Cartilha de Estruturação e Implementação da Gestão de Riscos

1ª edição. Janeiro/2022

Secretaria da Controladoria Geral do Estado

GOVERNO DO ESTADO
PERNAMBUCO
MAIS TRABALHO, MAIS FUTURO.

Expediente

GOVERNO DO ESTADO DE PERNAMBUCO

PAULO HENRIQUE SARAIVA CÂMARA
Governador do Estado

LUCIANA BARBOSA DE OLIVEIRA SANTOS
Vice-Governadora do Estado

MARCONI MUZZIO PIRES DE PAIVA FILHO
Secretário da Controladoria-Geral do Estado
Ouvidora-Geral do Estado

FILIPE CAMELO DE CASTRO
Secretário-Executivo da Controladoria-Geral do Estado

CRISTIANA BORGES DE B. E S. NOVELLINO
Diretora de Monitoramento, Avaliação e Controle

TIAGO BARBOSA DA FONSECA
Coordenador de Avaliação e Promoção da Qualidade do Gasto

ELABORAÇÃO:

VANESSA BEZERRA DUARTE DA SILVA
Chefe da Unidade de Promoção da Qualidade do Gasto

www.scge.pe.gov.br I www.transparencia.pe.gov.br
www.ouvidoria.pe.gov.br I www.lai.pe.gov.br

instagram: @scge_pe

SECRETARIA DA CONTROLADORIA-GERAL DO ESTADO
Rua Santo Elias, 535 - Espinheiro - Recife - PE - CEP.: 52020-095
Telefone: (081) 3183-0800

Sumário

1. Introdução 4

2. Por que implementar gestão de riscos na organização? 5

3. Metodologia 7

4. Eixo: Estruturação 9

5. Eixo: Implementação 28

6. Conclusão 38

1. Introdução

A Secretaria da Controladoria-Geral do Estado (SCGE) pretende com esta cartilha auxiliar os órgãos e entidades estaduais na estruturação e implementação da Gestão de Riscos, a partir da apresentação de boas práticas a serem observadas.

Vale ressaltar que as abordagens estabelecidas neste documento são orientativas, podendo sofrer ajustes ou adequações.

2. Por que implementar Gestão de Riscos na organização?

As organizações públicas do Estado de Pernambuco vem de forma exitosa implementando ferramentas para auxiliar na definição da missão, visão, valores e objetivos. Ressalta-se, porém, que existem fatores incertos que podem comprometer a realização dos objetivos traçados, sendo necessária a utilização de uma metodologia que permita, de forma estruturada, identificar, avaliar e priorizar riscos relevantes que possibilitem a adoção de controles para mitigar a probabilidade do risco se concretizar e, caso se concretizem, que reduzam o seu impacto.

A implementação e manutenção da gestão dos riscos possibilita para a organização a melhoria da sua governança, o aumento da probabilidade de atingir seus objetivos, apresentação de informações confiáveis para a tomada de decisão, melhoria dos controles e da aprendizagem organizacional, além de outros benefícios.

O Decreto Estadual nº 46.855/2018 define a gestão de riscos como um 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 (Art. 2º, IV).

Esse mesmo instrumento legal estadual, em seu art. 17, prevê que a alta administração das organizações da administração pública estadual 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.

Sendo assim, verifica-se que a implementação da gestão de riscos permitirá à organização elencar e tratar riscos que possam comprometer os objetivos traçados, sendo prevista a sua obrigatoriedade no Decreto Estadual nº 46.855/2018 em razão da sua importância.

3. Metodologia

Este documento está pautado, sobremaneira, nos entendimentos acerca dos eixos essenciais para o desenvolvimento da temática, especialmente pelas seguintes referências: ISO[1] 31000 (2018); Gerenciamento de Riscos Corporativos Integrado com Estratégia e Performance, COSO[2] (2017); e Referencial Básico de Gestão de Riscos do TCU[3] (2018).

Nesse contexto, no intuito de fomentar a cultura da gestão de riscos nos órgãos e entidades do Poder Executivo Estadual, foi desenvolvida esta cartilha, que é estruturada nos dois eixos abaixo:

- **Estruturação:** São as medidas importantes para criar um ambiente estruturado de gestão de riscos, correspondendo ao conjunto de política, planos, matriz de responsabilidades e outros pontos necessários para integrar a gestão de riscos às atividades e funções do órgão.

- **Implementação:** Correspondem aos pontos referentes ao processo de Gerenciamento de Risco, que inicia com a análise do contexto e definição de escopo e encerra com a elaboração do plano de tratamento.

