MANUAL DE GESTÃO DE RISCOS, CONTROLES INTERNOS E INTEGRIDADE

MINISTÉRIO DO DESENVOLVIMENTO REGIONAL

1ª Edição

Brasília 2020

Ministério do Desenvolvimento Regional

SUMÁRIO

Presidente da República
Jair Messias Bolsonaro

Ministro do Desenvolvimento Regional
Rogério Simonetti Marinho

Secretário Executivo
Claudio Xavier Seefelder Filho

Secretário-Adjunto da Secretaria Executiva
Daniel de Oliveira Duarte Ferreira

Chefe de Assessoria Especial de Controle Interno, Substituto
Rodrigo de Paula Chiari

Elaboração
Coordenação-Geral de Inteligência e Riscos

Flávia Amaral Silva de Sousa (Coordenadora-Geral)
Eduardo Augusto Lourenço Freitas (Coordenador)

Colaboração
Coordenação-Geral de Governança e Integridade

Rodrigo de Paula Chiari (Coordenador-Geral)
Marianne Macedo de Carvalho (Coordenadora)

Endereço:
Ministério do Desenvolvimento Regional (MDR)
Esplanada dos Ministérios, Bloco E, S/N - Zona Cívico-Administrativa, 8º andar
Brasília/DF - CEP 70 067-901
Telefone: (61) 2034-5815
CEP: 70067-900, Brasília – DF, Brasil

INTRODUÇÃO

A Sociedade anseia por uma administração pública ágil e eficiente, capaz de implementar políticas e programas de governo que entreguem o melhor valor para a população.

Diante disso, a adoção de práticas e estratégias eficazes de gestão exige responsabilidades e deveres do governo, bem como ações de governança e de gestão das instituições públicas, cujo objetivo precípuo é entregar o melhor valor público.

As incertezas que podem afetar os objetivos são algo inerente à atividade exercida por qualquer instituição e podem ter origem em diversos fatores, tais como: econômico, social, operacional, político e tecnológico. Assim, as incertezas representam os riscos aos quais uma organização está sujeita e, portanto, devem ser identificados, analisados e tratados, visando sempre a menor interferência possível nos objetivos do órgão.

A Gestão de Riscos, os Controles Internos e a Integridade constituem mecanismos que geram valor às instituições e aos seus processos quando atuam de forma coordenada, buscando tratar as incertezas que podem impedir ou dificultar o alcance dos objetivos da organização, bem como quando promovem o comportamento íntegro. Esses mecanismos visam aumentar a qualidade das decisões dos gestores públicos para o alcance do interesse público.

Posto isso, o objetivo deste manual é levar a todos os servidores, em especial dos gestores, orientações quanto à aplicação da metodologia de Gestão de Riscos do Ministério do Desenvolvimento Regional (MDR), a qual se encontra no Anexo IV, em conjunto com o Programa de Integridade do MDR.

Além dos procedimentos a serem empregados na aplicação da metodologia, este manual fornecerá conceitos, responsabilidades e diretrizes sobre boas práticas, a fim de demonstrar aos gestores a importância do seu papel e de realizar o gerenciamento de riscos, controles e integridade para o alcance dos objetivos institucionais do Ministério do Desenvolvimento Regional. A título de esclarecimento, no Anexo I, há uma lista de conceitos relevantes ao entendimento do tema.

O presente manual foi inspirado no Manual de Integridade, Gestão de Riscos e Controles Internos do antigo Ministério do Planejamento, Desenvolvimento e Gestão considerando que aquele órgão teve como base para sua Gestão de Riscos o mesmo *framework* utilizado pelo MDR.

Ademais, este manual se apresenta como um ponto inicial de conhecimento, não esgotando os temas aqui abordados, e o aprofundamento dos assuntos poderá ser adquirido em diversas outras publicações mais específicas sobre cada tema, permitindo ao leitor um processo contínuo de aprendizado.

NORMAS DA ADMINISTRAÇÃO PÚBLICA FEDERAL

No âmbito da Administração Pública Federal, existe um conjunto de normas e regulamentações relacionadas à Gestão de Riscos, Controles Internos e Integridade que devem ser observadas.

Com a publicação da IN Conjunta CGU/MP nº 1, de 10 de maio de 2016, os órgãos e entidades do Poder Executivo Federal passaram a promover medidas para institucionalizar práticas relacionadas à gestão de riscos, aos controles internos e à governança. A IN CGU/MP nº 1/2016 definiu os princípios, os objetivos e as estruturas basilares desses temas.

Na sequência, foi publicado o Decreto nº 9.203, de 22 de novembro de 2017, que dispõe sobre a política de governança da Administração Pública Federal direta, autárquica e fundacional. Esse Decreto também define os princípios, as diretrizes e os mecanismos para o exercício da boa governança, bem como institui o Comitê Interministerial de Governança (CIG).

Ambos os normativos definiram a integridade como um princípio da governança e o Decreto nº 9.203, de 2017, determina que os órgãos e as entidades da administração direta, autárquica e fundacional instituam seus programas de integridade com o objetivo de promover a adoção de medidas e ações institucionais destinadas à prevenção, à detecção, à punição e à remediação de fraudes e atos de corrupção.

Assim, a CGU publicou a Portaria nº 1089, de 25 de abril de 2018, que estabelece orientações para que os órgãos e as entidades da administração pública federal direta, autárquica e fundacional adotem procedimentos para a estruturação, a execução e o monitoramento de seus programas de integridade e dá outras providências. No ano seguinte, publicou a Portaria nº 57, de 04 de janeiro de 2019, alterando a Portaria CGU nº 1.089, de 2018, que estabelece orientações para que os órgãos e as entidades da administração pública federal direta, autárquica e fundacional adotem procedimentos para a estruturação, a execução e o monitoramento de seus programas de integridade e dá outras providências.

No âmbito do Ministério do Desenvolvimento Regional, foram publicados os seguintes normativos:

- Portaria MDR nº 1.427, de 20 de maio de 2020 – institui o Comitê Interno de Governança (Cigov);
- Portaria MDR nº 1.927, de 12 de agosto de 2020 – institui o Programa de Integridade do Ministério do Desenvolvimento Regional;
- Portaria MDR nº 1.469, de 26 de maio de 2020 – altera a Portaria MDR nº 1.927, de 12 de agosto de 2019, que institui o programa de Integridade do Ministério do Desenvolvimento Regional.

