonstra o fluxo para a seleção e consolidação dos objetos prioritários para serem submetidos à gestão de riscos. E, uma vez inserido o objeto no processo de gestão de riscos do Ministério, ele deverá ser acompanhado pelo tempo que o objeto permanecer ativo: a cada execução de plano de priorização, novos objetos serão agregados ao portfólio monitorado.



Fonte: Elaboração própria

Posteriormente, será aplicada aos processos priorizados a Metodologia de Gestão de Riscos do ME – baseada nos fundamentos da ABNT NBR ISO 31000 e COSO ERM – que se divide em seis etapas:

- Análise de contexto;
- Identificação de riscos;
- Avaliação de riscos;
- Resposta aos riscos (evitar, aceitar, reduzir, compartilhar);
- Comunicação; e
- Monitoramento.

A gestão de riscos deve ser realizada pelos respectivos Gestores de Riscos em cada um dos processos priorizados sob sua responsabilidade. A priorização feita deve ser comunicada à AECI, informando inclusive os critérios adotados para a sua escolha.

Assim, definidos os processos a serem trabalhados, bem como os papéis e responsabilidades dos gestores de riscos, estes prosseguirão com as etapas descritas a seguir.

3.2.6 Análise de Contexto

A análise de contexto refere-se ao levantamento e registro dos aspectos externos e internos, que compõem o ambiente onde a organização visa alcançar os seus objetivos, permitindo a compreensão clara do contexto em que a organização se insere a fim de proporcionar uma visão abrangente dos fatores que podem influenciar a capacidade da organização de atingir os resultados planejados.

O ambiente interno envolve aspectos como governança, estrutura organizacional, funções, alçadas e responsabilidades, políticas, estratégias, capacidades, competência,

sistemas de informação, processos decisórios, cultura organizacional.

O ambiente externo envolve aspectos como social, político, legal, regulatório, financeiro, tecnológico, econômico, ambiental, relações com partes interessadas externas e suas percepções e valores.

Para análise de contexto, destaca-se a ferramenta Análise SWOT (*Strengths*, *Weaknesses*, *Opportunities*, *Threats*), que auxilia a análise sobre os pontos fortes e fracos do ambiente interno e as oportunidades e ameaças do ambiente externo. Os insumos para a estruturação da Análise SWOT podem ser levantados por meio da utilização de uma tempestade de ideias (*Brainstorming*) – técnica para compartilhamento espontâneo de ideias – que poderá ser realizada em sessões de oficinas com a equipe responsável pelo processo de trabalho, sendo importante especificar o seu objetivo, a fim de identificar os fatores internos e externos que apoiam ou dificultam o seu alcance.

	Fatores Positivos	**Fatores Negativos**
Fatores Internos	***Strengths* (Forças)** Aspectos positivos tangíveis e intangíveis, internos à organização e sob seu controle. Ex.: equipe capacitada, tecnologia avançada, adaptabilidade às mudanças, etc.	***Weaknesses* (Fraquezas)** Aspectos negativos internos à organização e sob seu controle, que podem restringir o desempenho. Ex.: sistemas de informação obsoletos, baixa capacidade inovadora, ausência de planos de desenvolvimento de recursos humanos, etc.
Fatores Externos	***Opportunities* (Oportunidades)** Aspectos positivos externos à organização e fora do seu controle, que podem potencializar o atingimento de metas e crescimento organizacional. Ex.: novos clientes, disponibilidade de novos canais de divulgação/distribuição, ampliação do escopo de atuação.	***Threats* (Ameaças)** Aspectos negativos externos à organização e fora do seu controle, que podem prejudicar o atingimento das metas e comprometer o crescimento organizacional. Ex.: restrições orçamentárias, dispersão geográfica da clientela, etc.

Figura: Análise SWOT

Por fim, a análise do contexto também envolve a definição dos critérios de risco, como limites de exposição e atribuições dos agentes envolvidos na avaliação e tratamento de riscos. Essas informações subsidiam todo o processo de gestão de riscos, inclusive a etapa de comunicação.

Principais resultados da etapa de análise de contexto

- DEFINIÇÃO CLARA DO ESCOPO E OBJETIVO DO PROCESSO DE TRABALHO.
- PRINCIPAIS LEIS, REGULAMENTOS E NORMAS QUE INFLUENCIAM O PROCESSO DE TRABALHO.
- SISTEMAS E OU DEMAIS FERRAMENTAS (EX.: PLANILHA DE EXCEL) UTILIZADAS PARA OPERACIONALIZAR O PROCESSO DE TRABALHO.
- REGISTRO DA ANÁLISE SWOT (FORÇAS, FRAQUEZAS, OPORTUNIDADES E AMEAÇAS.)

3.2.7 Identificação de Riscos

A etapa de identificação de riscos envolve o reconhecimento, descrição e registro do evento de risco, com a identificação das suas causas (fontes) e consequências (efeitos).

Nessa etapa, deverá ser desenvolvida uma lista de eventos de riscos que podem constranger os resultados e o alcance dos objetivos, afetando o valor público a ser entregue à sociedade.

Como fonte de informação para identificação dos riscos, é desejável verificar também a existência de algum Acórdão ou Recomendação dos órgãos de controle (TCU e CGU), processos judiciais ou reclamações na Ouvidoria relacionados ao processo sob análise.

Para cada evento de risco identificado, deve-se especificar, explorar e ressaltar suas prováveis causas e possíveis consequências.

O risco deve ser descrito de forma precisa, atentando-se para não o descrever simplesmente como o "não alcance" do objetivo e não o confundir com suas causas, suas consequências ou com a ausência/deficiência de um controle existente. Em suma, a descrição do risco deve prover a compreensão do que pode dar errado.

A sintaxe a seguir auxilia a correta descrição dos riscos:

Devido a **<CAUSA, FONTE>,**
poderá acontecer **<EVENTO DE RISCO>,**
o que poderá levar a **<IMPACTO, EFEITO, CONSEQUÊNCIA>,**
constrangendo o **<OBJETIVO DEFINIDO>.**

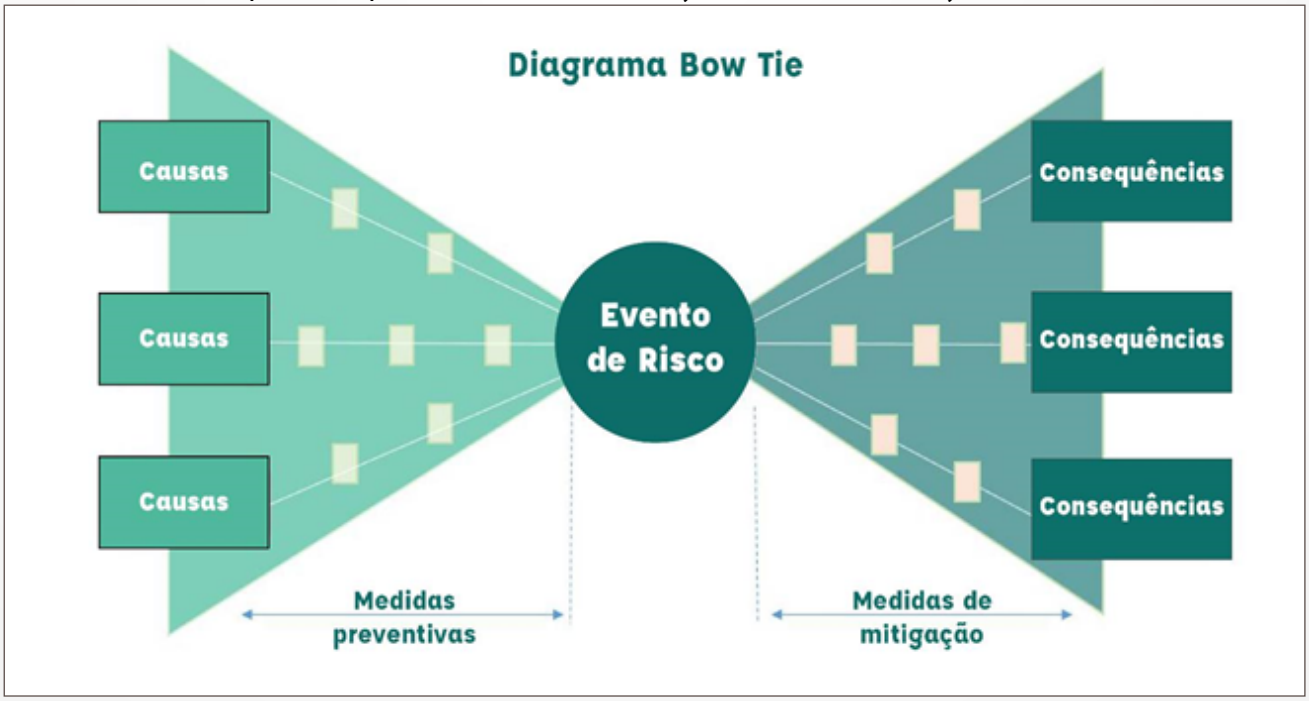
Fonte: Guia de Gestão de Riscos – STF

Na etapa de identificação de riscos, é imprescindível o envolvimento dos servidores responsáveis pela gestão do processo de trabalho. Preferencialmente, sugere-se que os servidores tenham recebido capacitação prévia a fim de aplicar a Metodologia de Riscos do ME.

Como apoio à coleta estruturada de informações, poderão ser utilizadas técnicas como *Brainstorming*, Diagrama de Ishikawa (espinha de peixe), *Bow-Tie*, entrevista com especialistas, análise de cenários.

Segundo norma ISO/IEC 31010:2009, análise *bow-tie* é uma maneira esquemática simples de descrever e analisar os caminhos de um risco desde as causas até as consequências. Além disso, apresenta barreiras entre as causas e o risco, que representam uma forma de prevenir a sua ocorrência, e entre o risco e as consequências, que representam formas de mitigar os impactos.

A norma ISO/IEC 31010:2009 traz um rol de técnicas mais amplo que pode ser consultado em apoio aos processos de identificação, análise e avaliação de riscos.



Fonte: Ministério do Planejamento, Desenvolvimento e Gestão. Manual de Gestão de Integridade, Riscos e Controles Internos da Gestão, p. 28, 2017. Figura adaptada.

Principais resultados da etapa de identificação de riscos

- LISTA DOS RISCOS IDENTIFICADOS.
- DESCRIÇÃO ADEQUADA DOS RISCOS MAIS RELEVANTES.

3.2.8 Avaliação de Riscos

A etapa de avaliação de riscos visa promover o entendimento do nível do risco e de sua natureza e estimar a sua probabilidade de ocorrência, o seu impacto e a eficácia dos controles que já existem para mitigá-los.

A análise da probabilidade considera o conhecimento técnico e experiências vivenciadas dos partícipes. Sempre que possível, deve-se fazer a avaliação quantitativa, com base nos dados estatísticos de eventos de riscos já materializados, por determinado período de tempo ou média histórica disponível. Quando não houver dados, é suficiente realizar a avaliação qualitativa.

O impacto, caso um evento de risco ocorra, relaciona-se às consequências que terá em algum âmbito relevante. Dessa forma, ele será avaliado conforme as consequências para âmbitos específicos, como desperdício de recursos ou mau desempenho do processo, desconformidade legal, danos ao Erário e danos à imagem.

Uma forma de se estimar o nível do risco é com a utilização de uma matriz impacto x probabilidade, exemplificada abaixo:

Nível do Risco – Matriz de Probabilidade x Impacto

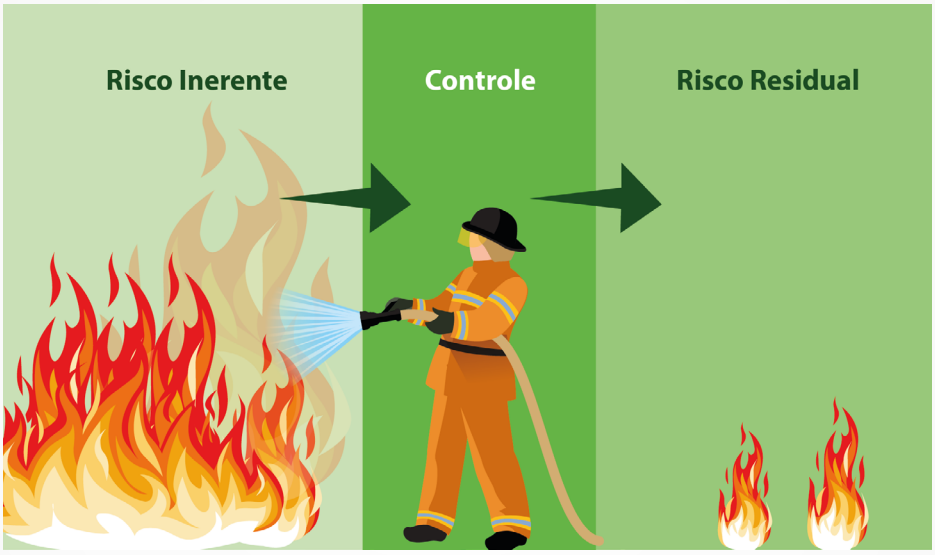
IMPACTO	Muito baixa	Baixa	Média	Alta	Muito alta
Catastrófico	Moderado	Alto	Crítico	Crítico	Crítico
Grande	Moderado	Alto	Alto	Crítico	Crítico
Moderado	Pequeno	Moderado	Alto	Alto	Crítico
Pequeno	Pequeno	Moderado	Moderado	Alto	Alto
Insignificante	Pequeno	Pequeno	Pequeno	Moderado	Moderado

PROBABILIDADE

A análise da eficácia dos controles existentes objetiva aferir se o risco residual se encontra dentro do nível de risco aceitável. De acordo com a Instrução Normativa Conjunta MP/CGU Nº 01/2016:

- Risco inerente: é o risco a que uma organização está exposta sem considerar quaisquer ações gerenciais que possam reduzir a probabilidade de sua ocorrência ou seu impacto. (Art. 2º, XIV).
- Risco residual: é risco a que uma organização está exposta após a implementação de ações gerenciais para o tratamento do risco. (Art. 2º, XV).