---

[1] *International Organization for Standardization* (Organização Internacional de Normalização).
[2] *Committee of Sponsoring Organizations of the Treadway Commission* (Comitê das Organizações Patrocinadoras da Comissão *Treadway*).
[3] Tribunal de Contas da União.

Em cada eixo, é listada uma série de pontos focais, que correspondem a boas práticas que devem ser observadas para auxiliar os gestores na estruturação e implementação da gestão de riscos da organização, sendo a abordagem estruturada a partir de uma breve explicação sobre o ponto focal seguido de sugestões de ações práticas para facilitar a aplicação dos conceitos apresentados.

Por fim, para melhor entendimento dos pontos focais, faz-se necessário diferenciarmos os conceitos de gestão de riscos e gerenciamento de riscos.

A **Gestão de Riscos** corresponde ao conjunto de atividades coordenadas para dirigir e controlar uma organização no que se refere a riscos (ISO Guia 75:2009). Já o **gerenciamento de riscos** é o processo de identificação, avaliação e resposta aos riscos, compreendendo desde as etapas de definição de contexto e escopo até a elaboração do plano de tratamento.

Sendo assim, verifica-se que a **Gestão de Riscos** engloba, além do **Gerenciamento de Riscos**, aspectos como a governança, cultura, ferramentas de comunicação e de monitoramento e mecanismos de análise crítica e melhoria contínua, por exemplo.

4. EIXO: Estruturação

4.1. Pontos focais

1º PONTO FOCAL: COMPROMETIMENTO DA ALTA ADMINISTRAÇÃO

Segundo a norma ISO 31000:2018, risco é o "efeito da incerteza nos objetivos". Esse efeito é um desvio em relação ao esperado, podendo ser positivo ou negativo. Conhecer os riscos que podem afetar os objetivos da organização é uma maneira de preservação de valor público e melhoria de seu desempenho, por meio da adoção de medidas que possam mitigar eventuais efeitos negativos decorrentes desses riscos. É possível ainda aproveitar as oportunidades (desvios positivos), quando identificadas.

Em virtude dessa importância, a condução da gestão de riscos não se restringe a apenas uma função ou departamento, devendo fazer parte da estrutura da organização, sendo, assim, necessário o comprometimento da alta gestão para encorajar todos os colaboradores a incorporar os conceitos e as ferramentas de gestão de riscos com vistas ao melhor atingimento dos objetivos organizacionais. Além disso, é necessário o apoio da alta gestão para permitir a integração da gestão de riscos na governança e em todas as atividades da organização, incluindo a tomada de decisão.

De acordo com a norma ISO 31000:2018, 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.

Importante

Diante de toda a explicação acima, o gestor pode chegar a realizar a seguinte pergunta:

- Caso, inicialmente, a Alta Gestão não demonstre apoio ao projeto de gestão de riscos, devemos necessariamente não iniciar o projeto?

Apesar de a maior parte da literatura e estruturas referentes a gestão de riscos citarem que o tom deve vir do topo "Tone at the top", nos casos em que ainda não tenha ocorrido dessa forma, uma alternativa é efetuar a prática oposta e começar a partir de ações específicas em determinadas áreas ou processos que, após validação, servirão de exemplo e poderão ser replicadas na organização.

Ações sugeridas:

- Relacionar alguns eventos relevantes que prejudicaram atividades, desempenho ou imagem do órgão/entidade para apresentar para a alta gestão;

• Relacionar e detalhar os efeitos enfrentados pela organização por não ter tais eventos de risco mapeados e um plano de tratamento para apresentar para a alta gestão;

• Apresentar os resultados do gerenciamento de riscos realizado em uma determinada área como forma de demonstrar a alta gestão a importância da gestão de riscos e assim conseguir o comprometimento.

• Apresentar à alta gestão os benefícios esperados com a implantação da gestão de riscos para a preservação de valor público, inclusive com o apoio da Secretaria da Controladoria Geral do Estado, caso necessário.

2º PONTO FOCAL: CRIAÇÃO DE GRUPO DE TRABALHO / COMISSÃO

Antes de detalharmos sobre o Grupo de Trabalho/ Comissão, é necessário entendermos os papéis de controle que podem ser desempenhados numa organização, conforme preconizado pelo Modelo das Três Linhas do Institute of Internal Auditors (IIA) 2020.

De acordo com o modelo, os controles devem ser estruturados numa organização através de 3 linhas, cujos papéis são os listados abaixo:

• Papéis de **primeira linha:** estão mais diretamente alinhados com a entrega de produtos e/ou serviços

aos clientes da organização, sendo responsável pela **identificação e avaliação** de riscos e **proposição** de controles.