- Portaria MDR nº 2.711, de 19 de novembro de 2019 – dispõe sobre as competências dos Agentes de Integridade do Programa de Integridade do Ministério do Desenvolvimento Regional e designa servidores para o exercício da função.
- Portaria MDR nº 1.807, de 25 de junho de 2020 – altera a Portaria nº 2.711, de 2019, que dispõe sobre as competências dos Agentes de Integridade do Programa de Integridade do Ministério do Desenvolvimento Regional e designa servidores para o exercício da função.
- Portaria nº 948, de 08 de abril de 2020 – estabelece o funcionamento da Ouvidoria-Geral e define os procedimentos a serem aplicados às manifestações de ouvidoria e aos pedidos de acesso à informação recebidos no âmbito do Ministério do Desenvolvimento Regional.
- Política e Metodologia de Gestão de Riscos - esses documentos foram apresentados ao CIGOV em reunião do dia 16 de janeiro de 2020, tendo sido aprovados. Contudo, após mudanças na gestão e na estrutura do MDR, no dia 27 de julho de 2020, houve nova submissão desses dois documentos ao CIGOV, tendo sido suas aprovações ratificadas.

MODELOS DE GESTÃO DE RISCO

Quando se fala em gestão de riscos, existem vários *frameworks* ou modelos de gestão de riscos utilizados mundialmente. Os modelos de gestão de riscos trazem as regras gerais que uma instituição deve se basear para um bom gerenciamento de riscos.

Os modelos que mais se destacam e são amplamente utilizados são o COSO, a ISO 31000 e o Orange Book, os quais serão brevemente apresentados nos tópicos abaixo.

O Ministério do Desenvolvimento Regional, na elaboração de sua metodologia de gestão de riscos, utilizou como base o modelo apresentado pelo COSO II ou COSO-ERM.

COSO

O COSO (*The Comitee of Sponsoring Organizations*), criado em 1985, é uma entidade privada sem fins lucrativos e com objetivo de aperfeiçoar a qualidade de relatórios financeiros, em especial quanto à ocorrência de fraudes.

Em 1992, o COSO publicou o guia *Internal Control – Integrated Framework* (COSO-IC ou COSO I) com o objetivo de orientar as organizações quanto às melhores práticas de controle interno.

Com a obra de 2004 "*Enterprise Risk Management – Integrated Framework*" (COSO ERM ou COSO II), tradução para o português "Gerenciamento de Riscos Corporativos – Estrutura Integrada", o COSO realizou um trabalho mais voltado para o gerenciamento de riscos corporativos, definindo esse termo assim:

> *É um 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. (COSO ERM, 2004)*

De acordo com o COSO II, 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 que são classificados em quatro categorias:

- Estratégicos - Metas gerais, alinhadas com sua missão;
- Operações - Utilização eficaz e eficiente dos recursos;
- Comunicação - Confiabilidade de relatórios; e
- Conformidade - Cumprimento de leis e regulamentos aplicáveis.

Comparado ao guia publicado em 1992, o COSO II traz um avanço justamente quanto à categoria de objetivos estratégicos, pois de nada adiantaria as operações serem eficientes, os relatórios confiáveis e as leis e os regulamentos serem cumpridos, se não há uma estratégia a ser alcançada.

Após esse avanço, a figura conhecida como "cubo do coso" foi redesenhada e passou a ser disposta assim:

Fonte: COSO (2004)

FIGURA 1 - 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 perpassa a gestão de riscos. Por fim, a dimensão frontal apresenta os oito componentes do gerenciamento de riscos, que serão abordados no capítulo de Gestão de Riscos deste manual, representando o que é necessário fazer, de forma integrada, para atingir os objetivos elencados na face superior.

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".

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; e
- Os riscos na execução da estratégia.

Fonte: COSO (2017)

FIGURA 2 - MODELO COSO ERM

Outro ponto importante na atualização de 2017 é o refinamento entre apetite a riscos e tolerância a riscos, agora com enfoque na variação aceitável do desempenho.

A primeira parte da publicação de 2017 oferece uma perspectiva dos conceitos atuais 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.

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

FIGURA 3 - COMPONENTES COSO 2017

ISO 31000

A ABNT NBR ISO 31000 foi elaborada pela Comissão de Estudo Especial de Gestão de Riscos (ABNT/CEE-63), sendo uma adoção idêntica, em conteúdo técnico, estrutura e redação, à ISO 31000:2009, preparada pelo *Technical Commitee risk management*, conforme ISO/IEC Guide 21-1:2005.

No ano de 2018, foi elaborada pela mesma comissão de Estudo Especial de Gestão de Riscos (ABNT/CEE-063) a segunda edição (ABNT NBR ISO 31000:2018), a qual cancela e substitui a edição anterior (ABNT NBR ISO 31000:2009).

Segundo a ISO 31000:2018, "Gerenciar riscos é iterativo e auxilia as organizações no estabelecimento de estratégias, no alcance de objetivos e na tomada de decisões fundamentadas. Gerenciar riscos é parte da governança e liderança, e é fundamental para a maneira como a organização é gerenciada em todos os níveis. Isto contribui para a melhoria dos sistemas de gestão. Gerenciar riscos é parte de todas as atividades associadas com uma organização e inclui interação com as partes interessadas."

Esse modelo de gestão de riscos 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 for 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 dos objetivos.

Os princípios elencados na ISO 31000:2018 fornecem orientações sobre as características da gestão de riscos eficaz e eficiente, comunicando seu valor e explicando sua intenção e propósito.

Já o objetivo da estrutura da gestão de riscos é apoiar a organização na integração da gestão de riscos em atividades significativas e funções.

E 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.

Os princípios, a estrutura e o processo, descritos na figura a seguir, são a base para gerenciar os efeitos da incerteza nos objetivos da organização, e podem ser adaptados ou melhorados, a fim de que a gestão de riscos seja eficiente, eficaz e consistente.