Controles são o conjunto de regras, procedimentos, diretrizes, protocolos, rotinas de sistemas informatizados, conferências ou trâmites de documentos e informações, entre outros, operacionalizados de forma integrada pela direção e pelo corpo de servidores das organizações, destinados a enfrentar os riscos e fornecer segurança razoável na consecução da missão da entidade (Art. 2º, V, IN Conjunta MP/CGU Nº 01/2016).



A avaliação dos controles existentes será notadamente quanto ao seu desenho e à sua operação:

Critérios de avaliação do desenho e operação do controle

Desenho do Controle	Operação do Controle
Se refere à normatização do controle executado, que pode estar formalizada por meio de instrução normativa, portaria, lei, decreto ou outro instrumento.	**Se refere à efetiva implementação de procedimentos de controle, independente de haver instrumento que regulamente sua execução. Pode acontecer do controle ser executado devido à experiência do servidor.**
(1) Não há procedimento de controle;	(1) Não há procedimento de controle;
(2) Há procedimentos de controle, mas não são adequados e nem estão formalizados;	(2) Há procedimentos de controle, mas não são executados;
(3) Há procedimentos de controle formalizados, mas não estão adequados (insuficientes);	(3) Os procedimentos de controle estão sendo parcialmente executados;
(4) Há procedimentos de controle adequados (suficientes), mas não estão formalizados;	(4) Os procedimentos de controle são executados, mas sem evidência de sua realização;
(5) Há procedimentos de controle adequados (suficientes) e formalizados.	(5) Procedimentos de controle são executados e com evidência de sua realização.

Os controles devem ser analisados sob a ótica de custo e benefício, de forma a otimizar a alocação de recursos e permitir maior alcance do valor público gerado. De forma geral, o custo de um controle não deve superar seu benefício gerado ou esperado. Além disso, a análise de riscos é o momento adequado para verificar se há controles onerosos que sejam desnecessários ou que podem ser simplificados, a depender do risco que objetivam mitigar.

Sempre que estiverem disponíveis, as consistências das avaliações probabilidade, impacto e controle devem ser sustentadas pelo registro de evidências, como dados, documentos, relatórios, documentos SEI.

Caso o órgão ou entidade utilize o sistema Ágatha, esclarecemos que há manuais específicos para o ambiente web – Sistema Ágatha Treina – e para o ambiente oficial.

Principais resultados da etapa de avaliação de riscos

- AVALIAÇÃO DO NÍVEL (PROBABILIDADE, IMPACTO E CONTROLE) DOS RISCOS.
- PRIORIZAÇÃO DOS RISCOS DE MAIOR NÍVEL.

3.2.9 Resposta aos Riscos

A resposta aos riscos é a etapa em que, a cada risco identificado e avaliado, poderá ser elaborada e proposta uma ou mais medidas (respostas ao risco) para sua mitigação, na forma de um Plano de Tratamento.

Há quatro possíveis tipos de respostas quanto aos riscos identificados:

- evitar: não iniciar ou descontinuar a atividade que origina o risco;
- aceitar: deixar a atividade como está, não adotando qualquer medida;
- reduzir: desenvolver ações para mitigar o risco, ou seja, remover suas fontes ou reduzir a probabilidade e/ou o impacto do risco; e
- compartilhar: distribuir parte do risco para outros atores (terceiros).

As respostas deverão observar os limites de exposição a riscos definidos pela alta administração, de forma que, para risco com nível de criticidade apurado superior ao definido, a organização deverá, após a análise de custo-benefício, instituir controles e/ou ações mitigadoras com o objetivo de reduzi-lo ou compartilhá-lo até sua conformidade com o limite de exposição aceitável.

Os controles propostos podem ser avaliados quanto a:

Tipo:

- **preventivo:** tem como objetivo prevenir a materialização do evento de risco. Via de regra atua sobre a causa do evento de risco (Ex.: verificação da credencial das pessoas antes de entrarem no prédio do ministério); ou
- **corretivo:** tem como objetivo mitigar falha que já ocorreu, apurada após o processamento inicial ter ocorrido. Atua sobre a consequência do evento. (Ex.: identificação, pela vigilância, das pessoas que estão no prédio, mas sem credencial).

Natureza:

- **manual:** controle realizado por pessoa (Ex.: conferência de assinatura);
- **automático:** controle processado por sistema, sem intervenção humana relevante (Ex.: senha de e-mail); ou
- **híbrido:** controle que mescla atividades manuais e automáticas.

Frequência: anual, semestral, bimestral, mensal, diária ou outra frequência adequada ao desenho do controle.

A implementação dos controles considera ainda aspectos como:

- os custos e esforços (diretos ou de oportunidade) de implementação envolvidos, bem como os benefícios decorrentes;
- os requisitos legais, normativos e regulatórios;
- os responsáveis por aprovar e implementar as ações (as funções devem ser segregadas);
- recursos necessários.

Principais resultados da etapa de resposta aos riscos

- DEFINIÇÃO DAS RESPOSTAS AOS RISCOS DE MAIOR NÍVEL.
- ELABORAÇÃO DO PLANO DE AÇÃO PARA A IMPLEMENTAÇÃO OU APERFEIÇOAMENTO DOS CONTROLES, QUANDO FOR O CASO.

3.2.10 Comunicação

A comunicação é a etapa contínua em que as instâncias envolvidas com Gestão de Riscos interagem. Abrange a coleta e a disseminação de informações e iniciativas a fim de

assegurar a compreensão suficiente a todos os agentes envolvidos dos riscos existentes em cada decisão.

É importante que as informações apresentadas nos meios de monitoramento possuam qualidade contextual e de representação com base nos critérios a seguir:

- Relevância: a informação deve ser útil para o objetivo do trabalho;
- Integralidade: as informações importantes e suficientes para a compreensão devem estar presentes;
- Adequação: o volume de informação deve ser adequado e suficiente;
- Concisão: a informação deve ser apresentada de forma compacta;
- Consistência: as informações apresentadas devem ser compatíveis;
- Clareza: a informação deve ser facilmente compreensível; e
- Padronização: a informação deve ser apresentada no padrão aceitável.

O acesso a informações confiáveis, íntegras e tempestivas é vital para a eficiência da gestão e visam facilitar o alcance dos objetivos. Para isso, o fluxo das comunicações deve permitir que as informações fluam em todas as direções, com a divulgação tempestiva e adequada das informações às partes interessadas.

Assim, devem ser observados aspectos como alçadas dos agentes e, quanto às informações, a gradual convergência para promover a relevância, integralidade, adequação, concisão, consistência, clareza e padronização.

Geralmente envolve a promoção de iniciativas e instâncias, como o Comitê Ministerial de Governança – CMG, o Comitê de Gestão de Riscos, Transparência, Controle e Integridade – CRTCI, as Oficinas, o Levantamento de Riscos Estratégicos, entre outros debates.

Principal resultado da etapa de comunicação

- **ENVIO TEMPESTIVO DAS INFORMAÇÕES PARA AS UNIDADES INTERESSADAS.**

3.2.11 Monitoramento

O ciclo de gestão de riscos deverá ser repetido periodicamente a fim de verificar se houve mudanças dos eventos de riscos. O Gestor de Riscos também fará o monitoramento

contínuo dos riscos sob sua responsabilidade, de tal modo que poderá, a qualquer momento, reavaliar seus riscos e informar os resultados à AECI.

As instituições utilizam-se de avaliações contínuas, independentes ou uma combinação das duas para assegurar que os controles permaneçam eficazes e que o ambiente de controle se mantenha efetivo.

O gerenciamento de riscos corporativos de uma organização modifica-se com o passar do tempo. As respostas a risco que se mostravam eficazes anteriormente podem tornar-se inócuas; as atividades de controle podem perder a eficácia ou deixar de ser executadas; ou os objetivos podem mudar. Diante dessas mudanças, a administração necessita determinar se o funcionamento do gerenciamento de riscos corporativos permanece eficaz. (COSO ERM – *Committee of Sponsoring Organizations of the Treadway Commission – Enterprise Risk Management*)

A implementação de atividades relacionadas à gestão de riscos e controles não é suficiente para assegurar que os objetivos dos processos sejam alcançados. O estabelecimento de limites de atuação de cada área/servidor, bem como a clareza das suas responsabilidades, é essencial para que cada um dos participantes saiba como seu cargo se encaixa na estrutura corporativa de gestão de riscos e controles.

No âmbito do ME, é possível destacar os seguintes papéis de monitoramento:

- Órgão ou Unidade: monitoramento de seus riscos específicos e retroalimentação às instâncias de decisão, com o apoio das unidades próprias de suporte;
- CRTCI: acompanhamento dos ciclos de gestão de riscos em cada órgão, e dos processos acompanhados e monitorados; e
- AECI: suporte ao CRTCI, supervisão e apoio metodológico e operacional a todos os órgãos e unidades, bem como o levantamento e acompanhamento de riscos estratégicos.

Nesse sentido, a compreensão do papel de primeira linha também é essencial. Formada pelos gestores dos processos, que são os proprietários dos riscos e os responsáveis pela implementação de ações corretivas, a primeira linha tem como objetivo manter um controle interno eficaz no dia a dia. Assim, monitora continuamente seus processos, assegurando que os riscos sejam mantidos nos níveis aceitáveis (tolerância a risco) e que os controles permaneçam eficazes.

Faz parte de suas atribuições identificar, avaliar, controlar e mitigar os riscos, guiando o desenvolvimento e a implementação de políticas e procedimentos internos para garantir que as atividades estejam de acordo com as metas e os objetivos.

Por ser uma função rotineira, o monitoramento contínuo da primeira linha deverá ser incorporado às atividades normais e repetitivas da organização, sendo preferencialmente um procedimento automatizado e direcionado para avaliar a eficácia dos controles considerados chave.

As atividades de monitoramento são originárias das atividades de gestão e podem incluir:

- confrontação de informações oriundas de fontes diversas;
- identificação de comportamentos fora do padrão; e
- variações cujos percentuais não estejam dentro dos limites estabelecidos.

São elementos essenciais nessa etapa os indicadores-chave de risco – ICR, na forma de medidas ou métricas em relação a um referencial definido, que sinalizam a exposição aos riscos, cabendo aos coordenadores, diretores e secretários monitorar o nível de risco de sua área e o impacto em toda a unidade setorial.

Os ICR são utilizados para alertar os gestores da necessidade de tomada tempestiva de ações corretivas. Devem estar diretamente relacionados aos processos, riscos e controles que tenham relevância ao atingimento dos objetivos.

O monitoramento por ICR tem a finalidade de acompanhar a eficácia dos controles e a manutenção dos riscos em níveis aceitáveis, observado o apetite de risco da instituição.

Tais indicadores são acompanhados pelos gestores, que, no caso de indicativos de deficiência, deverão avaliar e propor ações corretivas, como ajustes dos controles existentes.

Para cada processo analisado, é necessário definir uma periodicidade para sua revisão, com base em sua relevância, a fim de aprimorá-lo pelo aprendizado, corrigir eventuais falhas quanto à conformidade com as normas, controles internos deficientes, novos riscos não mapeados e riscos que perderam sua relevância de forma a aperfeiçoar a Gestão.

Principais resultados da etapa de monitoramento

- **ACOMPANHAMENTO AO LONGO DO TEMPO DOS RISCOS AVALIADOS E DAS RESPECTIVAS RESPOSTAS ELABORADAS.**
- **DEFINIÇÃO DA NECESSIDADE DE REAVALIAÇÃO DOS RISCOS, QUANDO NECESSÁRIO.**

Referências Bibliográficas

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO 31000**. Gestão de Riscos: Princípios e Diretrizes. Rio de Janeiro, 2018.

BRASIL. **Decreto nº 9203, de 22 de novembro de 2017**. Dispõe sobre a política de governança da administração pública federal direta, autárquica e fundacional. 2017. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/decreto/D9203.htm. Acesso em: 28 janeiro 2021.

BRASIL. Controladoria-Geral da União. **Instrução Normativa nº 3**, de 9 de junho de 2017. Aprova o Referencial Técnico da Atividade de Auditoria Interna Governamental do Poder Executivo Federal. 12 jun. 2017. Disponível em: https://www.in.gov.br/materia/-/asset_publisher/Kujrw0TZC2Mb/content/id/19111706/do1-2017-06-12-instrucao-normativa-n-3-de-9-de-junho-de-2017-19111304. Acesso em: 28 jan. 2021.