• Papéis de **segunda linha:** fornecem **assistência** no gerenciamento de riscos.

• Papéis de **terceira linha:** são desempenhados pela **auditoria interna**, que presta avaliação e assessoria independentes e objetivas sobre a adequação e eficácia da governança e do gerenciamento de riscos.

Com base no modelo acima, conclui-se que cabe ao Grupo de Trabalho ou Comissão os papéis de segunda linha, sendo o seu desempenho de extrema importância para auxiliar a gestão na estruturação e condução do projeto de implantação da gestão de riscos no órgão. Conduzido pela Unidade de Controle interno, é interessante que esse grupo:

1. Realize os estudos iniciais acerca do assunto;

2. Entenda a estrutura do órgão e seus processos;

3. Defina a estratégia de implementação.

Inicialmente, este grupo irá realizar os estudos acerca do tema, com o intuito de formar entendimento e disseminar conceitos, técnicas, modelos e boas práticas em gestão de riscos. Em seguida, o grupo irá analisar informações sobre estrutura e processos da organização e, com base nos resultados desses estudos, irá definir a estratégia de estruturação e implementação da gestão de riscos.

Após a alta administração e o grupo de trabalho indicado construírem entendimento sobre o assunto, é necessário promover capacitação ao corpo tático (gerentes, coordenadores, etc) e ao corpo operacional da unidade. Nesse momento, as capacitações visam trazer uma visão geral e conscientizar os servidores a respeito da importância da gestão de riscos, abordando os conceitos de uma forma geral e demonstrando os seus benefícios.

Ações sugeridas:

• Nomear um grupo de trabalho para coordenar o processo de implementação da gestão de riscos;

• Estudar gestão de riscos por meio de leitura de cartilhas e manuais, da participação em cursos, seminários, palestras sobre o assunto, etc.;

• Realizar benchmarking com outras instituições que já iniciaram o processo de gestão de riscos;

• Conhecer e analisar as informações da organização, tais como: regulamento, organograma, planejamento estratégico e processos mapeados (quando houver);

• Elaborar plano de ação para implementação da gestão de riscos;

• Disseminar o conhecimento sobre o tema por meio de reuniões, workshops internos.

3º PONTO FOCAL: DEFINIÇÃO DE RESPONSABILIDADES

Os papéis organizacionais, autoridades e responsabilidades dos servidores e das unidades, no que tange à gestão de riscos, devem ser definidos de forma clara. Dessa forma, todos terão ciência e poderão exercer seus papéis no gerenciamento de riscos dentro da organização.

Estabelecer estruturas e processos que auxiliem os gestores a gerenciar os riscos é responsabilidade da alta administração juntamente com as instâncias de governança.

De acordo com a norma ISO 31000:2018, convém que a Alta Direção e os órgãos de supervisão, onde aplicável, assegurem que as autoridades, responsabilidades e responsabilização para os papéis pertinentes à gestão de riscos sejam atribuídas e comunicadas a todos os níveis da organização.

A organização deverá atuar de forma a garantir que haja responsabilização, autoridade e competência apropriadas para gerenciar riscos, incluindo implementar e manter o processo de gestão de riscos.

Ações sugeridas:

- Analisar o contexto interno e externo, como é a atual estrutura de governança e os recursos disponíveis;

• Considerar o modelo de três Linhas do IIA ao definir papéis e responsabilidades;

• Identificar os proprietários dos riscos, que têm a responsabilidade e a autoridade para gerenciar riscos;

• Deixar claro que os gestores são responsáveis por gerenciar riscos e por fomentar a cultura de gestão de riscos no âmbito de suas unidades e de acordo com suas responsabilidades (1ª Linha);

• Atribuir responsabilidades de orientação e acompanhamento do processo de gerenciamento de riscos da organização a uma unidade ou grupo (2ª Linha);

• Apresentar responsabilidades por meio de matriz RACI

4º PONTO FOCAL: POLÍTICA DE GESTÃO DE RISCOS

O processo de gestão de riscos consiste na aplicação sistemática de políticas, procedimentos e práticas de gestão para as atividades de comunicação, consulta, estabelecimento do contexto, e na identificação, análise, avaliação, tratamento, monitoramento e análise crítica dos riscos (ISO 31000:2009).

Este processo deve ser desenhado com o objetivo de alcançar os diversos tipos de processos organizacionais, incluindo planejamento estratégico, todos os processos

de gestão de projetos e gestão de mudanças. Ou seja, devem alcançar atividades estratégicas, operacionais, decisões, projetos, etc.