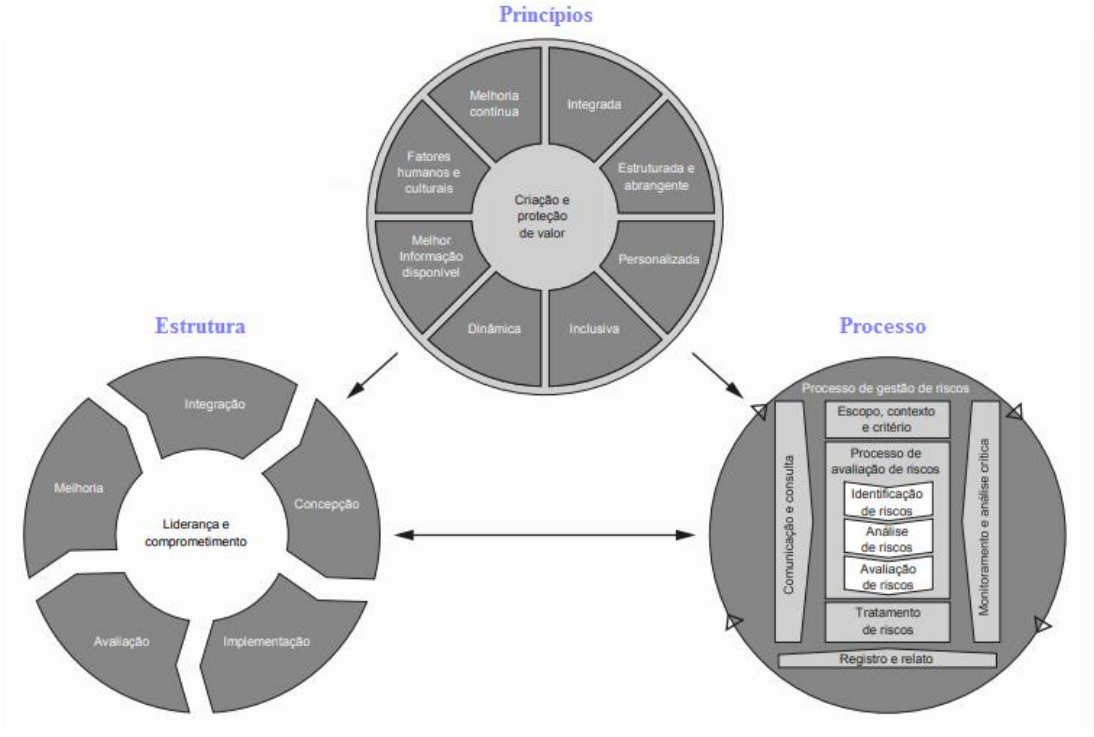


FIGURA 4 - PRINCÍPIOS, ESTRUTURA E PROCESSO ISO 31000

FONTE: ABNT NBR ISO 31000:2018

A organização deve avaliar suas práticas, processos e quaisquer lacunas existentes, abordando-os, com base nos princípios, no âmbito da estrutura e do processo apresentados pela ISO 31000:2018, personalizando seu funcionamento a fim de que a gestão de riscos atenda às necessidades da organização.

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 é compatível com padrões internacionais de gerenciamento de riscos, como COSO GRC e ISO 31000.

Segundo o Orange Book, mais importante que uma organização seguir qualquer norma ou estrutura de risco 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:

Fonte: UK (2004 – tradução livre)

FIGURA 5 - ESTRUTURA ORANGE BOOK

O modelo funciona em um ambiente em que o apetite de risco tenha sido definido e esse conceito perpassa por 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.

A estrutura de gerenciamento de riscos suporta a identificação consistente de riscos e a gestão de oportunidades e de ameaças dentro dos níveis de uma organização, apoiando a transparência, a inovação e a excelência na consecução dos objetivos.

No gerenciamento de risco, segundo esse modelo, para que a estrutura do modelo de gestão seja considerada eficaz, os seguintes princípios devem ser aplicados:

A. O gerenciamento de riscos é parte essencial da governança e da liderança, e é fundamental na maneira como a organização é dirigida, gerenciada e controlada em todos os níveis;
B. A gestão de riscos deve ser parte integrante de todas as atividades organizacionais para apoiar a tomada de decisão na consecução dos objetivos;
C. A gestão de riscos deve ser colaborativa e baseada nas melhores informações disponíveis;

D. O processo de gerenciamento de riscos deve ser estruturado, a fim de incluir:

a. Identificação e avaliação de riscos para determinar e priorizar como os riscos devem ser gerenciados;
b. A seleção, o desenho e a implementação de opções de tratamento de risco que visem mitigar os riscos para níveis aceitáveis;
c. O design e a operação de sistemas integrados, bem como o monitoramento e comunicação de riscos;
d. Relatórios oportunos, precisos e úteis a fim de melhorar a qualidade da tomada de decisão; e
e. Apoiar a gestão no cumprimento de suas responsabilidades.

A gestão de riscos deve ser continuamente aprimorada por meio de aprendizado e experiência.

POLÍTICA E METODOLOGIA

A Portaria MDR nº 1.427, de 20 de maio de 2020, em seu art. 1º, instituiu o Comitê Interno de Governança (Cigov), com a finalidade de assessorar o Ministro de Estado do Desenvolvimento Regional na execução da política de governança da administração pública federal, em consonância com os princípios, diretrizes e mecanismos estabelecidos pelo Decreto nº 9.203, de 22 de novembro de 2017.

Conforme o art. 2º da Portaria MDR nº 1.427/2020, são membros titulares do Comitê Interno de Governança: (i) o Ministro de Estado do Desenvolvimento Regional, que o presidirá; (ii) o Secretário-Executivo; (iii) o Secretário de Coordenação Estrutural e Gestão Corporativa; (iv) o Secretário Nacional de Proteção e Defesa Civil; (v) o Secretário Nacional de Segurança Hídrica; (vi) o Secretário Nacional de Mobilidade e Desenvolvimento Regional e Urbano; (vii) o Secretário Nacional de Habitação; e (viii) o Secretário Nacional de Saneamento.

A referida Portaria também define que compete ao Secretário-Executivo coordenar as atividades do Comitê Interno de Governança, bem como que o Chefe da Assessoria Especial de Controle Interno e o Consultor Jurídico do Ministério do Desenvolvimento Regional participarão das reuniões do Comitê Interno de Governança, com o fim de prestar assessoramento, em consonância com suas competências específicas.

Outros destaques referem-se à Secretaria-Executiva do Comitê Interno de Governança, a qual será exercida pela Secretaria de Coordenação Estrutural e Gestão Corporativa, e que o Comitê Interno de Governança será assessorado pela Comissão Técnica do Comitê Interno de Governança (CT-Cigov), constituída com a finalidade de subsidiar as reuniões e as deliberações de competência do Comitê.