BRASIL. Ministério da Economia. Comitê de Gestão de Riscos, Transparência, Controle e Integridade – CRTCI. **Resolução nº 3, de 27 de junho de 2019**. Dispõe sobre o primeiro levantamento de Riscos à Integridade no âmbito do Ministério da Economia, e sobre os Agentes de Integridade. 2019. Disponível em: https://www.gov.br/economia/pt-br/acesso-a-informacao/acoes-e-programas/integra/governanca/comites-tematicos-de-apoio-a-governanca/arquivos/documentos-crtci/resolucoes/res-crtci-3.pdf/view. Acesso em: 28 jan. 2021.

BRASIL. Ministério da Economia. Secretaria de Previdência. I**mplementando a Gestão de Riscos na SPREV**. Brasília, 2020.

BRASIL. Ministério da Transparência. Controladoria-Geral da União. **Portaria nº 1075, de 23 de abril de 2018.** Aprova o Plano de Integridade do Ministério da Transparência e Controladoria-Geral da União – CGU. 12 jun. 2017. Disponível em: https://repositorio.cgu.gov.br/bitstream/1/41335/5/Portaria_1075_2018_CGU.pdf. Acesso em: 28 jan. 2021.

BRASIL. Ministério do Planejamento, Orçamento e Gestão. Controladoria-Geral da União. **Instrução Normativa Conjunta nº 1**, de 10 de maio de 2016. Dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo federal. 11 maio 2016. Disponível em: https://www.in.gov.br/materia/-/asset_publisher/Kujrw0TZC2Mb/content/id/21519355/do1-2016-05-11-instrucao-normativa-conjunta-n-1-de-10-de-maio-de-2016-21519197. Acesso em: 28 jan. 2021

BRASIL. Ministério do Planejamento, Orçamento e Gestão: GESPÚBLICA. Projeto de Desenvolvimento do Guia de Orientação para o Gerenciamento de Riscos. **Guia de Orientação para o Gerenciamento de Riscos. Brasília**, 1 mar. 2013. Disponível em: http://www.gespublica.gov.br/content/guia-de-orientação-para-o-gerenciamento-de-riscos. Acesso em: 28 jan. 2021

BRASIL. **Rede GIRC**. Disponível em: https://gestgov.discourse.group/c/rede-girc/13. Acesso em: 28 jan. 2021.

BRASIL. Superintendência Nacional de Previdência Complementar – PREVIC. **Metodologia em Gestão de Riscos**. Brasília, Junho 2018.

COSO GRC. **Gerenciamento de Riscos Corporativos – Integrado com Estratégia e Performance**.

Junho 2017. Disponível em: https://repositorio.cgu.gov.br/bitstream/1/41825/8/Coso_portugues_versao_2017.pdf. Acesso em: 28 jan. 2021.

HM TREASURY. **The Orange Book**: Management of Risk – Principles and Concepts. 2004. Disponível em: https://www.who.int/management/general/risk/managementofrisk.pdf. Acesso em: 28 jan. 2021.

THE INSTITUTE OF INTERNAL AUDITORS (IIA). **Modelo das Três Linhas do IIA 2020**: Uma atualização das Três Linhas de Defesa. 2020. Disponível em: https://iiabrasil.org.br/noticia/novo-modelo-das-tres-linhas-do-iia-2020. Acesso em: 28 jan. 2021.

THE INTERNATIONAL ORGANIZATION OF SUPREME AUDIT INSTITUTIONS (INTOSAI). **Guidelines for Internal Control Standards for the Public Sector**. 2020. Disponível em: https://www.issai.org/pronouncements/endorsed-as-intosai-gov-9100/. Acesso em: 28 jan. 2021.

Anexos

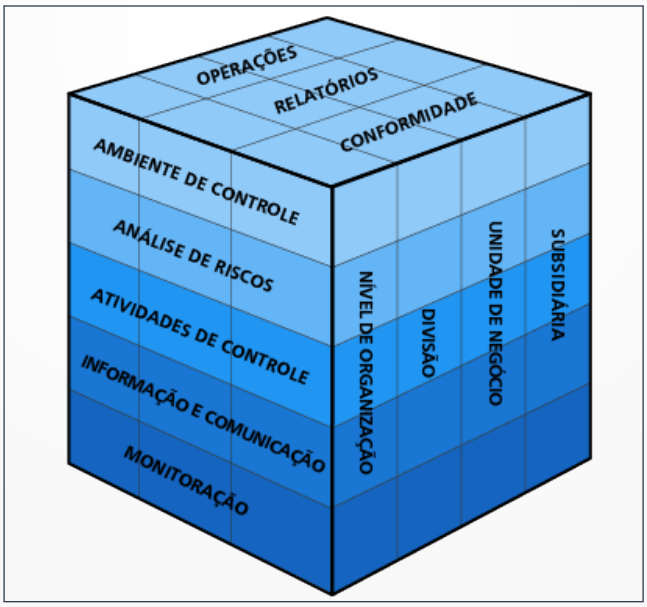
1. Referencial Teórico

Apresentam-se neste anexo as estruturas de gerenciamento de riscos mundialmente reconhecidas e que têm sido base para a implementação da gestão de riscos na maior parte das organizações em todo o mundo. A maioria dessas normas apresenta mais semelhanças que diferenças e é aplicável a qualquer tipo de organização, observando eventual necessidade de adaptação às suas características, atividades e cultura.

1. 1 COSO e COSO GRC/COSO II

O COSO (*The Committee of Sponsoring Organizations of the Treadway Commission* – Comitê das Organizações Patrocinadoras) é uma entidade sem fins lucrativos dedicada à melhoria dos relatórios financeiros por meio da ética, efetividade dos controles internos e governança corporativa. Criada em 1985, sua origem está relacionada a um grande número de escândalos financeiros na década de 70 nos Estados Unidos, que colocaram em dúvida a confiabilidade dos relatórios corporativos. Em 1992, o COSO publicou um trabalho denominado Controle Interno: um modelo integrado (COSO I), revisado em 2013.

O COSO I tornou-se referência por auxiliar as organizações a avaliar e aperfeiçoar seus sistemas de controle interno, sendo essa estrutura incorporada em políticas, normas e regulamentos adotados por milhares de organizações para controlar melhor suas atividades visando o cumprimento dos objetivos estabelecidos (TCU, 2009).



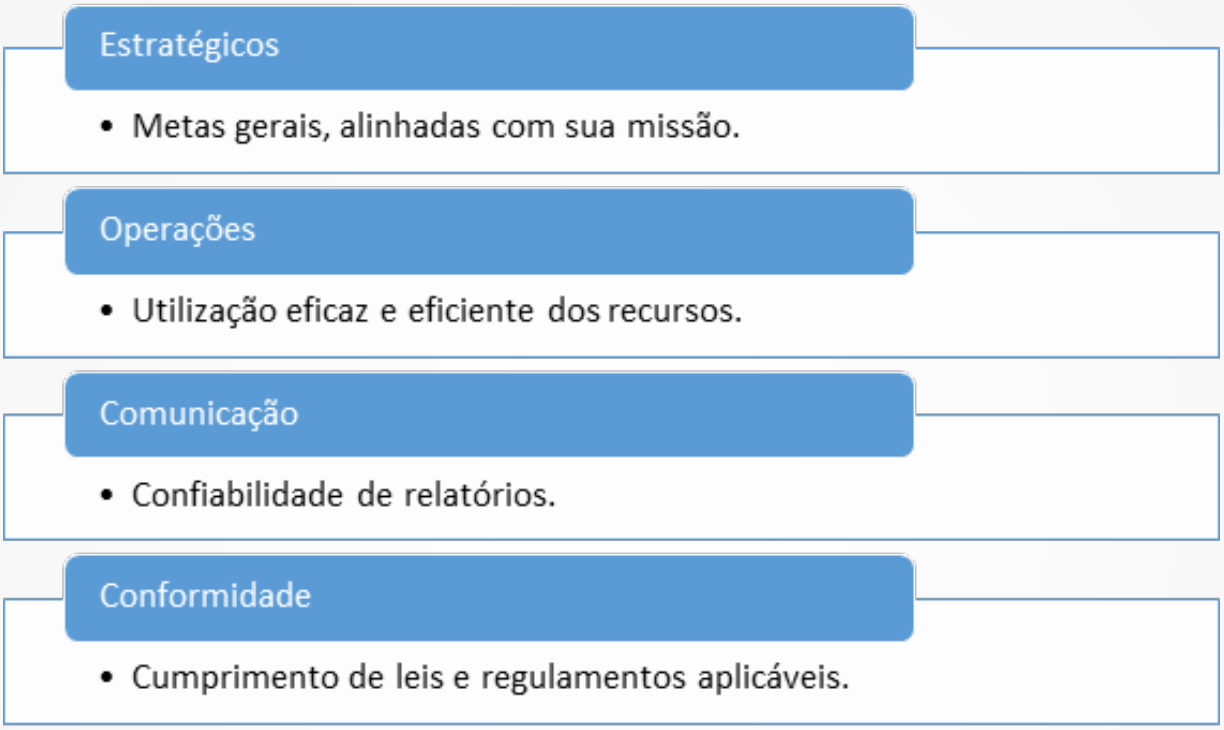
Fonte: COSO

Em 2004, a preocupação com riscos se intensificou. Tal fato se deve à crise ocorrida no início dos anos 2000, quando foram descobertas manipulações contábeis em diversas empresas, tais como Enron, Worldcom, Xerox, Parmalat (Itália). Naquele momento, o COSO divulgou o trabalho Enterprise Risk Management – Integrated Framework (Gerenciamento de Riscos Corporativos – Estrutura Integrada), também conhecido como COSO ERM, COSO GRC ou COSO II, com um foco mais voltado para o gerenciamento de riscos corporativos.

O COSO ERM define o termo risco como: Processo conduzido em uma organização pelo conselho de administração, diretoria e demais empregados, aplicado no estabelecimento de estratégias, formuladas para identificar em toda a organização eventos em potencial, capazes de afetá-la, e administrar os riscos de modo a mantê-los compatível com o apetite a risco da organização e possibilitar garantia razoável do cumprimento dos seus objetivos.

De acordo com o COSO GRC, com base na missão ou visão estabelecida por uma organização, a administração estabelece os planos principais, seleciona as estratégias e determina o alinhamento dos objetivos nos níveis da organização.

Essa estrutura de gerenciamento de riscos é orientada a fim de alcançar os objetivos de uma organização e são classificados em quatro categorias:

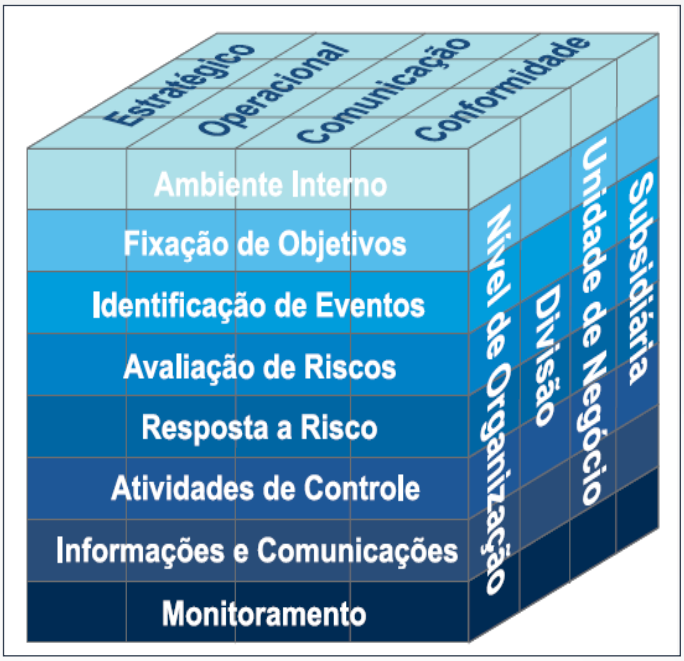


Fonte: COSO

Um avanço da estrutura do COSO GRC em relação ao COSO I, que tinha como enfoque os controles internos de uma organização, é justamente a categoria de objetivos estratégicos.

A lógica por trás dessa inclusão é que, em se tratando de atingimento de objetivos de uma organização, de nada adiantaria as operações serem eficientes, os relatórios confiáveis e leis e regulamentos serem cumpridos, se não há uma estratégia a ser alcançada, ou seja, se a organização não sabe onde quer chegar.

A figura a seguir ficou conhecida como Cubo do Coso. A dimensão superior apresenta os objetivos que devem ser objeto do gerenciamento de risco, conforme abordado anteriormente. Já a dimensão lateral representa os níveis da organização por onde perpassam a gestão de riscos. Por fim, a dimensão frontal apresenta os oito componentes do gerenciamento de riscos, que serão abordados de forma sucinta a seguir, representando o que é necessário fazer, de forma integrada, para atingir os objetivos elencados na face superior.



Fonte: COSO (2004)

1.1.1. Ambiente Interno

O ambiente interno é moldado pela história e cultura da organização e, por sua vez, molda, de maneira explícita ou não, a cultura de gestão dos riscos da organização e a forma como eles são encarados e gerenciados (tom da organização), influenciando a consciência de controle das pessoas (TCU, 2009).