Como a gestão de riscos envolve toda a estrutura da organização, é necessária a padronização dos conceitos, procedimentos e critérios através de um documento que permita ser utilizado por todos os colaboradores da unidade, sendo o documento este denominado de Política de Gestão de Riscos.

A política de gestão de riscos é um documento que contém a declaração das intenções e diretrizes gerais relacionadas à gestão de riscos em uma organização. Convém que a política estabeleça claramente os objetivos e o comprometimento da organização em relação à gestão de riscos (ISO 31000:2009).

Buscando auxiliar os órgãos e entidades na elaboração da sua Política de Gestão de Riscos, a SCGE divulgou um modelo de Política de Gestão de Riscos em seu sítio eletrônico.

Ainda de acordo com esta norma, convém que a política traga as seguintes informações:

I. Categorias de Riscos;

II. Definição e critérios para a elaboração do Plano de Monitoramento e Análise Crítica;

III. Definição e critérios para a elaboração do Plano de Comunicação;

IV. Definição e critérios para a elaboração do Declaração de Apetite;

V. Princípios e objetivos da Gestão de Riscos aplicados à unidade;

VI. Critérios de priorização dos processos;

VII. Etapas de Gerenciamento de Riscos;

VIII. Partes interessadas e responsabilidades; e

IX. Prazos de revisão da política.

Após a elaboração da política de gestão de riscos, esta deve ser comunicada adequadamente a todos da organização.

Ações sugeridas:

• Trocar informações com outras organizações que já passaram por esta etapa, conhecendo suas políticas de gestão de riscos;

• Utilizar modelo disponibilizado pela SCGE como referência para elaboração da política;

• Definir critérios para analisar a significância dos riscos, incluindo a definição de como a probabilidade, o impacto e os níveis de riscos serão calculados;

• Definir diretrizes para avaliar e priorizar os riscos e selecionar as respostas para tratá-los;

• Estabelecer procedimentos e técnicas para gerenciar riscos (incluindo a identificação, análise, avaliação, registro e elaboração de resposta aos riscos);

• Obter aprovação da alta administração, visto que este documento deverá guiar toda a organização quanto à gestão de riscos.

• Divulgar a política, deixando clara a sua importância para auxiliar a gestão e os gestores a alcançarem os objetivos traçados pela organização.

5º PONTO FOCAL: DECLARAÇÃO DE APETITE

No momento da implementação da metodologia de gestão de riscos, é comum o gestor fazer o seguinte questionamento: *"Minha unidade conta com vários processos, inúmeras atividades e, em consequência, diversos riscos. Devo tratar todos?"* A resposta direta à dúvida é de que a dimensão da quantidade e tipos de riscos que serão tratados depende do apetite a riscos da organização.

"E o que seria apetite a riscos?" O apetite ao risco é a quantidade de risco que a empresa deseja assumir para conseguir atingir seus objetivos. Podemos dizer também que apetite a risco é a quantidade de riscos, no sentido mais amplo, que uma organização está disposta a aceitar em sua busca para agregar valor.

Mesmo diante dos conceitos até então apresentados neste ponto focal, o gestor ainda continua com dúvida. *"E se o risco classificado dentro do apetite ao risco (não tratado) for concretizado?"*

Uma resposta a essa indagação pode ser encontrada através da boa prática contida na Política do Ministério das Cidades, publicada através da Portaria nº 650, de 16 de novembro de 2017, conforme segue:

> *"a indesejada materialização de um risco de baixa criticidade (problema), à vista de critério previamente fixado pela administração diante de seu apetite a riscos, não ensejará responsabilização, de per si, de servidor público federal por omissão, relativamente a possível feito administrativo-disciplinar".*

Um outro conceito importante é o de **tolerância**, que corresponde ao nível admissível de variação no desempenho da Organização na realização dos objetivos.

O conceito de apetite e tolerância se relacionam na medida em que as empresas, ao definir o seu apetite a

risco em sua estratégia, devem considerar a tolerância, que se relaciona aos objetivos e às metas estabelecidas para cada um de seus processos organizacionais.

O apetite e a tolerância a riscos da organização são sistematizados através de um documento denominado Declaração de Apetite aos Riscos, que define o posicionamento institucional acerca do tema.

Seguem abaixo algumas informações importantes que podem constar na Declaração de Apetite aos Riscos:

I - a missão da organização;

II - tipologia e níveis de risco definidos pelo órgão;

III - nível de apetite em função da tipologia definida e de outros critérios pela gestão;

IV - opções de tratamento por tipo de risco;

V - unidades administrativas responsáveis por sua aprovação, revisão e monitoramento;

VI - período de revisão do apetite;

Ações sugeridas:

• A Alta administração deve definir o apetite ao risco da organização.