A Comissão Técnica do Comitê Interno de Governança será constituída pelos seguintes membros: (i) Diretor de Gestão Estratégica e Coordenação Estrutural; (ii) Coordenador-Geral de Gestão da Secretaria Nacional de Proteção e Defesa Civil; (iii) Coordenador-Geral de Gestão Integrada da Secretaria Nacional de Segurança Hídrica; (iv) Coordenador-Geral de Gestão Integrada de Mobilidade da Secretaria Nacional de Mobilidade e Desenvolvimento Regional e Urbano; (v) Coordenador-Geral de Gestão Integrada de Desenvolvimento Regional e Urbano da Secretaria Nacional de Mobilidade e Desenvolvimento Regional e Urbano; (vi) Coordenador-Geral de Gestão Integrada da Secretaria Nacional de Habitação; e (vii) Coordenador-Geral de Gestão Integrada da Secretaria Nacional de Saneamento.

A Política de Gestão de Riscos, no âmbito do MDR, possui como finalidade estabelecer conceitos, princípios, objetivos, diretrizes, competências e responsabilidades da gestão de riscos.

A Política aplica-se aos órgãos de assistência direta e imediata ao Ministro de Estado, aos órgãos específicos singulares e às unidades descentralizadas, abrangendo os servidores, prestadores de serviço, colaboradores, estagiários, consultores externos e quem, de alguma forma, desempenhe atividades no MDR. Ressalte-se que devido às mudanças de estrutura do Ministério, promovidas pelo Decreto nº 10.290, de 24 de março de 2020, foram necessárias alterações nessa política, a qual foi ratificada pelo Cigov em reunião realizada no dia 27/07/2020.

A estrutura do Sistema de Gestão de Riscos do MDR (SGR-MDR) é definida pelo art. 8º da Política de Gestão de Riscos, e possui como instâncias responsáveis: (i) o Comitê Interno de Governança (Cigov); (ii) a Secretaria Executiva (SECEX); (iii) as Unidades Organizacionais; e (iv) os Gestores de risco.

O Comitê Interno de Governança representa o nível estratégico da ação, sendo responsáveis por decisões estratégicas e diretrizes no âmbito da gestão de riscos, a Secretaria Executiva representa o nível tático da ação, sendo responsáveis pela coordenação das ações, monitoramento do SGR-MDR e consolidação de informações estruturadas sobre riscos, e as Unidades Organizacionais e os Gestores de riscos representam o nível operacional da ação, sendo responsáveis pelo gerenciamento das ações de identificação, avaliação e tratamento dos riscos.

A Política visa estruturar os processos de gerenciamento dos riscos de forma a se integrarem ao planejamento estratégico, aos processos e às políticas do MDR, considerando as características específicas e a cultura organizacional do Ministério.

A partir da política de gestão de riscos, e de forma aderente, foi elaborada a Metodologia de Gestão de Riscos do Ministério do Desenvolvimento Regional.

Essa metodologia esclarece que gerenciar riscos é um processo de melhoria contínua de identificação, avaliação, administração e controle de potenciais eventos de riscos, sejam eles ameaças ou

oportunidades. Esta gestão é importante na medida em que permite aos gestores e tomadores de decisão avaliar a factibilidade no alcance dos objetivos organizacionais, e assim decidir pela manutenção ou revisão de procedimentos para garantir o sucesso da organização. O desenvolvimento de uma gestão de riscos eficaz e eficiente, ao aumentar a probabilidade de atingimento dos objetivos do MDR, contribuirá ao cabo para uma condução mais eficiente das políticas públicas.

Dessa forma, o capítulo seguinte irá detalhar as etapas da metodologia, visando orientar, de forma prática e direta, como cada uma dessas etapas deve ser realizada, com indicação de eventuais técnicas complementares, de forma a estruturar mais adequadamente o método de gerenciamento de riscos adotado pelo MDR.

GESTÃO DE RISCOS

O processo de gestão de riscos definido na Metodologia do MDR está aderente às diretrizes definidas na Política de Gestão de Riscos do MDR, a qual, no seu artigo 6º, define, no mínimo, as seguintes etapas:

I. Análise do ambiente e dos objetivos;
II. Identificação dos riscos;
III. Avaliação dos riscos;
IV. Resposta aos riscos;
V. Monitoramento e Comunicação.

FIGURA 6 - ETAPAS DA GESTÃO DE RISCOS

Antes de detalhar as etapas, cumpre informar que, para a implementação do gerenciamento de riscos, será utilizado o sistema informatizado denominado Agatha para documentar as etapas da gestão de riscos, o qual está disponível em https://agatha.mdr.gov.br. Para orientações específicas do sistema e de como solicitar o acesso, veja o manual disponível no Anexo VII.

ANÁLISE DO AMBIENTE E DOS OBJETIVOS

Esta etapa trata do levantamento e registro dos aspectos externos e internos essenciais ao alcance dos objetivos institucionais, permitindo a compreensão clara do ambiente em que a organização se insere e a identificação dos fatores que podem influenciar a capacidade da organização de atingir os resultados planejados.

A análise do ambiente tem a finalidade de colher informações para apoiar a identificação de eventos de riscos, bem como contribuir para a escolha de ações mais adequadas para assegurar o alcance dos objetivos do macroprocesso/processo.

Quanto ao Ambiente Interno, é importante verificar elementos atinentes à integridade, valores éticos, competência das pessoas, estrutura de governança do Ministério e da unidade, bem como as políticas e as práticas desenvolvidas pela área de gestão de pessoas.

No tocante à Fixação de Objetivos, inclui verificar, em todos os níveis da unidade (departamentos, divisões, processos e atividades), se os objetivos foram fixados e comunicados, se estão alinhados à missão e à visão do Ministério. Essas informações poderão ser obtidas por meio do planejamento estratégico, de relatórios gerenciais, relatórios dos órgãos de fiscalização e controle, entre outros.

Após essas definições, deve-se registrar o objetivo geral do processo, as leis e regulamentos e os sistemas utilizados na sua execução. Essas informações deverão estar consonantes com a cadeia de valor do Ministério/unidade e com o mapeamento do processo, caso já exista.

Uma importante ferramenta para auxiliar nesta etapa da gestão de riscos é a Análise de *Swot*, por meio da qual são identificadas forças e fraquezas (ambiente interno) e oportunidades e ameaças (ambiente externo), conforme detalhamento na figura abaixo.

FIGURA 7 - ANÁLISE SWOT

Todas as informações coletadas (normas, fluxograma, responsáveis, etc.) são fundamentais para a realização das demais etapas do gerenciamento de riscos, controles internos da gestão e integridade. Esses dados e documentos deverão ser arquivados a título de evidência, caso, posteriormente, haja algum questionamento dos órgãos de controle. Poderá ser criado um processo no SEI ou incluídos os documentos no anexo do Sistema Ágatha.