Segundo o COSO GRC, esse componente fornece a base pela qual os riscos são identificados e abordados pelo seu pessoal, sendo o alicerce para os demais. Integridade, valores éticos e competência dos colaboradores (funcionários, servidores, etc.) são alguns dos fatores que compõem o Ambiente Interno. Além deles, a forma como a gestão delega autoridade e responsabilidades, define seu apetite a riscos, bem como posiciona sua estrutura de governança e define as políticas e práticas de recursos humanos também fazem parte desse componente.

1.1.2 Fixação de objetivos

A estrutura do COSO GRC requer que todos os níveis da organização tenham objetivos fixados e comunicados (estratégicos, operacionais, comunicação e conformidade), antes da identificação dos eventos que possam influenciar em seu atingimento.

Os objetivos estratégicos devem estar alinhados à missão da entidade e devem ser compatíveis com o apetite a riscos. Tais objetivos são metas de nível geral, alinhadas com a missão/visão da organização e fornecendo-lhe apoio. Devem refletir como a alta administração escolheu uma forma de gerar valor para as partes interessadas que, na esfera pública em última instância, é a sociedade.

1.1.3 Identificação de eventos

Eventos são situações em potencial – que ainda não ocorreram – que podem causar impacto na consecução dos objetivos da organização, caso venham a ocorrer.

Podem ser positivos ou negativos, sendo que a estrutura do COSO GRC denomina os eventos negativos como riscos, enquanto os positivos são chamados de oportunidades.

Por meio da identificação de eventos, pode-se planejar o tratamento adequado para as oportunidades e para os riscos, devendo ser entendidos como parte de um contexto, e não de forma isolada, já que muitas vezes um risco que parece trazer grande impacto pode ser minimizado pela existência conjunta de uma oportunidade.

Após a identificação de eventos, a organização atua sobre os riscos, avaliando-os e determinando a forma de tratamento para cada evento identificado e qual o tipo de resposta a ser dada a esse risco.

1.1.4 Avaliação de Riscos

Os eventos identificados no componente anterior, externos e internos, devem ser avaliados sob a perspectiva de probabilidade e impacto de sua ocorrência. Essa avaliação é justificada para que a administração desenvolva estratégias para dar resposta aos riscos, ou seja, como os riscos serão administrados, de modo a diminuir a probabilidade de ocorrência e/ou a magnitude do impacto.

Os riscos devem ser avaliados quanto a sua condição de inerentes e residuais. Entende-se por risco inerente aquele que uma organização terá de enfrentar na falta de medidas que a administração possa adotar para alterar a probabilidade ou o impacto dos eventos. Já o risco residual é aquele que ainda permanece após a resposta da administração (COSO, 2004).

1.1.5 Resposta a riscos

Para cada risco identificado será prevista uma resposta. A escolha dependerá do nível de exposição a riscos previamente estabelecido pela organização em confronto com a avaliação que se fez do risco e pode ser de 4 tipos: evitar, aceitar, compartilhar ou reduzir. A administração deve obter uma visão dos riscos em toda organização e desenvolver ações concretas para manter o nível de riscos residuais alinhado aos níveis de tolerância e apetite a riscos da organização.

De acordo com o COSO (2004), “Evitar” sugere que nenhuma opção de resposta tenha sido identificada para reduzir o impacto e a probabilidade a um nível aceitável. “Reduzir” ou “Compartilhar” reduzem o risco residual a um nível compatível com as tolerâncias desejadas ao risco, enquanto “Aceitar” indica que o risco inerente já esteja dentro das tolerâncias ao risco.

Ao analisar as respostas, a administração poderá considerar eventos e tendências anteriores, e o potencial de situações futuras (COSO, 2004).

É importante que se tenha consciência que sempre existirá algum nível de risco residual,

não somente porque os recursos são limitados, mas também em decorrência da incerteza e das limitações inerentes a todas as atividades de uma organização.

1.1.6 Atividades de controle

Segundo o COSO GRC, ao selecionar as respostas aos riscos, a administração identifica as atividades de controle necessárias para assegurar que estas sejam executadas de forma adequada e oportuna.

Essas atividades contribuem para assegurar que os objetivos sejam alcançados, que as diretrizes administrativas sejam cumpridas e que as ações necessárias para gerenciar os riscos com vistas ao atingimento dos objetivos da entidade estejam sendo implementadas.

Ao selecionar as atividades de controle, a administração deve levar em consideração a forma como essas atividades se relacionam entre si. Há situações em que uma única atividade de controle aborda diversas respostas a riscos. Em outras, diversas atividades de controle são necessárias para dar resposta a apenas um risco. E, ainda, há aquelas situações em que a administração poderá constatar que as atividades de controle existentes são suficientes para assegurar a execução eficaz das novas respostas a riscos (COSO, 2004).

1.1.7 Informação e Comunicação

Esse componente abrange informações e sistemas de comunicação, permitindo que as pessoas da organização coletem e troquem informações necessárias para conduzir, gerenciar e controlar suas operações. É importante que toda a informação relevante, relacionada aos objetivos – riscos – controles, sejam capturadas tempestivamente e comunicadas por toda a organização.

A organização também deve possuir mecanismos para coletar informações do ambiente externo que possam afetá-la, e deve transmitir externamente aquelas que sejam relevantes aos stakeholders, inclusive à sociedade, que, no caso das organizações públicas, pode ser considerada a principal parte interessada.

A comunicação deverá ser oportuna e adequada, além de abordar aspectos financeiros, econômicos, operacionais e estratégicos. Deve ser entendida como um canal que movimenta as informações em todas as direções – dos superiores aos subordinados, e vice-versa – pois determinados assuntos são mais bem visualizados pelos integrantes dos níveis mais subordinados (COSO, 2004). A habilidade da administração de tomar decisões apropriadas é afetada pela qualidade da informação, que deve ser útil, isto é, apropriada, tempestiva, atual e precisa.

1.1.8 Monitoramento

Monitorar diz respeito a avaliar, certificar e revisar a estrutura de gestão de riscos e controles internos para saber se estão sendo efetivos ou não. Tem, portanto, o objetivo de avaliar a qualidade da gestão de risco e dos controles internos ao longo do tempo, buscando assegurar que estes funcionam como previsto e que são modificados apropriadamente, de acordo com mudanças nas condições que alterem o nível de exposição a riscos (TCU, 2009).

O processo completo de riscos e controles deve ser monitorado e modificações devem ser feitas para o seu aprimoramento. Assim, a estrutura de controle interno pode "reagir" de forma dinâmica, ajustando-se conforme as condições o determinem. O monitoramento pode ser realizado por meio de:

As atividades contínuas são incorporadas as demais atividades normais da organização e as avaliações independentes, realizadas por auditores internos e ou externos, garantem a eficácia do gerenciamento dos riscos ao longo do tempo. Modernamente também são utilizadas as autoavaliações, processo que pode ter um grande auxílio dos auditores.

O monitoramento contínuo ocorre no decurso normal das atividades de administração. O alcance e a frequência das avaliações independentes dependerão basicamente de uma avaliação dos riscos e da eficácia dos procedimentos contínuos de monitoramento.

Diferentemente das atividades de controle, que são concebidas para dar cumprimento aos processos e políticas da organização e visam tratar os riscos, as de monitoramento objetivam identificar fragilidades e possibilidades de melhorias (BRASIL, 2017).

1.2 COSO 2017 – Integração com Estratégia e Desempenho

Em 2017 ocorreu a revisão do COSO ERM: *Enterprise Risk Management: Integrating with Strategy and Performance* (COSO, 2017), que estabelece que o gerenciamento de riscos corporativos "não é uma função ou departamento. É a cultura, os recursos e as práticas que as organizações integram com a estratégia definida e executada, com o objetivo de gerenciar o risco na criação, preservação e valorização" (tradução livre).

De maneira geral, o novo modelo passa a integrar o gerenciamento de riscos com outros processos da organização, tais como governança, definição da estratégia, definição dos objetivos e gestão do desempenho. O novo modelo explora a gestão da estratégia e dos riscos a partir de três perspectivas, quais sejam:

- Possibilidade de os objetivos estratégicos e de negócios não se alinharem com a missão, a visão e os valores fundamentais da organização;
- As implicações da estratégica escolhida;
- Os riscos na execução da estratégia.

Fonte: COSO (2017)

Um ponto importante atualizado no documento é o refinamento entre apetite a riscos e tolerância a riscos, agora com enfoque na variação aceitável do desempenho.

A primeira parte da publicação oferece uma perspectiva dos conceitos atuais e em desenvolvimento e aplicações do gerenciamento de riscos corporativos. A segunda parte da publicação apresenta 20 princípios organizados em 5 componentes inter-relacionados: Governança e cultura, Estratégia e definição de objetivos, Performance, Monitoramento do desempenho e revisão; e finalmente Informação, comunicação e divulgação.

Aderir a estes princípios pode conferir a organização uma razoável expectativa de que ela entende e se esforça para gerenciar os riscos associados à sua estratégia e objetivos de negócios.

Fonte: COSO Enterprise Risk Management – Integrating with Strategy and Performance (COSO, 2017 – tradução livre).

1.2.1 Governança e Cultura (fornece a base para os demais componentes)

1. Exercita a Supervisão de Riscos pelo Conselho – A alta administração supervisiona a estratégia e executa responsabilidades de governança para apoiar a gestão na consecução da estratégia e dos objetivos de negócios.
2. Estabelece Estruturas Operacionais – A organização estabelece estruturas operacionais na busca de objetivos estratégicos e de negócios.
3. Define Cultura Desejada – A organização define os comportamentos desejados que

caracterizam a cultura desejada pela entidade.

4. Demonstra Compromisso com Valores Fundamentais – A organização demonstra compromisso com os valores fundamentais da entidade.
5. Atrai, Desenvolve e Mantém Indivíduos Capazes – A organização está empenhada em construir capital humano em alinhamento com a estratégia e os objetivos de negócios.

1.2.2 Estratégia e Definição de Objetivos

6. Analisa o Contexto de Negócio – A organização considera os potenciais efeitos do contexto dos negócios no perfil de risco.
7. Define o Apetite ao Risco – A organização define o apetite a riscos no contexto de criação, preservação e realização de valor.
8. Avalia Estratégias Alternativas – A organização avalia estratégias alternativas e potencial impacto sobre o perfil de risco.
9. Elabora Objetivos de Negócios – A organização considera o risco ao estabelecer os objetivos de negócios em vários níveis que alinham e apoiam a estratégia.

1.2.3 Desempenho

10. Identifica Riscos – A organização identifica o risco que afeta o desempenho da estratégia e dos objetivos de negócios.
11. Avalia a Severidade do Risco – A organização avalia a gravidade do risco.
12. Prioriza Riscos – A organização prioriza os riscos como base para a seleção das respostas aos riscos.
13. Implementa Respostas a Riscos – A organização identifica e seleciona respostas a riscos.
14. Desenvolve Visão de Portfólio – A organização desenvolve e avalia uma visão de portfólio de risco

1.2.4 Revisão

15. Avalia Mudanças Substanciais – A organização identifica e avalia mudanças que podem afetar substancialmente a estratégia e os objetivos de negócios.
16. Revê Riscos e Desempenho – A organização revê o desempenho da entidade e considera o risco.
17. Persegue a Melhoria no Gerenciamento de Riscos Corporativos – A organização busca a melhoria do gerenciamento de riscos corporativos

1.2.5 Informação, Comunicação e Divulgação

18. Aproveita a Informação e a Tecnologia – A organização aproveita os sistemas de tecnologia da informação da entidade para apoiar a gestão de riscos corporativos.
19. Comunica Informações de Risco – A organização usa canais de comunicação para suportar o gerenciamento de riscos corporativos.
20. Reporta sobre Risco, Cultura e Desempenho – A organização informa sobre risco, cultura e desempenho em vários níveis e em toda a entidade.

1.3 ISO 31000

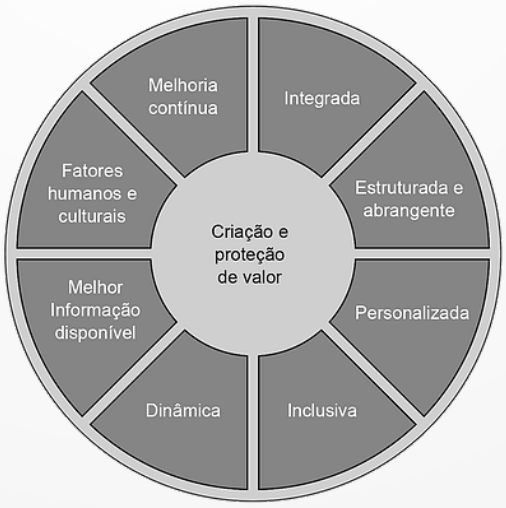
A ABNT NBR ISO 31000 foi elaborada pela Comissão de Estudo Especial de Gestão de Riscos, sendo uma adoção idêntica, em conteúdo técnico, estrutura e redação, à ISO 31000:2018, preparada pelo *Technical Commitee risk management*, conforme ISO/IEC Guide 21–1:2005.