• O grupo de trabalho/comitê deve, após definição do apetite ao risco pela alta administração, elaborar a Declaração de Apetite aos Riscos.

6º PONTO FOCAL: PLANO DE COMUNICAÇÃO

O Plano de Comunicação tem como principal objetivo garantir que as partes interessadas no processo de gestão de riscos tenham informações e possam supervisionar e tomar as decisões de forma eficiente.

O plano de comunicação deve conter pelo menos:

I - Etapa do processo de gestão de riscos

II - Produto associado à etapa

III - Objetivo da Comunicação

IV - Comunicador

V - Destinatários

VI - Meio de Comunicação;

VII - Sistema a ser utilizado para envio da comunicação;

VIII - Frequência.

O plano poderá também prever um conjunto de medidas

necessárias para incentivar o engajamento e fomentar o conhecimento dos colaboradores em relação aos seguintes temas:

I. Promoção da conscientização e do entendimento da gestão de riscos através de informações sobre o que é, qual o seu objetivo, os benefícios e a quem se destina.

II. Disseminação de informações relevantes sobre o plano de Gestão de Riscos, comunicando sobre as atividades e os resultados.

Há diversas maneiras de realizar essas medidas, tais como: realização de workshops, envio de emails aos servidores, publicações periódicas sobre o tema na intranet, divulgação de notícias e informações no site, redes sociais e imprensa.

Ações sugeridas:

• Estabelecer a forma e a periodicidade de repasse, para a alta administração, os órgãos de governança e controle e demais partes interessadas, do andamento das ações de gerenciamento dos riscos;

• Promover palestras sobre gestão de riscos para conscientizar os servidores da importância do tema;

• Enviar e-mails periódicos para os servidores com informações do tipo “Você sabia?”;

• Divulgar notícias e informações nas redes sociais oficiais, na intranet e no site do órgão;

• Criar canais de comunicação que possibilitem ouvir os colaboradores que compõem a organização;

7º PONTO FOCAL: PLANO DE MONITORAMENTO E ANÁLISE CRÍTICA

Segundo o COSO ERM, o gerenciamento de riscos corporativos de uma organização modifica-se com o passar do tempo, visto que as seguintes situações podem acontecer:

a. As respostas aos riscos que se mostravam eficazes na época do gerenciamento podem tornar-se obsoletas;

b. as atividades de controle podem perder a eficácia ou deixar de ser executadas; ou

c. os objetivos podem mudar.

Diante dessas mudanças, a administração necessita monitorar continuamente se o funcionamento do gerenciamento de riscos corporativos permanece eficaz, podendo revisar as ações, caso necessário. Para o monitoramento e revisão funcionarem, é importante a discussão e definição de um plano sistematizado chamado de Plano de Monitoramento e Revisão.

Assim, o Plano terá como principal objetivo garantir que a construção, implementação e resultados do processo de gestão de riscos estão se concretizando conforme esperado. Além disso, busca-se também a melhoria contínua desse processo.

Diante da possibilidade de uma organização gerenciar diversos riscos, é possível que o gestor realize a pergunta abaixo no momento da implementação:

- Todos os riscos e medidas de tratamento contempladas no plano de ação serão acompanhados diretamente pela Alta Gestão?

Em regra, não. O monitoramento direto de todo o gerenciamento de riscos é realizado pela primeira linha. O acompanhamento e facilitação das ações da primeira linha são realizados por intermédio da segunda linha, que poderá ser realizado pelo comitê, Unidade de Controle Interno ou órgão equivalente de segunda linha . Já a Alta Gestão irá acompanhar o processo de uma forma mais consolidada através de indicadores e dashboads, caso existam. Além disso, a Alta Gestão poderá acompanhar diretamente a evolução de alguns tipos específicos de riscos e controles.

Em função disso, para efeito de acompanhamento da gestão de riscos de uma forma geral, o monitoramento ocorre através dos seguintes níveis: operacional, gerencial e estratégico.

Em relação ao monitoramento em **nível operacional**, ele é realizado pelos servidores e responsáveis pelo gerenciamento de riscos dos objetivos e/ou processos, e visa:

a) acompanhar a execução do plano de tratamento proposto;

b) verificar a eficácia dos controles/medidas de tratamento implementadas;

b) identificar mudanças que acarretem em alteração de controles/medidas de tratamento e;

c) atualizar as informações referentes ao gerenciamento de riscos.