Fator relevante a ser definido e que deve ser formalizado é o escopo do processo. É de suma importância que se registre qual(is) etapa(s) do processo se está(ão) avaliando no processo de gerenciamento dos riscos, qual o início o e o fim da análise. É o caso, por exemplo, do processo de contratação que pode ter como escopo apenas a fase interna da licitação ou as fases interna e externa, até a assinatura do contrato, se houver. Essa escolha deve ser feita pela equipe que está analisando o processo e deverá ser devidamente registrada no Sistema Ágatha.

De acordo com a ISO 31000, as entradas para o processo de gerenciar riscos são baseadas em fontes de informação, tais como dados históricos, experiências, retroalimentação das partes interessadas, observações, previsões, e opiniões de especialistas. Entretanto, convém que os tomadores de decisão se informem e levem em consideração eventuais limitações dos dados e modelagem utilizados, bem como a possibilidade de divergências entre especialistas. E tudo isso deve ser devidamente registrado.

IDENTIFICAÇÃO DOS RISCOS

A etapa de identificação dos riscos envolve reconhecimento, descrição e registro do evento de risco, com a caracterização de suas prováveis causas e possíveis consequências, caso o evento ocorra. Convém que pessoas com um conhecimento adequado sejam envolvidas na identificação dos riscos.

Nesta etapa, deverá ser desenvolvida uma lista de eventos de riscos que podem comprometer negativamente os resultados e o alcance dos objetivos, afetando o valor público a ser entregue à sociedade. É relevante não deixar de incluir nessa análise os resultados e as informações registrados na primeira etapa (análise do ambiente e dos objetivos).

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

O risco não deve ser descrito simplesmente como o "não alcance" do objetivo do processo. A descrição do risco deve prover *insights* sobre o que pode dar errado no processo.

Nesta etapa, para facilitar, pode-se pensar em algumas perguntas, tais como: o que pode dar errado neste processo, quais ativos (recursos, informações, reputação, legalidade) estão em risco; de quais fontes provêm; com quem está o risco; quais fatores podem restringir o desempenho do programa, da política ou do processo; etc. A título de auxílio, há, no Anexo V, uma lista com alguns eventos de riscos operacionais.

Posteriormente à definição dos riscos, deverão ser elencadas todas as possíveis causas e consequências. Como apoio à coleta estruturada de informações, poderão ser utilizadas técnicas como *Brainstorming*, Diagrama de *Ishikawa*, *Bow-Tie*, entrevista com especialistas, e análise de cenários. Algumas dessas técnicas estão descritas na norma da ISO 31010.

Dessa forma, a ideia é a seguinte:

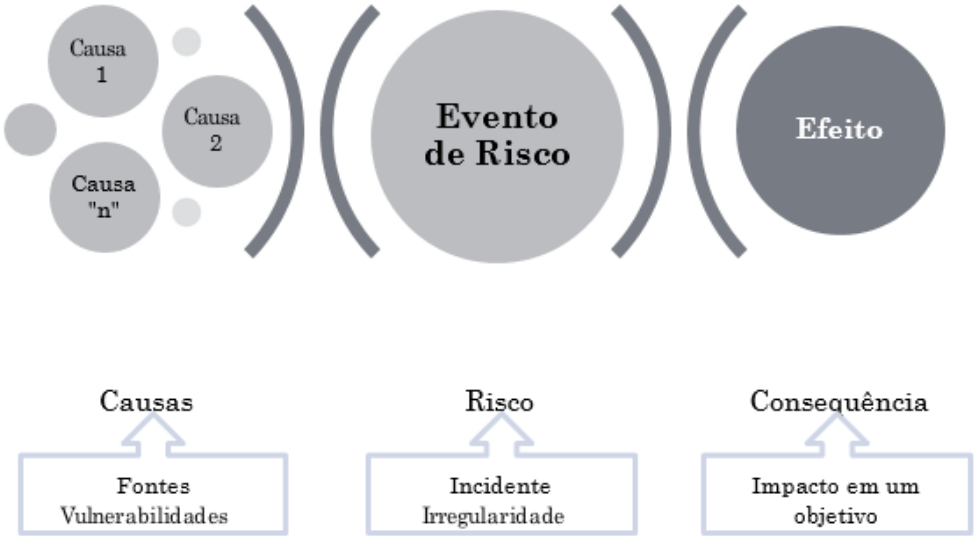


FIGURA 8 - COMPONENTES DO EVENTO DE RISCO

Causas: condições que dão origem à possibilidade de um evento ocorrer, também chamadas de fatores de riscos e podem ter origem no ambiente interno e externo.

Risco: possibilidade de ocorrência de um evento que venha a ter impacto no cumprimento dos objetivos.

Consequência: o resultado de um evento de risco sobre os objetivos do processo

Nesta etapa, sugere-se a identificação de todos os riscos, mesmo que suas fontes (causas) não estejam sob o controle do Ministério/unidade ou não sejam evidentes. Além de identificar o que pode acontecer, é necessário considerar possíveis causas e cenários que mostrem quais consequências podem ocorrer.

A sintaxe a seguir para descrição de aspectos envolvendo um evento de risco auxilia na reflexão e desenvolvimento desta etapa:

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

Depois de se ter(em) definido o(s) risco(s), suas causas e consequências, deve-se classificar esse(s) riscos, de acordo com as seguintes categorias definidas na Metodologia do MDR:

- **Operacional:** eventos que podem comprometer as atividades da unidade, normalmente associados a falhas, deficiência ou inadequação de processos internos, pessoas, infraestrutura e sistemas, afetando o esforço da gestão quanto à eficácia e à eficiência dos processos organizacionais;

- **Orçamentário:** eventos que podem comprometer a capacidade da unidade de contar com os recursos orçamentários necessários à realização de suas atividades ou eventos que possam comprometer a própria execução orçamentária;

- **Reputação:** eventos que podem comprometer a confiança da sociedade em relação à capacidade da unidade em cumprir sua missão institucional interferindo na imagem do órgão;

- **Fiscal:** eventos que podem afetar negativamente o equilíbrio das contas públicas;

- **Conformidade:** eventos que podem afetar o cumprimento de leis e regulamentos aplicáveis;

- **Social:** eventos que podem comprometer o valor público esperado ou percebido pela sociedade em relação ao resultado da prestação de serviços públicos da instituição; e

- **Integridade:** eventos relacionados a corrupção, fraudes, irregularidades e/ou desvios éticos e de conduta, que possam comprometer os valores preconizados pelo Ministério e a realização de seus objetivos.