A ISO 31000 tem talvez a mais simples definição de riscos dentre todas as outras normas e estruturas de gestão de riscos. Segundo ela, risco é o "efeito da incerteza nos objetivos". Esse efeito é um desvio em relação ao esperado, podendo ser positivo ou negativo.

Essa é uma das diferenças entre essa norma e o COSO GRC, já que este considera risco apenas como algo negativo, chamando de oportunidade quando o evento é positivo.

Segundo essa norma o propósito da gestão de riscos é a criação e proteção de valor. Ela melhora o desempenho, encoraja a inovação e apoia o alcance de objetivos.

Os princípios, descritos na Figura a seguir, são a base para gerenciar riscos e convém que sejam considerados quando se estabelecerem a estrutura e os processos de gestão de riscos da organização. Convém que estes princípios possibilitem uma organização a gerenciar os efeitos da incerteza nos seus objetivos.



Fonte: ABNT NBR ISO 31000

a) Integrada

A gestão de riscos é parte integrante de todas as atividades organizacionais.

b) Estruturada e abrangente

Uma abordagem estruturada e abrangente para a gestão de riscos contribui para resultados consistentes e comparáveis.

c) Personalizada

A estrutura e o processo de gestão de riscos são personalizados e proporcionais aos contextos externo e interno da organização relacionados aos seus objetivos.

d) Inclusiva

O envolvimento apropriado e oportuno das partes interessadas possibilita que seus conhecimentos, pontos de vista e percepções sejam considerados. Isto resulta em melhor conscientização e gestão de riscos fundamentada.

e) Dinâmica

Riscos podem emergir, mudar ou desaparecer à medida que os contextos externo e interno de uma organização mudem. A gestão de riscos antecipa, detecta, reconhece e responde a estas mudanças e eventos de uma maneira apropriada e oportuna.

f) Melhor informação disponível

As entradas para a gestão de riscos são baseadas em informações históricas e atuais, bem como em expectativas futuras. A gestão de riscos explicitamente leva em consideração quaisquer limitações e incertezas associadas a estas informações e expectativas. Convém que a informação seja oportuna, clara e disponível para as partes interessadas pertinentes.

g) Fatores humanos e culturais

O comportamento humano e a cultura influenciam significativamente todos os aspectos da gestão de riscos em cada nível e estágio.

h) Melhoria contínua

A gestão de riscos é melhorada continuamente por meio do aprendizado e experiências.

O propósito da estrutura da gestão de riscos é apoiar a organização na integração da gestão de riscos em atividades significativas e funções. A eficácia da gestão de riscos dependerá da sua integração na governança e em todas as atividades da organização, incluindo a tomada de decisão. Isto requer apoio das partes interessadas, em particular da Alta Direção.

O desenvolvimento da estrutura engloba integração, concepção, implementação, avaliação e melhoria da gestão de riscos através da organização. A Figura a seguir ilustra os componentes de uma estrutura.

Fonte: ABNT NBR ISO 31000

Convém que a organização avalie suas práticas e processos existentes de gestão de riscos, avalie quaisquer lacunas e aborde estas lacunas no âmbito da estrutura.

Convém que os componentes da estrutura e o modo como funcionam em conjunto sejam personalizados para as necessidades da organização.

Liderança e comprometimento

Convém que a Alta Direção e os órgãos de supervisão, onde aplicável, assegurem que a gestão de riscos esteja integrada em todas as atividades da organização.

Integração

A integração da gestão de riscos apoia-se em uma compreensão das estruturas e do contexto organizacional. Estruturas diferem, dependendo do propósito, metas e complexidade da organização. O risco é gerenciado em todas as partes da estrutura da organização. Todos na organização têm responsabilidade por gerenciar riscos.

Integrar a gestão de riscos em uma organização é um processo dinâmico e iterativo, e convém que seja personalizado para as necessidades e cultura da organização.

Convém que a gestão de riscos seja uma parte, e não separada, do propósito organizacional, governança, liderança e comprometimento, estratégia, objetivos e operações.

Concepção

Entendendo a organização e seu contexto

Ao conceber a estrutura para gerenciar riscos, convém que a organização examine e entenda seus contextos externo e interno.

Articulando o comprometimento com a gestão de riscos

Convém que a Alta Direção e os órgãos de supervisão, onde aplicável, demonstrem e articulem o seu comprometimento contínuo com a gestão de riscos por meio de uma política, uma declaração ou outras formas que claramente transmitam os objetivos e o comprometimento com a gestão de riscos de uma organização.

Convém que o comprometimento com a gestão de riscos seja comunicado na organização e às partes interessadas, como apropriado.

Atribuindo papéis organizacionais, autoridades, responsabilidades e responsabilizações

Convém que a Alta Direção e os órgãos de supervisão, onde aplicável, assegurem que as autoridades, responsabilidades e responsabilizações para os papéis pertinentes à gestão de riscos sejam atribuídas e comunicadas a todos os níveis da organização.

Alocando recursos

Convém que a Alta Direção e os órgãos de supervisão, onde aplicável, assegurem a alocação de recursos apropriados para a gestão de riscos. Convém que a organização considere as capacidades e restrições dos recursos existentes.

Estabelecendo comunicação e consulta

Convém que a organização estabeleça uma abordagem aprovada para comunicação e consulta para apoiar a estrutura e facilitar a aplicação eficaz da gestão de riscos. Comunicação envolve compartilhar informação com públicos-alvo. A consulta também envolve o fornecimento de retorno pelos participantes, com a expectativa de que isto contribuirá para as decisões e sua formulação ou outras atividades. Convém que os métodos e conteúdo da comunicação e consulta reflitam as expectativas das partes interessadas, onde for pertinente.

Convém que a comunicação e a consulta sejam oportunas e assegurem que a informação pertinente seja coletada, consolidada, sintetizada e compartilhada, como apropriado, e que o retorno seja fornecido e as melhorias sejam implementadas.

Implementação

Convém que a organização implemente a estrutura de gestão de riscos por meio de:

- desenvolvimento de um plano apropriado, incluindo prazos e recursos;
- identificação de onde, quando e como diferentes tipos de decisões são tomadas pela organização, e por quem;
- modificação dos processos de tomada de decisão aplicáveis, onde necessário;
- garantia de que os arranjos da organização para gerenciar riscos sejam claramente compreendidos e praticados.

A implementação bem-sucedida da estrutura requer o engajamento e a conscientização das partes interessadas. Isso permite que as organizações abordem explicitamente a incerteza

na tomada de decisão, enquanto também asseguram que qualquer incerteza nova ou posterior possa ser levada em consideração à medida que ela surja.

Adequadamente concebida e implementada, a estrutura de gestão de riscos assegurará que o processo de gestão de riscos é parte de todas as atividades da organização, incluindo a tomada de decisão, e que as mudanças nos contextos externo e interno serão adequadamente capturadas.

Avaliação

Para avaliar a eficácia da estrutura de gestão de riscos, convém que a organização:

- mensure periodicamente o desempenho da estrutura de gestão de riscos em relação ao seu propósito, planos de implementação, indicadores e comportamento esperado;
- determine se permanece adequada para apoiar o alcance dos objetivos da organização

Melhoria

Adaptação

Convém que a organização monitore e adapte continuamente a estrutura de gestão de riscos para abordar as mudanças externas e internas. Ao fazer isso, a organização pode melhorar seu valor.

Melhoria contínua

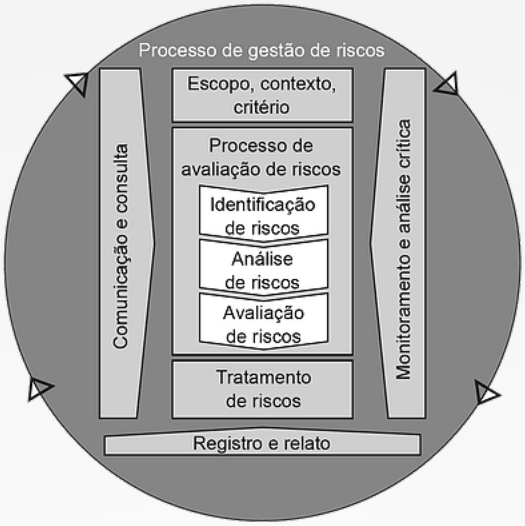
Convém que organização melhore continuamente a adequação, suficiência e eficácia da estrutura de gestão de riscos e a forma como o processo de gestão de riscos é integrado.

À medida que lacunas ou oportunidades de melhoria pertinentes são identificadas, convém que a organização desenvolva planos e tarefas e os atribua àqueles responsabilizados pela implementação.

Uma vez implementadas, convém que estas melhorias contribuam para o aprimoramento da gestão de riscos.

Processo

O processo de gestão de riscos envolve a aplicação sistemática de políticas, procedimentos e práticas para as atividades de comunicação e consulta, estabelecimento do contexto e avaliação, tratamento, monitoramento, análise crítica, registro e relato de riscos. Este processo é ilustrado na Figura a seguir:



Fonte: ABNT NBR ISO 31000

Convém que o processo de gestão de riscos seja parte integrante da gestão e da tomada de decisão, e seja integrado na estrutura, operações e processos da organização. Pode ser aplicado nos níveis estratégico, operacional, de programas ou de projetos.

Comunicação e consulta

O propósito da comunicação e consulta é auxiliar as partes interessadas pertinentes na compreensão do risco, na base sobre a qual decisões são tomadas e nas razões pelas quais ações específicas são requeridas. A comunicação busca promover a conscientização e o entendimento do risco, enquanto a consulta envolve obter retorno e informação para auxiliar a tomada de decisão. Convém que uma coordenação estreita entre as duas facilite a troca de informações factuais, oportunas, pertinentes, precisas e compreensíveis, levando em consideração a confidencialidade e integridade da informação, bem como os direitos de privacidade dos indivíduos.

Convém que ocorram comunicação e consulta com partes interessadas apropriadas externas e internas, no âmbito de cada etapa e ao longo de todo o processo de gestão de riscos.

Escopo, contexto e critérios

O propósito do estabelecimento do escopo, contexto e critérios é personalizar o processo de gestão de riscos, permitindo um processo de avaliação de riscos eficaz e um tratamento de riscos apropriado.

Escopo, contexto e critérios envolvem a definição do escopo do processo, a compreensão dos contextos externo e interno.

Definindo o escopo

Convém que a organização defina o escopo de suas atividades de gestão de riscos.

Como o processo de gestão de riscos pode ser aplicado em diferentes níveis (por exemplo, estratégico, operacional, programa, projeto ou outras atividades), é importante ser claro sobre o

escopo em consideração, os objetivos pertinentes a serem considerados e o seu alinhamento aos objetivos organizacionais.

Contextos externo e interno

Os contextos externo e interno são o ambiente no qual a organização procura definir e alcançar seus objetivos.

Convém que o contexto do processo de gestão de riscos seja estabelecido a partir da compreensão dos ambientes externo e interno no qual a organização opera, e convém que reflita o ambiente específico da atividade ao qual o processo de gestão de riscos é aplicado.

Definindo critérios de risco

Convém que a organização especifique a quantidade e o tipo de risco que podem ou não assumir em relação aos objetivos. Convém também que estabeleça critérios para avaliar a significância do risco e para apoiar os processos de tomada de decisão. Convém que os critérios de risco sejam alinhados à estrutura de gestão de riscos e sejam personalizados para o propósito específico e o escopo da atividade em consideração. Convém que os critérios de risco reflitam os valores, objetivos e recursos da organização e sejam consistentes com as políticas e declarações sobre gestão de riscos. Convém que os critérios de risco sejam estabelecidos levando em consideração as obrigações da organização e os pontos de vista das partes interessadas.

Embora convenha que os critérios de risco sejam estabelecidos no início do processo de avaliação de riscos, eles são dinâmicos; e convém que sejam continuamente analisados criticamente e alterados, se necessário.

Processo de avaliação de riscos

O processo de avaliação de riscos é o processo global de identificação de riscos, análise de riscos e avaliação de riscos.

Convém que o processo de avaliação de riscos seja conduzido de forma sistemática, iterativa e colaborativa, com base no conhecimento e nos pontos de vista das partes interessadas. Convém que use a melhor informação disponível, complementada por investigação adicional, como necessário.

Identificação de riscos

O propósito da identificação de riscos é encontrar, reconhecer e descrever riscos que possam ajudar ou impedir que uma organização alcance seus objetivos. Informações pertinentes, apropriadas e atualizadas são importantes na identificação de riscos.

A organização pode usar uma variedade de técnicas para identificar incertezas que podem afetar um ou mais objetivos. Convém que os seguintes fatores e o relacionamento entre estes fatores sejam considerados:

- fontes tangíveis e intangíveis de risco;
- causas e eventos;

- ameaças e oportunidades;
- vulnerabilidades e capacidades;
- mudanças nos contextos externo e interno;
- indicadores de riscos emergentes;
- natureza e valor dos ativos e recursos;
- consequências e seus impactos nos objetivos;
- limitações de conhecimento e de confiabilidade da informação;
- fatores temporais;
- vieses, hipóteses e crenças dos envolvidos.

Convém que a organização identifique os riscos, independentemente de suas fontes estarem ou não sob seu controle. Convém considerar que pode haver mais de um tipo de resultado, o que pode resultar em uma variedade de consequências tangíveis ou intangíveis.