Em relação ao monitoramento em **nível gerencial**, ele é realizado pelo grupo de trabalho ou comitê, Unidade de Controle Interno ou órgão equivalente de segunda linha, e tem como objetivo verificar se a primeira linha está cumprindo as ações de monitoramento listadas acima, bem como, em relação aos principais riscos, verificar a implementação e acompanhar a efetividade dos controles/medidas de tratamento definidas pelas áreas responsáveis.

Por fim, temos o monitoramento em **nível estratégico** dos riscos-chaves. Em regra, o interesse de acompanhamento direto da Alta Gestão reside nos seguintes tipos de riscos:

a) Riscos estratégicos, de integridade e de imagem,

b) Riscos cujo impacto seja alto ou muito alto

b) riscos residuais classificados na avaliação como alto, muito alto e críticos.

c) riscos cujas medidas de tratamento requeiram a sua ação direta.

Dessa forma, deve-se elaborar um plano de monitoramento e revisão, que contenha: a forma, os responsáveis e a periodicidade de realização. É interessante que o plano de monitoramento e análise crítica apresente, no mínimo, as seguintes informações:

I - Modelo de Planilha de Monitoramento;

II - Indicadores de desempenho, nos casos em que for possível o cálculo;

III - Responsáveis diretos pelo monitoramento contínuo dos controles adotados;

IV - Periodicidade do monitoramento;

Ações sugeridas:

- Estabelecer medidas de desempenho / indicadores;

- Definir a periodicidade e responsáveis pelo monitoramento do gerenciamento de riscos;

Importante

Quanto ao estabelecimento e acompanhamento dos indicadores:

a) Identifique os indicadores já existentes, se houver;

b) Avalie esses indicadores;

c) Identifique ponto de ajustes e proponha melhoria;

d) Foque nos riscos mais relevantes;

e) Realize a mensuração de forma sistemática e constante, ex: mensalmente, bimestralmente, etc.

5. EIXO: Implementação

Agora é a hora de colocar em prática tudo que foi definido pela organização. É o momento de entender o contexto, identificar, analisar, avaliar e tratar os riscos dos projetos, processos ou atividades selecionadas pela organização.

5.1. Pontos focais

1º PONTO FOCAL: ANÁLISE DE CONTEXTO E ESCOPO

ENTENDER O CONTEXTO

Antes de partir para o processo de avaliação de riscos (identificar, analisar, avaliar e tratar) é importante analisar e compreender os contextos externo e interno da organização.

Sugestão de aspectos a serem observados nessa etapa:

Na Organização	No Processo
Missão, Visão e Valores;	Objetivo do Processo;
Governança Corporativa;	Objetivo Estratégico associado;
Nível de Maturidade em GR;	Principais Forças, Fraquezas, Ameaças e Oportunidades;
Sistemas informatizados;	Partes interessadas.
Parcerias estabelecidas.	

DEFINIR E ANALISAR O ESCOPO

1. Através de critérios objetivos

Como exemplo de método de priorização de processos baseado em critérios objetivos, temos o do Ministério de Planejamento, Desenvolvimento e Gestão[4]. Nesse método, a avaliação é realizada através de dois enfoques: quantitativo e qualitativo.

Na **avaliação quantitativa**, os processos serão verificados quanto à Materialidade, quanto à necessidade de Recursos Humanos (qualificação técnica especializada) e quanto aos Recursos Tecnológicos para a execução do processo.

Na **avaliação qualitativa,** os processos serão verificados de acordo com os seguintes fatores relacionados aos processos: Processo Estratégico, Demandas do TCU, Demandas da CGU, Relevância do Processo, Valores Não Orçamentário e Reclamações Registradas na Ouvidoria.

O resultado final da avaliação classifica o processo através das faixas abaixo:

E – **Essencial:** expressa os processos mais significativos, que deverão ter prioridade sobre os demais no gerenciamento de riscos;

[4] https://www.gov.br/economia/pt-br/centrais-de-conteudo/publicacoes/planejamento/controle-interno/metodo_de_priorizacao_de_processos___v1_1.pdf

R – **Relevante:** expressa os processos de grande importância ou que merecem destaque, e que deverão ter uma prioridade média sobre os demais no gerenciamento de riscos;

M – **Moderado:** expressa os processos de menor importância, que deverão ter prioridade baixa sobre os demais no gerenciamento de riscos.

Na Secretaria da Controladoria Geral do Estado de Pernambuco também foi estabelecido um critério objetivo para priorização dos processos de maior agregação de valor, sendo observados os seguintes fatores: relevância estratégica (relevância para a realização dos objetivos-chave da organização), maturidade (prática de gestão consistente e padronizada) e imagem institucional (percepção da imagem da SCGE perante o Governo, os órgãos e entidades estaduais e a Sociedade).