Caso o evento de risco esteja associado a duas ou mais categorias de classificação, deverá ser escolhida a categoria que reflita o aspecto mais relevante quanto ao impacto que o evento de risco poderá trazer, caso se materialize.

No tocante ao risco à integridade, no item RISCOS DE INTEGRIDADE deste Manual há um detalhamento sobre seu conceito e exemplos que facilitarão identificar esse tipo de risco. Importante salientar que o risco à integridade não deve ser entendido apenas em termos de infração às normas e leis, mas sim de maneira mais ampla, englobando atos de fraudes, abuso de poder/influência, conflito de interesses, uso indevido e vazamento de informação sigilosa, como também práticas antiéticas.

AVALIAÇÃO DOS RISCOS

A etapa de avaliação dos riscos visa promover o entendimento do nível do risco e de sua natureza, especialmente quanto à estimativa da probabilidade de ocorrência e do impacto destes eventos identificados como risco nos objetivos dos processos organizacionais. Normalmente as causas se relacionam à probabilidade de o evento ocorrer e as consequências ao impacto, caso o evento se materialize.

Inicialmente, deverá ser feita uma avaliação do risco inerente (risco bruto, sem considerar qualquer controle), em seguida, será feita uma análise do(s) controle(s) já existente(s) e, por fim, do risco residual (considerando os controles identificados e avaliados quanto ao desenho e a sua execução), conforme figura abaixo.

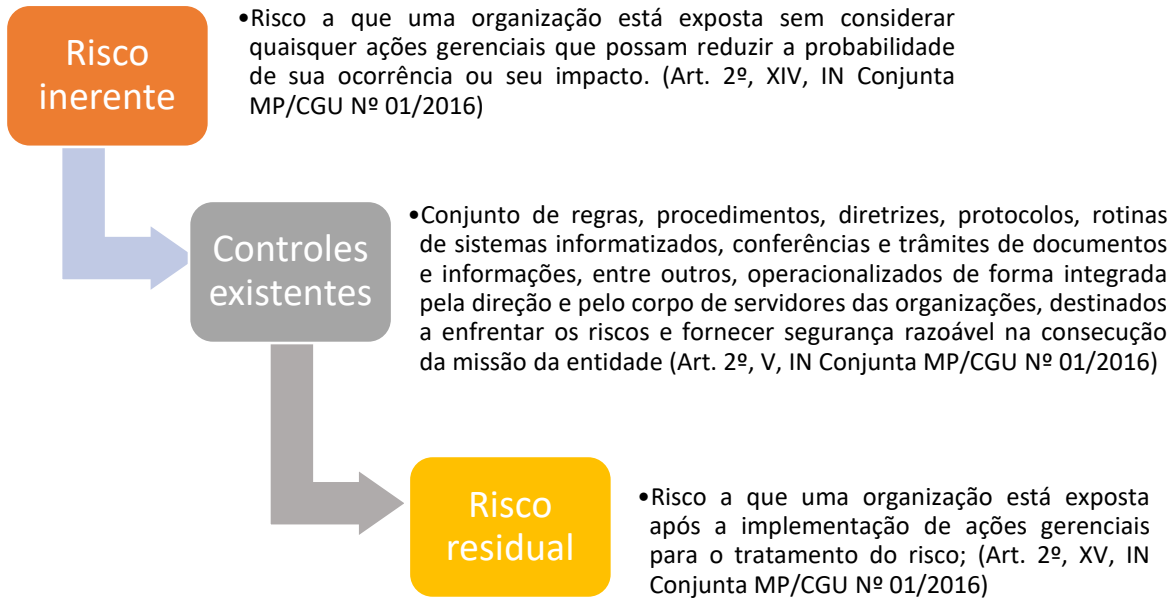


FIGURA 9 - SUB-ETAPAS DA AVALIAÇÃO DOS RISCOS

Avaliação do Risco Inerente

A avaliação do risco inerente deve ser feita quanto à probabilidade com base em avaliação quantitativa ou qualitativa que utilizará conhecimento técnico e experiências vivenciadas dos partícipes no processo a ser avaliado e, sempre que possível, será feita também uma avaliação quantitativa, com base nos dados estatísticos de eventos de riscos já materializados, por determinado período de tempo ou média

histórica disponível. Nesse caso, é também possível o uso de técnicas de apoio à coleta estruturada de informações.

Convém que sejam estabelecidos e ressaltados fatores como a divergência de opinião entre especialistas, a incerteza, a disponibilidade, a qualidade, a quantidade e a contínua pertinência das informações, ou as limitações sobre a modelagem. A análise de riscos pode ser realizada com diversos graus de detalhe, dependendo do risco, da finalidade da análise e das informações, dados e recursos disponíveis.

A avaliação da probabilidade utiliza da relação de aspecto avaliativo, frequência e valor do peso para apuração do risco, em cinco níveis, conforme tabela abaixo:

Peso	Faixa	Aspecto avaliativo	Frequência observada/esperada
1	Muito baixa	evento que pode ocorrer apenas em circunstâncias excepcionais	≤ 20%
2	Baixa	evento pode ocorrer em algum momento	> 20% e ≤ 40%
3	Média	evento deve ocorrer em algum momento	> 40% e ≤ 60%
4	Alta	evento deve ocorrer na maioria das circunstâncias	> 60% e ≤ 80%
5	Muito alta	evento com altíssima probabilidade de ocorrência	> 80%

TABELA 1 - DADOS DA PROBABILIDADE

A avaliação de **impacto** utilizará os seguintes fatores de análise e pesos de distribuição caso o evento de risco ocorra:

Impacto - Fatores para Análise						
	Estratégico-Operacional				Econômico-Financeiro	Peso
	Resultados nas Políticas Públicas Setoriais	Resultados Organizacionais (entregas estratégicas e PPA)	Conformidade / Regulação	Imagem / Reputação	Orçamentário / Financeiro	
	25%	20%	15%	10%	30%	100%
Orientações para atribuição de pesos	Impacto muito alto nas políticas públicas	Impacto muito alto nas metas estratégicas ou do PPA	Pode acarretar interrupção das atividades	Com destaque na mídia nacional e internacional, podendo atingir os objetivos estratégicos e a missão	> = 25%	5-Muito alto
	Impacto alto nas políticas públicas	Impacto alto nas metas estratégicas ou do PPA	Pode acarretar ações de caráter pecuniários (multas/dano ao erário)	Com algum destaque na mídia nacional, provocando exposição significativa	> = 10% < 25%	4-alto
	Impacto moderado nas políticas públicas	Impacto moderado nas metas estratégicas ou do PPA	Pode acarretar ações de caráter corretivo (determinação)	Pode chegar à mídia provocando a exposição por um curto período de tempo	> = 3% < 10%	3-Moderado
	Impacto baixo nas políticas públicas	Impacto baixo nas metas estratégicas ou do PPA	Pode acarretar ações de caráter orientativo (recomendação)	Tende a limitar-se às partes envolvidas	> = 1% < 3%	2-Baixo
	Pouco ou nenhum impacto	Pouco ou nenhum impacto nas metas estratégicas ou do PPA	Pouco ou nenhum impacto	Impacto apenas interno/sem impacto	< 1%	1-Muito baixo