Análise de riscos

O propósito da análise de riscos é compreender a natureza do risco e suas características, incluindo o nível de risco, onde apropriado. A análise de riscos envolve a consideração detalhada de incertezas, fontes de risco, consequências, probabilidade, eventos, cenários, controles e sua eficácia. Um evento pode ter múltiplas causas e consequências e pode afetar múltiplos objetivos.

A análise de riscos pode ser realizada com vários graus de detalhamento e complexidade, dependendo do propósito da análise, da disponibilidade e confiabilidade da informação, e dos recursos disponíveis.

As técnicas de análise podem ser qualitativas, quantitativas ou uma combinação destas, dependendo das circunstâncias e do uso pretendido.

Convém que a análise de riscos considere fatores como:

- a probabilidade de eventos e consequências;
- a natureza e magnitude das consequências;
- complexidade e conectividade;
- fatores temporais e volatilidade;
- a eficácia dos controles existentes;
- sensibilidade e níveis de confiança.

A análise de riscos pode ser influenciada por qualquer divergência de opiniões, vieses, percepções do risco e julgamentos. Influências adicionais são a qualidade da informação utilizada, as hipóteses e as exclusões feitas, quaisquer limitações das técnicas e como elas são executadas.

Convém que estas influências sejam consideradas, documentadas e comunicadas aos

tomadores de decisão.

Avaliação de riscos

O propósito da avaliação de riscos é apoiar decisões. A avaliação de riscos envolve a comparação dos resultados da análise de riscos com os critérios de risco estabelecidos para determinar onde é necessária ação adicional. Isto pode levar a uma decisão de:

- fazer mais nada;
- considerar as opções de tratamento de riscos;
- realizar análises adicionais para melhor compreender o risco;
- manter os controles existentes;
- reconsiderar os objetivos.

Convém que as decisões levem em consideração o contexto mais amplo e as consequências reais e percebidas para as partes interessadas externas e internas.

Convém que o resultado da avaliação de riscos seja registrado, comunicado e então validado nos níveis apropriados da organização.

Tratamento de riscos

O propósito do tratamento de riscos é selecionar e implementar opções para abordar riscos.

O tratamento de riscos envolve um processo iterativo de:

- formular e selecionar opções para tratamento do risco;
- planejar e implementar o tratamento do risco;
- avaliar a eficácia deste tratamento;
- decidir se o risco remanescente é aceitável;
- se não for aceitável, realizar tratamento adicional

Seleção de opções de tratamento de riscos

Selecionar a(s) opção(ões) mais apropriada(s) de tratamento de riscos envolve balancear os benefícios potenciais derivados em relação ao alcance dos objetivos, face aos custos, esforço ou desvantagens da implementação.

As opções de tratamento de riscos não são necessariamente mutuamente exclusivas ou apropriadas em todas as circunstâncias.

A justificativa para o tratamento de riscos é mais ampla do que apenas considerações econômicas, e convém que leve em consideração todas as obrigações da organização, compromissos voluntários e pontos de vista das partes interessadas. Convém que a seleção de opções de tratamento de riscos seja feita de acordo com os objetivos da organização, critérios de risco e recursos disponíveis.

Ao selecionar opções de tratamento de riscos, convém que a organização considere os valores, percepções e potencial envolvimento das partes interessadas, e as formas mais apropriadas para com elas se comunicar e consultar. Embora igualmente eficazes, alguns tratamentos de riscos podem ser mais aceitáveis para algumas partes interessadas do que para outras.

Monitoramento e análise crítica precisam ser parte integrante da implementação do tratamento de riscos, para assegurar que as diferentes formas de tratamento se tornem e permaneçam eficazes.

O tratamento de riscos também pode introduzir novos riscos que precisem ser gerenciados.

Se não houver opções de tratamento disponíveis ou se as opções de tratamento não modificarem suficientemente o risco, convém que este seja registrado e mantido sob análise crítica contínua.

Convém que os tomadores de decisão e outras partes interessadas estejam conscientes da natureza e extensão do risco remanescente após o tratamento de riscos. Convém que o risco remanescente seja documentado e submetido a monitoramento, análise crítica e, onde apropriado, tratamento adicional.

Preparando e implementando planos de tratamento de riscos

O propósito dos planos de tratamento de riscos é especificar como as opções de tratamento escolhidas serão implementadas de maneira que os arranjos sejam compreendidos pelos envolvidos, e o progresso em relação ao plano possa ser monitorado. Convém que o plano de tratamento identifique claramente a ordem em que o tratamento de riscos será implementado.

Convém que os planos de tratamento sejam integrados nos planos e processos de gestão da organização, em consulta com as partes interessadas apropriadas.

Monitoramento e análise crítica

O propósito do monitoramento e análise crítica é assegurar e melhorar a qualidade e eficácia da concepção, implementação e resultados do processo. Convém que o monitoramento contínuo e a análise crítica periódica do processo de gestão de riscos e seus resultados sejam uma parte planejada do processo de gestão de riscos, com responsabilidades claramente estabelecidas.

Convém que monitoramento e análise crítica ocorram em todos os estágios do processo. Monitoramento e análise crítica incluem planejamento, coleta e análise de informações, registro de resultados e fornecimento de retorno.

Convém que os resultados do monitoramento e análise crítica sejam incorporados em todas as atividades de gestão de desempenho, medição e relatos da organização.

Registro e relato

Convém que o processo de gestão de riscos e seus resultados sejam documentados e relatados por meio de mecanismos apropriados. O registro e o relato visam:

- comunicar atividades e resultados de gestão de riscos em toda a organização;
- fornecer informações para a tomada de decisão;
- melhorar as atividades de gestão de riscos;
- auxiliar a interação com as partes interessadas, incluindo aquelas com responsabilidade e com responsabilização por atividades de gestão de riscos.

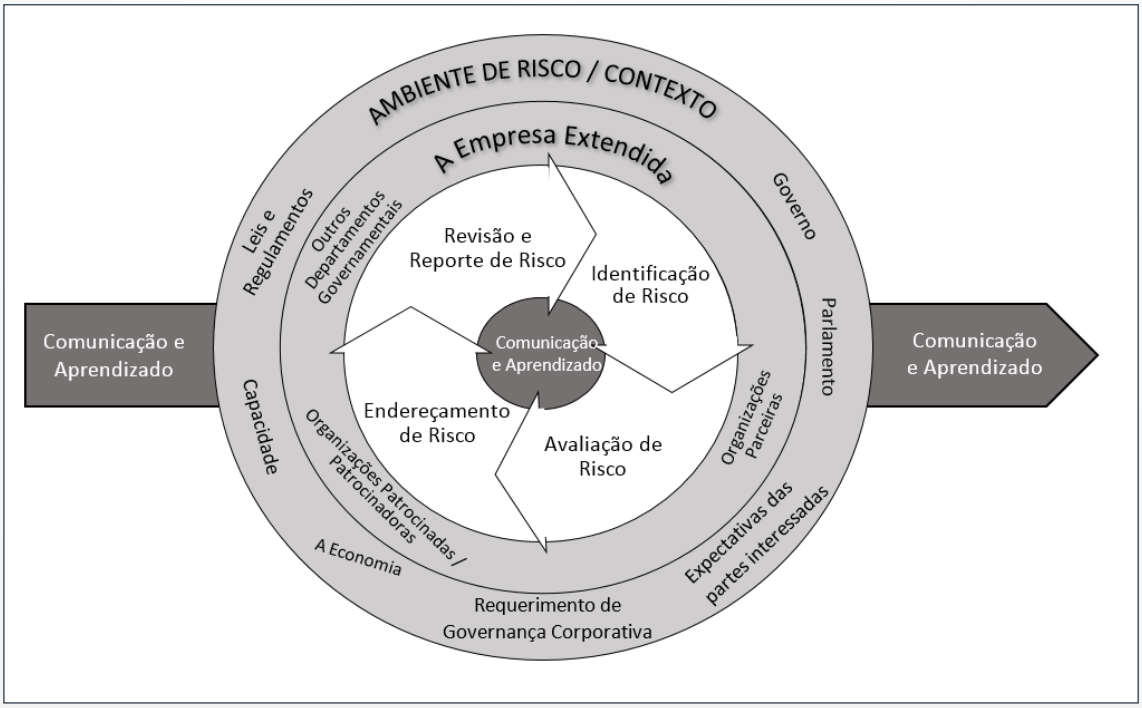
Convém que as decisões relativas à criação, retenção e manuseio de informação documentada levem em consideração, mas não se limitem a, o seu uso, a sensibilidade da informação e os contextos externo e interno.

O relato é parte integrante da governança da organização e convém que melhore a qualidade do diálogo com as partes interessadas e apoie a Alta Direção e os órgãos de supervisão a cumprirem suas responsabilidades.

1.4 *Orange Book*

O documento *The Orange Book Management of Risk – Principles and Concepts* (Gerenciamento de Riscos – Princípios e Conceitos) foi produzido e publicado pelo *HM Treasury* do Governo Britânico (UK, 2004), sendo amplamente utilizado como a principal referência do Programa de Gerenciamento de Riscos do Governo do Reino Unido, iniciado em 2001. O modelo foi atualizado em 2004 e tem como vantagens, além de ser compatível com padrões internacionais de gerenciamento de riscos, como COSO GRC e ISO 31000.

Segundo o documento, mais importante que uma organização seguir qualquer norma ou estrutura de risco em particular é sua habilidade em demonstrar que os riscos são gerenciados, com suas particularidades e de uma maneira que efetivamente suporta a entrega de seus objetivos (UK, 2004). O modelo de gerenciamento de riscos do *Orange Book* é ilustrado a seguir:



https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/866117/6.6266_HMT_Orange_Book_Update_v6_WEB.PDF

A gestão do risco não é um processo linear, mas o equilíbrio de uma série de elementos entrelaçados que interagem uns com os outros e que devem estar em equilíbrio para que a gestão de risco seja efetiva.

Além disso, os riscos específicos não podem ser abordados isoladamente um do outro, pois a gestão de um risco pode ter impacto em outro, e podem ser desenvolvidas ações efetivas que controlem mais de um risco simultaneamente (Ibidem, 2004).

Nenhuma organização é inteiramente autônoma, apresentando uma série de interdependências com outras organizações. O modelo chama essas interdependências de "empresa / organização estendida" e impactam a gestão de risco da organização, dando origem a certos riscos adicionais que precisam ser gerenciados.

O modelo funciona em um ambiente em que o apetite de risco tenha sido definido e esse conceito perpassa toda sua estrutura. Ele divide o processo central de gerenciamento de risco em elementos (identificação, avaliação, resposta e monitoramento) para fins ilustrativos, em consonância com o que vimos em outras estruturas de riscos. Além disso, o modelo ilustra como o processo central de gerenciamento de riscos não é algo isolado, mas que ocorre em um contexto.

O Projeto de Desenvolvimento do Guia de Orientação para o Gerenciamento de Riscos do GesPública, afirma que uma das vantagens do *Orange Book* é tratar riscos de forma simples, sendo que estes devem ser gerenciados em três níveis: estratégico, de programas e de projetos e atividades. A organização deve ser capaz de gerenciar riscos em todos eles.

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 políticas e as ações prioritárias de Governo. Ocorre a transformação da estratégia em ações.

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

1.5 O Modelo das Três Linhas

Embora não traga uma proposta de estrutura ao gerenciamento de riscos em uma organização, o modelo das Três Linhas é uma forma simples e eficaz de melhorar a comunicação do gerenciamento de riscos e controle por meio do esclarecimento dos papéis e responsabilidades essenciais de cada um dentro de uma organização, sendo aplicável a qualquer órgão ou entidade – não importando o seu tamanho ou a sua complexidade – ainda que não exista uma estrutura ou sistema formal de gestão de riscos.

As organizações são empreendimentos humanos, operando em um mundo cada vez mais incerto, complexo, interconectado e volátil. Geralmente, elas têm vários stakeholders com interesses diversos, mutáveis e, às vezes, concorrentes. Os *stakeholders* confiam a supervisão organizacional a um órgão de governança, que, por sua vez, delega recursos e autoridade à gestão para tomar as ações apropriadas, incluindo o gerenciamento de riscos (IIA – Modelo de Três Linhas, 2020).

No modelo de Três Linhas, o gestor é a primeira linha no gerenciamento de riscos, as diversas funções de controle de riscos e supervisão de conformidade estabelecidas pela gerência são a segunda linha e a avaliação independente é a terceira. Cada uma dessas três linhas desempenha um papel distinto dentro da estrutura mais ampla de governança da organização.

O modelo de três linhas é organizado em torno de seis princípios:

1. Governança;
2. Papéis dos órgãos de governança;
3. Gestão e os papéis da primeira e da segunda linhas;
4. Papéis da terceira linha;
5. Independência da terceira linha; e
6. Criação e proteção do valor.

Esses princípios são detalhados e explicados no "Novo modelo das Três Linhas do IIA 2020" do Instituto de Auditores Internos (IIA), disponível em https://iiabrasil.org.br/noticia/novo-modelo-das-tres-linhas-do-iia-2020.

Fonte: Novo modelo das Três Linhas do IIA 2020

1ª Linha: Gestão

Como primeira linha, os gerentes operacionais gerenciam os riscos e têm propriedade sobre eles. Eles também são os responsáveis por implementar as ações corretivas para resolver deficiências em processos e controles.