Importante

Mesmo que os critérios objetivos de priorização sejam institucionalizados, a Alta Gestão pode retirar ou incluir algum processo na priorização de forma justificada.

2. Através de discussões internas

Outra forma de priorizar processos é através de discussões no âmbito estratégico da organização, sendo escolhidos os processos com base na experiência de gestores. Ressalte-se que a falta de critérios objetivos cria uma dependência das avaliações subjetivas dos integrantes da Alta Gestão que realizaram a priorização.

Por fim, é importante que seja realizada uma análise detalhada do processo objeto do gerenciamento de riscos. Um instrumento muito útil para essa análise é a Matriz SWOT. Por meio dela, a organização poderá discutir e sistematizar as oportunidades, ameaças, forças e fraquezas referentes ao processo específico.

Ações sugeridas:

• Definir critérios objetivos ou utilizar os utilizados por outros órgãos para priorizar os processos que serão objeto do gerenciamento de riscos.

• Utilizar a metodologia de Matriz SWOT para identificar ameaças, oportunidades, forças e fraquezas do processo objeto da identificação de riscos. Esse processo irá permitir uma discussão que facilitará a condução do gerenciamento nas fases seguintes.

2º PONTO FOCAL: IDENTIFICAÇÃO, ANÁLISE E AVALIAÇÃO DOS RISCOS

IDENTIFICAR OS RISCOS

É conveniente que a organização identifique os eventos de risco, causas e consequências potenciais. A finalidade desta etapa é gerar uma lista abrangente de riscos que possam evitar, reduzir, ou atrasar a realização dos objetivos. A identificação deve incluir todos os riscos, estando suas fontes sob o controle da organização ou não, bem como o exame de reações em cadeia provocadas por consequências específicas, incluindo os efeitos cumulativos e em cascata. Todas as causas e consequências significativas devem ser consideradas (ISO 31000:2009).

Para facilitar o entendimento, apresenta-se, na figura abaixo, os componentes de risco com as palavras que podem ajudar no momento de identificação de cada um deles.

Em relação ao momento de identificação dos componentes do risco, é possível que o gestor realize a pergunta abaixo no momento da implementação:

• Estou sem conseguir ter criatividade para identificar e descrever os componentes de risco. O que posso ler para me ajudar ?

Existem alguns documentos internos que podem auxiliar na discussão de alguns riscos, como, por exemplo, os listados abaixo:

- Fluxos de Processos Organizacionais
- Resultados da etapa da Definição do Contexto
- Experiências das Equipes Técnicas
- Relatórios de Auditoria
- Manifestações da Ouvidoria

Dica!

Em relação a identificação das causa, ela pode ser encontrada através da associação abaixo:

Causa = Fonte + Vulnerabilidade *

Exemplificativamente:

Fonte	Vulnerabilidade
Pessoas	Em número insuficiente
	Sem capacitação
	Com perfil inadequado
	Desmotivadas
Processos	Mal concebidos
	Sem manual ou instruções formalizadas
	Com ausência de segregação de funções
Sistemas	Obsoletos
	Sem integração
	Sem manuais de operação
	Inexistência de Controles de Acesso lógico/backups

Fonte	Vulnerabilidade
Infraestrutura Organizacional	Falta de clareza quanto a funções e responsabilidade
	Deficiências nos fluxos de informação e comunicação
	Centralização de responsabuilidades
	Delegações exorbitantes
Infraestrutura Física	Localização inadequada
	Instalações ou layouts inadequados
	Inexistência de controles de acesso físico
Tecnologia	Técnica de produção ultrapassada /produto obsoleto
	Inexistência de investimentos em P&D
	Tecnologia em proteção de patentes
	Processo produtivo sem proteção contra espionagem

É possível que o gestor traga durante o processo de gerenciamento de riscos a seguinte crítica seguida de questionamento:

- *É muito complicado identificar riscos e falhas da organização numa reunião com o meu chefe. Não tenho coragem para falar que o controle é falho, por exemplo. O que fazer?*

Existem diversas técnicas para identificar riscos e controle. O ISO 30.010 prevê diversas técnicas e discorre detalhadamente sobre cada uma delas. Em relação à indagação acima, existem técnicas, como é o caso do Método Delphi, que funciona através de respostas de forma anônima, sendo agregadas e compartilhadas com o grupo após rodadas de discussão.

IDENTIFICAR E AVALIAR OS CONTROLES EXISTENTES

Nesta etapa, serão identificados e avaliados os controles existentes no momento da identificação dos riscos. É nesse momento quando já se pensa em possíveis melhorias nos controles e se eles estão devidamente formalizados ou não.

ANALISAR E AVALIAR OS RISCOS

Na etapa de análise, deverá haver um exame das causas e consequências elencadas para possibilitar, respectivamente, a definição da probabilidade do evento ocorrer e do impacto caso o risco se materialize.

Na etapa de avaliação de riscos, deverá ser comparado o nível de risco encontrado durante o processo de análise com os critérios de risco estabelecidos pela organização, possibilitando, assim, a definição do tipo de resposta ao risco a ser dado.

Ações sugeridas:

- Promover oficinas para explicar quais procedimentos deverão ser realizados durante o processo de gerenciamento dos riscos. É interessante que os treinamentos sejam priorizados levando em consideração os processos e as áreas selecionadas para iniciar a implantação.

- Assegurar que os interesses das partes interessadas

sejam compreendidos e considerados em todas as etapas do processo;

• Realizar reuniões com as partes interessadas para identificar e avaliar os riscos de cada processo selecionado, podendo ser utilizadas técnicas para fomentar a sugestão de idéias, como a brainstorm.

• Se necessário, reunir diferentes áreas de especialização em conjunto para análise dos riscos;

• Elaborar uma lista abrangente de riscos e avaliar a probabilidade e o impacto, conforme critérios definidos pela organização. **Atentar que, em geral, a probabilidade está ligada às causas e o impacto às consequências imediatas nos objetivos do processo.**

• Descrever e avaliar os controles existentes considerando o conjunto de controles, independente se formais ou não.

• Registrar e relatar cada etapa do processo de gerenciamento de riscos.

3º PONTO FOCAL: RESPOSTA AOS RISCOS

TRATAR OS RISCOS

O tratamento de riscos é a etapa que envolve a seleção de medidas de controle a serem adotadas com o objetivo de reduzir o nível do risco, atuando de modo a mitigar a sua

probabilidade de ocorrência e/ou seu impacto.

A resposta aos riscos geralmente é detalhada através de um plano de ação, que contém, dentre outras informações, a ação necessária para responder ao risco (controle), prazo e responsável.

Ações sugeridas:

• Elaborar o plano de tratamento dos riscos levando em consideração a relação entre o custo e o benefício da proposição de novos controles.

• Evitar descrição genérica de proposição de controles. Quanto maior a especificação da ação, maior será a chance de aprovação do plano de ação e melhor será o acompanhamento.

• Para cada ação proposta no plano de ação, recomendamos associar apenas um responsável.

• Preencher no campo "prazo" uma data desafiadora e exequível que motive o responsável para a concretização do objetivo.

Importante

Em complemento ao conteúdo deste tópico 6, a SCGE disponibiliza em seu site o "Guia Prático de Gerenciamento de Riscos", que traz os aspectos práticos dessa atividade.

6. Conclusão

Neste documento foram expostas boas práticas e sugeridas ações para estruturação e implementação da gestão de riscos na sua organização. A inclusão da gestão de riscos na cultura e nas atividades da organização produzirá benefícios que impactarão desde o nível estratégico até o operacional.

Além disso, a gestão de riscos bem executada promoverá melhoria no desempenho da organização, dos seus serviços, resultando em melhores entregas à sociedade.

Para informações mais detalhadas, verificar os modelos de documentos disponibilizados no site da SCGE. Outras informações, entrar em contato com a Diretoria de Monitoramento, Avaliação e Controle, através do e-mail gestaoderiscos@cge.pe.gov.br

Referências bibliográficas

ABNT. Gestão de Riscos – Princípios e diretrizes. NBR ISO 31000. Associação. Brasileira de Normas Técnicas. 2009.

ABNT. Gestão de riscos - Diretrizes. NBR ISO 31000. Associação Brasileira de Normas Técnicas. 2018.

COSO. Gerenciamento de Riscos Corporativos Integrado com Estratégia e Performance – Sumário Executivo. Junho de 2017. Tradução: Instituto dos Auditores Internos do Brasil (IIA Brasil) e Pricewaterhousecoopers. Disponível em https://repositorio.cgu.gov.br/bitstream/1/41825/8/Coso_portugues_versao_2017.pdf. Acesso em 20 Jun. 2021.

BRASIL. Tribunal de Contas da União. 10 Passos para a Boa Gestão de Riscos. 31 p. Brasília : TCU, Secretaria de Métodos e Suporte ao Controle Externo (Semec), 2018b. Disponível em: https://portal.tcu.gov.br/10-passos-para-a-boa-gestao-de-riscos.htm. Acesso em: 20 Jun. 2021.