Se pensarmos em uma organização do setor público, essa primeira linha é aquela realizada por cada agente público no exercício de suas competências legais.

Segundo o IIA (2020), a gerência operacional é responsável por "liderar e dirigir ações (incluindo gerenciamento de riscos) e aplicação de recursos para atingir os objetivos da organização".

Essa gerência identifica, avalia, controla e mitiga os riscos, guiando o desenvolvimento e a implementação de políticas e procedimentos internos e garantindo que as atividades estejam de acordo com as metas e objetivos. Por meio de uma estrutura de responsabilidades em cascata, os gerentes do nível médio desenvolvem e implementam procedimentos detalhados que servem como controles e supervisionam a execução desses procedimentos. No caso do setor público, os coordenadores, chefes de divisão, gerentes de projeto, ou qualquer cargo semelhante têm essa responsabilidade.

A primeira linha contempla os controles primários, que devem ser instituídos e mantidos pelos gestores responsáveis pela implementação das políticas públicas durante a execução de atividades e tarefas no âmbito de seus processos.

2ª Linha: Suporte à gestão

As instâncias de segunda linha estão situadas ao nível da gestão e objetivam assegurar que as atividades realizadas pela primeira linha sejam desenvolvidas e executadas de forma apropriada.

Segundo o IIA (2020), são papéis da segunda linha:

1. Fornecer expertise complementar, apoio, monitoramento e questionamento quanto ao gerenciamento de riscos, incluindo:

    a) Desenvolvimento, implantação e melhoria contínua das práticas de gerenciamento de riscos (incluindo controle interno) nos níveis de processo, sistemas e entidade.

    b) O atingimento dos objetivos de gerenciamento de riscos, como: conformidade com leis, regulamentos e comportamento ético aceitável; controle interno; segurança da informação e tecnologia; sustentabilidade; e avaliação da qualidade.

2. Fornecer análises e reportar sobre a adequação e eficácia do gerenciamento de riscos (incluindo controle interno).

Dessa forma, algumas de suas funções são:

1. Função (e/ou comitê) de gerenciamento de riscos que facilite e monitore a implementação de práticas eficazes de gerenciamento de riscos por parte da gerência operacional e auxilie os proprietários dos riscos a definir a meta de exposição ao risco e a reportar adequadamente informações relacionadas a riscos em toda a organização;

2. Função de conformidade que monitore diversos riscos específicos, tais como a não conformidade com as leis e regulamentos aplicáveis. Nesse quesito, a função separada reporta diretamente à alta administração e, em alguns setores do negócio, diretamente ao órgão de governança. Múltiplas funções de conformidade existem frequentemente na mesma organização, com responsabilidade por tipos específicos de monitoramento da conformidade, como saúde e segurança, cadeia de fornecimento, ambiental e monitoramento da qualidade.

3. Função de controladoria que monitore os riscos financeiros e questões de reporte financeiro.

Essas instâncias são destinadas a apoiar o desenvolvimento dos controles internos e realizar atividades de supervisão e de monitoramento das atividades desenvolvidas no âmbito da primeira linha, que incluem gerenciamento de riscos, conformidade, verificação de qualidade, controle financeiro, orientação e treinamento.

Como exemplo, no Poder Executivo Federal, os Assessores e Assessorias Especiais de Controle Interno – AECI nos Ministérios integram a segunda linha e podem ter sua atuação

complementada por outras estruturas específicas definidas pelas próprias organizações.

3ª Linha: Auditoria Interna

Os auditores internos fornecem ao órgão de governança e à alta administração avaliações abrangentes baseadas no maior nível de independência e objetividade dentro da organização. Esse alto nível de independência não está disponível na segunda linha.

A auditoria interna provê avaliações sobre a eficácia da governança, do gerenciamento de riscos e dos controles internos, incluindo a forma como a primeira e a segunda linhas alcançam os objetivos de gerenciamento de riscos e controle.

Na Administração Pública Federal, o responsável por essa 3ª linha é a Controladoria-Geral da União – CGU, que é considerada a auditoria interna do Poder Executivo Federal. Além disso, em algumas entidades há Auditorias Internas próprias, que atuam em sinergia com a CGU.

Por fim, especificamente em relação aos riscos, essa linha deve:

1. Executar testes independentes e avaliar se a estrutura de apetite de risco, políticas de risco, procedimentos de risco e controles relacionados estão funcionando como previsto; e
2. Fornecer avaliação à administração quanto à qualidade e eficácia do programa de gerenciamento de riscos, incluindo apetite a riscos.

O órgão de governança, a gestão e a auditoria interna têm responsabilidades distintas, mas todas as atividades precisam estar alinhadas com os objetivos da organização. A base para uma coerência bem-sucedida é a coordenação, colaboração e comunicação regulares e eficazes.

2. Exemplos de Riscos à Integridade

2.1 Subcategoria 1: Desvio Ético ou de Conduta

1. Atraso no andamento dos trabalhos, por conduta profissional dissonante dos interesses institucionais;
2. Execução de atividades alheias ao serviço, durante o expediente;
3. Uso do cargo ou função para favorecimento pessoal ou de terceiros;
4. Não realização das atribuições com zelo, dedicação, presteza, responsabilidade e qualidade;
5. Não cumprimento da carga horária, ou ausência do trabalho, sem prévio aviso ou autorização da chefia;
6. Omissão do servidor em denunciar ou representar ocorrência de irregularidade;
7. Assédio moral ou sexual, preconceito (raça, gênero, religião, origem, orientação sexual).

2.2 Subcategoria 2: Ameaças à Isenção e à Autonomia Técnicas

8. Desconsideração da posição técnica na tomada de decisão;
9. Direcionamento na seleção de pessoas ou empresas prestadoras de serviços.;
10. Emissão de parecer técnico tendencioso, em desconsideração às evidências constantes em processo;
11. Omissão deliberada de informações relevantes em parecer ou instrução técnica encaminhada para tomada de decisão;
12. Emissão de pareceres quando há impedimento ou suspeição;
13. Fragilização ou desconsideração da atuação da Gestão de Risco.

2.3 Subcategoria 3: Conflito de Interesses

14. Prestação de serviços profissionais particulares pelo agente público, em conflito com as atribuições da função pública ou do órgão;
15. Ato ou omissão do servidor por influência externa, em detrimento do interesse público – “risco de captura”;
16. Influência indevida na contratação de terceiros – nepotismo;
17. Designação de funções críticas a um mesmo servidor – falta de segregação de funções;
18. Participação do servidor ou gestor em decisão de que é beneficiário particular – conflito de interesses.

2.4 Subcategoria 4: Uso indevido ou manipulação de dados/informações

19. Acesso ou concessão de acesso indevido aos dados e informações, inclusive com uso de persuasão e eventual ingenuidade dos usuários – "engenharia social" –, devido à ausência de cultura de segurança da informação e comunicação;
20. Acesso ou concessão de acesso a dados ou informações restritas para uso ou divulgação indevida;
21. Manipulação e alteração de dados e informações para benefício próprio ou de terceiros.

2.5 Subcategoria 5: Desvio de pessoal ou de recursos materiais

22. Desvio de função de estagiários, servidores, terceirizados e contratados;
23. Utilização de recursos logísticos e materiais em finalidade estranha às necessidades do serviço;
24. Ingerência em contratações, a fim de obter benefícios próprios ou em favor de terceiros;
25. Utilização da administração pública para fins eleitorais.

2.6 Subcategoria 6: Corrupção, Fraude, Desvio Irregular de Verbas Públicas

26. Influência indevida de interesses privados nas decisões ou procedimentos de órgãos singulares ou colegiados;
27. Direcionamento de normas ou da atuação do órgão para favorecimento de interesses privados;
28. Indícios de enriquecimento ilícito e/ou lavagem de dinheiro;
29. Indícios de fraudes em processos licitatórios.

3. Exemplos de Medidas de Tratamento a Riscos à Integridade

Apresentam-se, a seguir, alguns exemplos de medidas de tratamento de riscos à integridade. Nada impede, entretanto, que tais exemplos sejam rediscutidos no momento oportuno

Conjunto exemplificativo de medidas de tratamento a riscos para a Integridade.

- Atualização do Banco de Talentos da entidade pelos servidores, como estímulo para processos de solicitação de capacitação e promoção na carreira;
- Ações de sensibilização voltadas à prevenção de condutas antiéticas;
- Estudo sobre critérios para identificação e avaliação de líderes da entidade, para atualização da Política de Gestão de Pessoas;
- Revisão do Código de Conduta Profissional do Servidor da entidade;
- Ações permanentes de monitoramento de acesso a sistemas e pastas de rede;

- Adoção de postura proativa para identificação de temas específicos com vistas a fomentar a capacitação interna;
- Implantação da Base de Conhecimento da entidade;
- Mapeamento e divulgação dos Canais de Denúncia e de fluxos dos processos da Comissão de Ética;
- Elaboração de normativo que trate sobre a omissão de irregularidades de forma intencional Projeto "Programa de Valores da Entidade";
- Programa de Desenvolvimento de Líderes;
- Aperfeiçoamento de ferramentas de trabalho e comunicação interna, que possibilitam a edição de trabalhos de maneira colaborativa;
- Procedimentos e trilhas para identificação de casos de nepotismo na entidade;
- Exigência de declaração de parentesco no momento da posse para cargos em comissão, funções e confiança, terceirizados ou estagiários;
- Orientação contínua reforçando a obrigatoriedade de utilização dos controles existentes nos processos de auditoria;
- Metodologia para implementação das revisões de qualidade no âmbito do Programa de Avaliação e Melhoria da Qualidade das Ações de Controle;
- Política de rotação periódica de servidores / coordenadores; e
- Política que impeça que auditores da entidade que estavam atuando na gestão em unidades auditadas realizem trabalhos de auditoria sobre a mesma unidade pelo período de 2 anos.

4. Exemplos de Eventos de Risco Operacional

Apresentam-se, a seguir, alguns exemplos de riscos operacional. Nada impede, entretanto, que tais exemplos sejam rediscutidos pelo CRTCI/ME no momento oportuno.

Processos

Comunicação Interna:

- Os insumos e as informações não são recebidos em tempo adequado para a execução do processo;
- Ausência de padrões mínimos definidos para a execução do processo; e
- Erros e falhas de informações que afetam a execução do processo.

Modelagem:

- Fluxo desatualizado e não reflete a prática atual utilizada na execução do processo;
- Ausência de avaliações periódica sobre a adequabilidade do desenho do processo;

- Ausência ferramenta para análise e melhoria contínua do processo; e
- Falha ou falta de metodologia que auxilie no mapeamento do processo.

Segurança Física:

- Falha ou falta de segurança no ambiente de trabalho que afeta a execução do processo; e
- Acesso a áreas consideradas como críticas sem que as pessoas estejam devidamente credenciadas e identificadas

Adequação à Legislação:

- Descumprimento de prazos legais na execução do processo;
- Ausência de compilação e distribuição de legislação pertinente ao processo em execução;
- Execução do processo em desacordo com o regimento interno/normas;
- Descumprimento de prazo judicial na execução do processo; e
- Descumprimento de obrigação regulatória na execução do processo

Pessoas

Carga de trabalho:

- Rotatividade (turnover) de pessoal acima do esperado que afeta a execução do processo;
- Capacidade operacional insuficiente para a execução do processo; e
- Falha ou falta de dimensionamento da capacidade operacional com impacto na execução do processo.

Competências:

- Capacitação da equipe é insatisfatória para a execução do processo;
- Concentração de conhecimentos em determinados servidores afetando a execução do processo;
- Falha ou falta de disseminação de conhecimento afetando a execução do processo; e
- Falha ou falta de capacitação que afeta a execução do processo.

Ambiente Organizacional:

- Ausência de satisfação e/ou de bem-estar do servidor na execução de sua tarefa;
- Desconhecimento dos objetivos do processo por parte dos Servidores;
- Servidores desconhecem as suas responsabilidades individuais na execução do

processo;

- Ausência de recursos necessários para execução das tarefas; e
- Resistência de Servidores em promover alterações nas condições de trabalho.

Conduta:

- Ausência de postura ética nas atividades e nos relacionamentos interpessoais;
- Falta de atenção e zelo na execução do processo;
- Ausência de imparcialidade, cumprimento das leis e normas/regulamentares, confidencialidade e comprometimento na execução do processo; e
- Quebra de sigilo e confidencialidade.

Ambiente Tecnológico

Segurança Lógica:

- Ausência de estrutura de perfis de acesso aos sistemas para execução do processo
- Ausência de controle de acesso lógico
- Ausência de logon próprio na rede institucional
- Falha ou falta de meios seguros de acesso aos sistemas
- Inexistência de registro nos sistemas (log) das transações críticas
- Ausência de formalização que defina as responsabilidades do usuário externo do sistema
- Incapacidade do sistema de prover informações confiáveis e suficientes sobre o processo em execução

Infraestrutura Tecnológica:

- Grau de informatização do processo inadequado para execução do processo
- Informações e dados armazenados em diretórios não protegidos e sem controle de acesso
- Ausência de backup de arquivos, planilhas e bancos de dados essenciais à execução do processo
- A estação de trabalho não possui acionado dispositivo de time-out
- Descarte de mídias sem antes terem apagados os com conteúdo reservado
- Sobrecarga de sistemas de processamento de dados no momento da execução do processo
- Inadequação de sistemas operacionais/aplicativos para execução do processo

- Falhas de hardware, faltas de backup e de legalização do software afetando a execução do processo
- Obsolescência dos sistemas e equipamentos afetando a execução do processo
- Ataques lógicos à rede de computadores afetando a execução do processo

Soluções de TI:

- Inexistência de controle nas requisições e nas melhorias requeridas nos sistemas cuja falta de implementação afeta a execução do processo
- Falha ou falta de homologação de sistema impedindo a execução do processo de forma automatizada

Comunicação:

- Instabilidade nos sistemas operacionais que afeta a execução do processo
- Incompatibilidade e/ou indisponibilidade de informações afetando a execução do processo

Eventos Externos

Desastres Naturais e Catástrofe:

- Ação Humana: ações intencionais executadas por terceiros para lesar o órgão, como por exemplo: (i) roubos, falsificações, furtos, atos de vandalismos, fraudes externas; (ii) degradação do meio ambiente; e (iii) alterações no ambiente econômico, político e social
- Força Maior: (i) enchentes, terremotos, catástrofes (queda de prédio) e outros desastres naturais

Ambiente Regulatório

- Alterações inesperadas na legislação ou em marcos regulatórios pelos órgãos fiscalizadores e reguladores

Ambiente Social

- Cenário socioeconômico interfere na execução do processo
- Retrações ou não-aproveitamento de oportunidades de mercado provocadas por eventos relacionados a segurança patrimonial que impede a execução do processo

Fornecedores:

- Indisponibilidade de recursos em virtude de concentração em um único fornecedor que impede a execução do processo
- Falhas ou indisponibilidade de serviços públicos que afeta a execução do processo

5. Exemplos de Controles Básicos

Apresentam-se, a seguir, alguns exemplos de controles básicos. Nada impede, entretanto, que tais exemplos sejam rediscutidos no momento oportuno. O que permite atualizar a resolução sobre riscos à integridade.

Pessoas (carga de trabalho, competências, ambiente organizacional, conduta)

- Planejamento de curto, médio e longo prazos;
- Acordo de Trabalho;
- Pesquisa de Clima Organizacional;
- Reuniões participativas;
- Identificação da necessidade de conhecimentos/habilidades;
- Atividades de treinamento e capacitação;
- Padronização de normas e procedimentos internos;
- Ferramentas de autoavaliação de conhecimentos/habilidades
- Canais de comunicação com a alta administração;
- Processo de gerenciamento de equipes;
- Valores éticos e normas de conduta da organização;
- Mecanismos de incentivos (motivação/recompensa/punição) e prática de disciplina e demissão;
- Reconhecimento formal de responsabilidades;
- Conferência de autorizações;
- Rodízio de funcionário;
- Segregação de funções; e
- Testes de Conformidade.

Processos (comunicação interna, modelagem, segurança física, adequação à legislação)

- Canais de comunicação com funcionários;
- Normas e procedimentos internos;
- Ferramentas para análise e melhoria contínuas de processos;
- Metodologia de autoavaliação de riscos e controles;
- Validações – *backtesting*;
- Mecanismos de monitoramento e reporte;

- Mecanismos de segurança física;
- Controles de acesso físico;
- Atualização e manutenção de equipamentos; e
- Testes de conformidade.

Ambiente Tecnológico (segurança lógica, infraestrutura e tecnologia, comunicação)

- Políticas e Diretrizes;
- Controles de acesso lógico;
- Arquivo e preservação de registros;
- Manutenção de equipamentos;
- Layout de formulários e sistemas;
- Validações – backtesting;
- Atividade de treinamento; e
- Planos de Contingência.

Eventos Externos (desastres naturais atuais e catástrofes, ambiente regulatórios, ambiente social, fornecedores)

- Planos de Contingências;
- Análise de conjuntura política e econômica nacional e internacional; e
- Controles de serviços terceirizados.

6. Glossário

Accountability – obrigação dos agentes e das organizações que gerenciam recursos públicos de assumir integralmente as responsabilidades por suas decisões e pela prestação de contas de sua atuação de forma voluntária, inclusive sobre as consequências de seus atos e omissões. (IN CGU Nº 3, 09 de junho de 2017).

Ágatha – Solução integrada e gratuita disponibilizada em apoio às rotinas de gerenciamento de riscos.

Análise de contexto – levantamento e registro dos aspectos externos e internos, que compõem o ambiente onde a organização visa alcançar os seus objetivos, permitindo a compreensão clara do contexto em que a organização se insere a fim de proporcionar uma visão abrangente dos fatores que podem influenciar a capacidade da organização de atingir os resultados planejados.

Análise de riscos – compreender a natureza do risco e suas características, incluindo o nível de risco, onde apropriado. A análise de riscos envolve a consideração detalhada de incertezas, fontes de risco, consequências, probabilidade, eventos, cenários, controles e sua eficácia (ABNT, 2018).

Apetite a risco – quantidade de risco em nível amplo que uma organização está disposta a aceitar na busca de seus objetivos (INTOSAI, 2007). Quantidade e tipo de riscos que uma organização está preparada para buscar, reter ou assumir (ABNT, 2009a).

Avaliação de risco – envolve a comparação dos resultados da análise de riscos com os critérios de risco estabelecidos para determinar onde é necessária ação adicional.

Controles (Sistema de Controle) – processos estruturados para mitigar os possíveis riscos com vistas ao alcance dos objetivos institucionais e para garantir a execução ordenada, ética, econômica, eficiente e eficaz das atividades da organização, com preservação da legalidade e da economicidade no dispêndio de recursos públicos. (Decreto Nº 9.203/2017).

Controles Detectivos – são controles desenhados para detectar erros (intencionais e não-intencionais) que já ocorreram, seu enfoque é "a posteriori".

Controles internos da gestão – conjunto de regras, procedimentos, diretrizes, protocolos, rotinas de sistemas informatizados, conferências e trâmites de documentos e informações, entre outros, operacionalizados de forma integrada pela direção e corpo de servidores das organizações, destinados a enfrentar os riscos e fornecer segurança razoável de que na consecução da missão da entidade os seguintes objetivos gerais serão alcançados: (i) execução ordenada, ética, econômica, eficiente e eficaz das operações; (ii) cumprimento das obrigações de *accountability*; (iii) cumprimento das leis e regulamentos aplicáveis; e (iv) salvaguarda dos recursos para evitar perdas, mau uso e danos. O estabelecimento de controles internos no âmbito da gestão pública visa essencialmente aumentar a probabilidade de que os objetivos e metas estabelecidos sejam alcançados, de forma eficaz, eficiente, efetiva e econômica.).

Controles Preventivos – são controles desenhados para prevenir a ocorrência de erros (intencionais e não-intencionais), seu enfoque é "a priori".

Ética – refere-se aos princípios morais, sendo pré-requisito e suporte para a confiança pública.

Evento – um incidente ou uma ocorrência de fontes internas ou externas à organização, que podem impactar a implementação da estratégia e a realização de objetivos de modo negativo, positivo ou ambos (INTOSAI, 2007). Eventos com impacto negativo representam riscos. Eventos com impacto positivo representam oportunidades; ocorrência ou mudança em um conjunto específico de circunstâncias, podendo consistir em alguma coisa não acontecer. A expressão "eventos potenciais" é muitas vezes utilizada para caracteriza

Fraude – ato ou omissão intencional concebido por um ou mais indivíduos, responsáveis pela governança, empregados ou terceiros, para obter vantagem ilícita, em prejuízo alheio, caracterizado pela desonestidade, dissimulação ou quebra de confiança (IN CGU Nº 3, 09 de junho de 2017 e NBC T 11 – IT – 03 – fraude e erro).

Gestão de Riscos – conjunto de princípios, estruturas, alçadas, processos e atividades coordenados para dirigir e controlar uma organização no que se refere a riscos. Trata-se do "processo de natureza permanente, estabelecido, direcionado e monitorado pela alta administração, que contempla as atividades de identificar, avaliar e gerenciar potenciais eventos que possam afetar a organização, destinado a fornecer segurança razoável quanto à realização de seus objetivos" (Decreto n. 9.203/2017, Art. 2º, inciso IV).

Governança Pública – conjunto de mecanismos de liderança, estratégia e controle postos em prática para avaliar, direcionar e monitorar a gestão, com vistas à condução de políticas públicas e à prestação de serviços de interesse da sociedade. (Decreto Nº 9.203/2017)

Impacto – efeito resultante da ocorrência do evento de risco.

Indicadores – "medidas, de ordem quantitativa ou qualitativa, dotada de significado particular e utilizada para organizar e captar as informações relevantes dos elementos que compõem o objeto da observação. É um recurso metodológico que informa empiricamente sobre a evolução do aspecto observado" (Brasil, 2010, p. 21).

Indicadores-chaves de desempenho – número, percentagem ou razão que mede um aspecto do desempenho na realização de objetivos estratégicos e operacionais relevantes para o negócio, relacionados aos objetivos-chaves da organização, com o objetivo de comparar esta medida com metas preestabelecidas (TCU, 2010).

Indicadores-chaves de risco – número, percentagem ou razão estabelecido para monitorar as variações no desempenho em relação à meta para o cumprimento de objetivos estratégicos e operacionais relevantes para o negócio, relacionados aos objetivos-chaves da organização (TCU, 2010).

Matriz de risco – matriz gráfica que exprime o conjunto de combinações de probabilidade e impacto de riscos para classificar os níveis de risco.

Medidas de contingência – ações previamente planejadas que devem ser executadas caso um ou mais riscos se concretizem visando mitigar os impactos

Modelo de três linhas – Anteriormente conhecido como Três Linhas de Defesa. O gestor é a primeira linha no gerenciamento de riscos, as diversas funções de controle de riscos e supervisão de conformidade estabelecidas pela gerência são a segunda linha e a avaliação independente é a terceira. Cada uma dessas três linhas desempenha um papel distinto dentro da estrutura mais ampla de governança da organização.

Monitoramento – verificação, supervisão, observação crítica ou identificação da situação, executadas de forma contínua, a fim de identificar mudanças no nível de desempenho requerido ou esperado. Monitoramento pode ser aplicado a riscos, a controles, à estrutura de gestão de riscos e ao processo de gestão de riscos.

Nível de risco – magnitude de um risco ou combinação de riscos, expressa em termos da combinação das consequências [impacto] e de suas probabilidades (ABNT, 2009).

Política de gestão de riscos – documento que contém a declaração das intenções e diretrizes gerais relacionadas à gestão de riscos e estabelece claramente os objetivos e o comprometimento da organização em relação à gestão de riscos. Não se trata de uma declaração de propósitos genérica, mas de um documento que, além de declarar os princípios, explica porque a gestão de riscos é adotada, o que se pretende com ela, onde, como e quando ela é aplicada, quem são os responsáveis em todos os níveis, dentre outros aspectos (ABNT, 2009).

Probabilidade – medida da possibilidade de ocorrência de um evento de risco.

Respostas a risco – opções e ações gerenciais para tratamento de riscos. Inclui evitar o risco pela decisão de não iniciar ou descontinuar a atividade que dá origem ao risco porque o risco está além do apetite a risco da organização e outra resposta não é aplicável; transferir o risco a outra parte ou compartilhar o risco com outra parte; aceitar o risco por uma escolha consciente; ou mitigar o risco diminuindo sua probabilidade de ocorrência ou minimizando suas consequências (INTOSAI, 2007).

Risco – possibilidade de um evento ocorrer e afetar adversamente a realização de objetivos (COSO GRC, 2004); efeito da incerteza nos objetivos (ABNT, 2018); possibilidade de ocorrência de um evento que venha a ter impacto no cumprimento dos objetivos. O risco é medido em termos de impacto e de probabilidade. (IN CGU Nº 3, 09 de junho de 2017)

Risco à Integridade – efeito da incerteza relacionado a corrupção, fraudes, irregularidades e/ou desvios éticos e de conduta, que possa comprometer os valores e padrões preconizados pela Instituição e a realização de seus objetivos.

Risco inerente – risco a que uma organização está exposta sem considerar quaisquer ações gerenciais que possam reduzir a probabilidade de sua ocorrência ou seu impacto. (IN CONJ. CGU/MP Nº 001, 10 de maio de 2016)

Risco residual – risco a que uma organização está exposta após a implementação de ações gerenciais para o tratamento do risco. (IN CONJ. CGU/MP Nº 001, 10 de maio de 2016

Tolerância a Risco – representa a variação aceitável em desempenho, intimamente ligada

com apetite a risco.

Valor público – produtos e resultados gerados, preservados ou entregues pelas atividades de uma organização que representem respostas efetivas e úteis às necessidades ou às demandas de interesse público e modifiquem aspectos do conjunto da sociedade ou de alguns grupos específicos reconhecidos como destinatários legítimos de bens e serviços públicos. (Decreto Nº 9.203/2017)

SECRETARIA DE GESTÃO CORPORATIVA
SECRETARIA EXECUTIVA
MINISTÉRIO DA ECONOMIA

PÁTRIA AMADA BRASIL
GOVERNO FEDERAL