TABELA 2 - DADOS DO IMPACTO

É desejável que a consistência das percepções de probabilidade e impacto seja sustentada pelo registro de evidências, como dados, documentos, relatórios e documentos constantes no SEI e, se possível, do Sistema Ágatha.

A multiplicação da avaliação de probabilidade e impacto forma o resultado final da avaliação de risco inerente, o qual está inserido em um dos 4 (quatro) níveis da Matriz de Risco: Pequeno (>3); Moderado (entre 4 e 6); Alto (entre 8 e 12); e Crítico (entre 15 e 25).

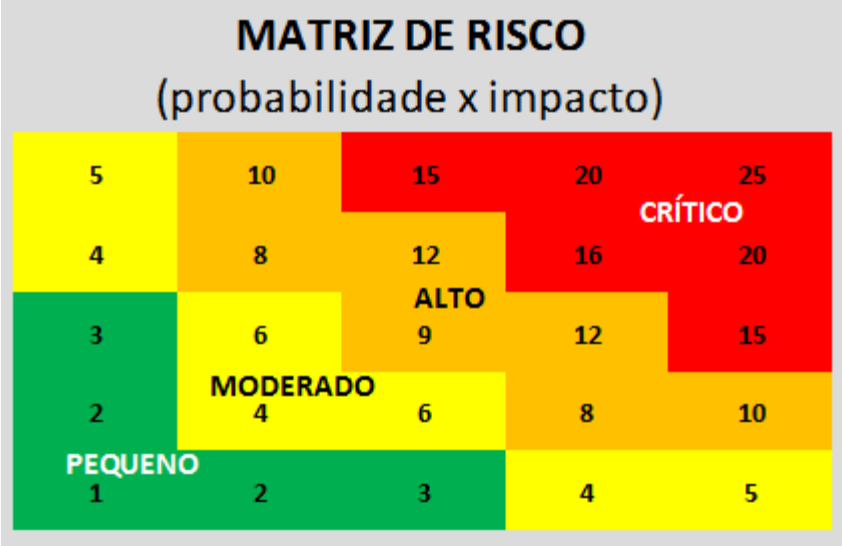


FIGURA 10 - MATRIZ DE RISCOS

Avaliação dos Controles Existentes

A próxima ação é a avaliação dos controles existentes. Assim, uma vez mensurado o risco inerente, deve-se identificar e avaliar os controles que respondam aos eventos de riscos identificados, quanto ao seu desenho e quanto à sua operação. Com vistas a auxiliar, há uma pequena lista de alguns controles básicos no Anexo VI.

Em síntese, avaliar o desenho refere-se à concepção (forma como está ou deveria ser implementado) do controle e a operação refere-se ao seu funcionamento, buscando, assim, identificar o alcance dos objetivos do controle.

O desenho e a operação podem ser avaliados conforme os critérios descritos nas tabelas abaixo:

Quanto ao DESENHO: há procedimento de controle suficiente e formalizado?	
1	Não há procedimento de controle.
2	Há procedimentos de controle, mas insuficiente e não formalizado.
3	Há procedimentos de controle formalizado, mas insuficientes.
4	Há procedimentos de controle suficientes, mas não formalizados.
5	Há procedimentos de controle suficientes e formalizados.

TABELA 3 - AVALIAÇÃO DO DESENHO DO CONTROLE

Quanto ao PROCEDIMENTO: há procedimento de controle sendo executado? Há evidências de sua execução?	
1	Não há procedimento de controle.
2	Há procedimentos de controle, mas não são executados.
3	Há procedimentos de controle, mas são parcialmente executados.
4	Há procedimentos de controle executados, mas não evidenciados.
5	Há procedimentos de controle executados de forma evidenciável.

TABELA 4 - AVALIAÇÃO DO PROCEDIMENTO DO CONTROLE

Orienta-se que todo o processo de Gestão de Riscos observe os controles 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.

Avaliação do Risco Residual

Após avaliar a eficácia dos controles existentes, deve-se aferir o nível de risco residual, indicando os novos pesos relativos à probabilidade e ao impacto. Multiplicando-se esses pesos, obteremos o valor do risco residual e em qual nível da Matriz de Apetite a Risco ele estará inserido, observando as ações a serem adotadas para cada nível de risco, conforme demonstrado abaixo:

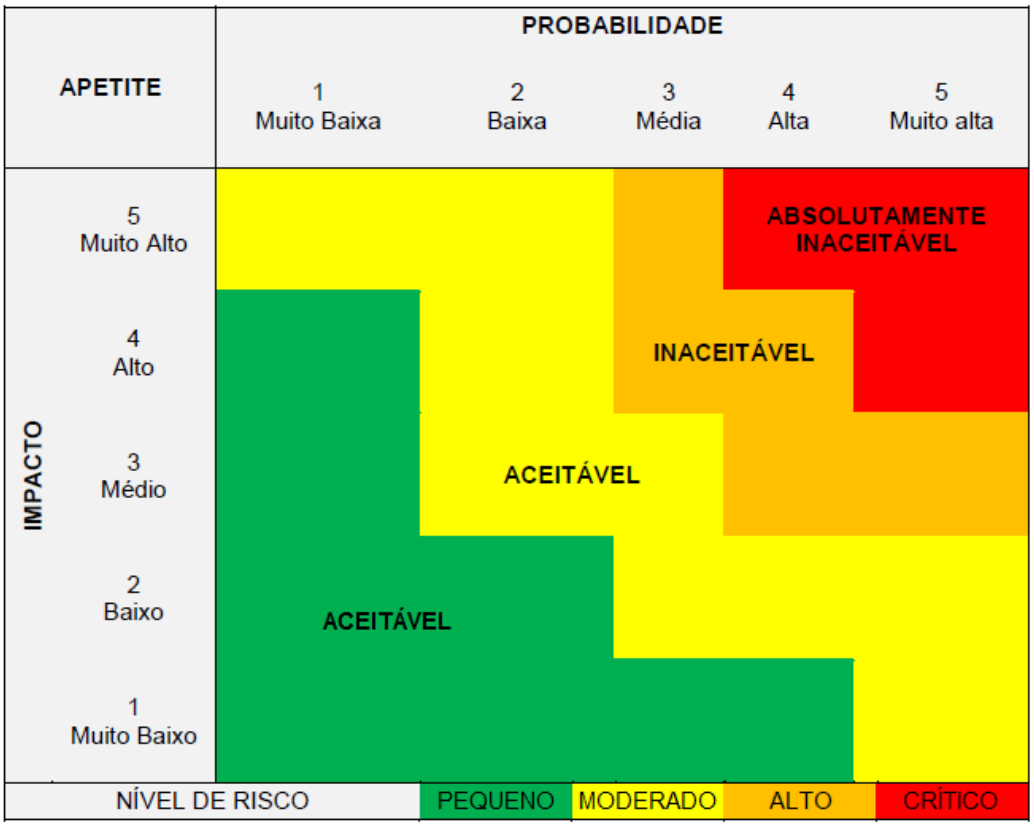


FIGURA 11 - MATRIZ APETITE A RISCOS

(Fonte: TST 2015)

Aceitável (Nível Pequeno): é possível conviver com o risco, mantendo as práticas e controles existentes;

Aceitável (Nível Moderado): é possível promover ações que atenuem as causas e/ou consequências ou aceitar o risco;

Inaceitável (Nível Alto): é necessária a elaboração de plano de ação para evitar ou eliminar as causas e/ou consequências;

Totalmente Inaceitável (Nível Crítico): é necessária a elaboração de plano de ação para evitar ou eliminar as causas e/ou consequências, bem como considerar a necessidade de mobilização imediata de recursos, materiais e pessoal capacitado, com vistas ao tratamento desse risco.

Antes de prosseguir, é importante validar os níveis dos riscos residuais, definidos pelos analistas dos riscos, com o gestor do processo que seria, no mínimo, o DAS/FCPE 4 da sua unidade.

RESPOSTA AOS RISCOS

Conhecido o nível de risco residual, verifique qual estratégia a ser adotada para responder ao evento de risco. A escolha da estratégia dependerá do nível de exposição a riscos previamente estabelecido em confronto com a avaliação que se fez do risco (matriz apetite a riscos).

Há quatro possíveis tipos de respostas quanto aos riscos identificados, a saber:

- **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).

Conforme explicitado anteriormente, as respostas deverão observar os limites de exposição a riscos definidos pelo Ministério do Desenvolvimento Regional. Para todos os riscos altos e críticos deverão ser instituídos controles e/ou ações mitigadoras com o objetivo de reduzi-lo ou compartilhá-lo até sua conformidade com o limite de exposição aceitável pelo Ministério.

É importante destacar que cada tipo de resposta requer um tipo de ação, ou seja, ao **aceitar** um risco, as instâncias superiores da gestão devem ser comunicadas quanto às justificativas para a não adoção de quaisquer respostas ou tratamentos. Assim, caso a instância superior aceite as justificativas, a responsabilidade dos analistas de riscos passa a ser compartilhada no caso de materialização do risco. Sugere-se que se faça o registro formal, via SEI, desse processo decisório.

Ao **transferir** os riscos, pretende-se repassar o ônus de tratamento e/ou seus respectivos custos e impactos para outras agentes externos como outros órgãos, seguradoras ou empresas terceirizadas. Não se deve confundir a transferência do risco com os casos em que se faz necessário compartilhar o tratamento, envolvendo outras unidades organizacionais na construção de soluções. Neste caso, a resposta ao risco poderá ser conjunta e, em casos extremos, os níveis superiores da gestão poderão ser acionados e atribuirão um agente apropriado para definir o tratamento.

Ao se optar por **evitar ou eliminar** riscos, pretende-se tratar as causas geradoras dos riscos impedindo sua materialização ou diminuindo a probabilidade de que venham a ocorrer. Por outro lado, quando o risco não pode ser evitado, devemos nos preparar para tratar as consequências, ou seja, reduzir

ou mitigar os efeitos de sua materialização sobre os objetivos organizacionais, por exemplo, por meio de planos de contingência.

Dessa forma, em algumas circunstâncias, a avaliação de riscos pode levar à decisão de se proceder a uma análise mais aprofundada mantendo-se os controles existentes. Esta decisão será influenciada pela atitude perante o risco da organização e pelos critérios de risco que foram estabelecidos.

Ao se decidir por implementar novos controles ou melhorar os já existentes, é importante estabelecer algumas informações sobre os controles. Há o **preventivo**, cujo objetivo é prevenir a materialização do evento de risco (ex: verificação da credencial das pessoas, antes de entrarem no prédio do Ministério). Por outro lado, há o **corretivo** que mitiga uma falha concretizada (ex: identificação, pela vigilância, das pessoas que estão no prédio, mas sem credencial).

Quanto à natureza, os controles podem ser **manuais** - realizados por pessoa (ex: conferência de assinatura)-; **automáticos** - processados por sistema, sem intervenção humana relevante (ex: senha de e-mail)-; e **híbridos**- mesclam atividades manuais e automáticas.

Já no tocante à frequência, podem ser: **anuais, semestrais, bimestrais, mensais, diários**.

Há, ainda, o controle **compensatório** que tem como objetivo mitigar o risco até a implementação do controle **definitivo**. No setor público existem situações em que a ação ideal não pode ser implementada ou não o pode ser no curto prazo em função de complexidade, alto custo, alto nível de interveniência, etc. Nesses casos, devem ser propostas, complementarmente, medidas alternativas de baixo custo e que atuem sobre o evento de riscos (controle compensatório). É o caso, por exemplo, da informatização de um processo que, como é custosa e depende de variáveis, até que ocorra, podem ser usadas planilhas ou controles manuais.

Portanto, quando se decide melhorar ou implementar um controle, deverá ser elaborado o **Plano de Controle**, que é um conjunto de ações necessárias para adequar os níveis de riscos, identificando: se é preventivo, corretivo ou compensatório; se é para melhoria de um controle já existente ou adoção de um novo; a área responsável pela implementação; o **cargo** do servidor responsável (evite colocar apenas o nome do servidor); se há áreas intervenientes que auxiliarão nesse controle; como será implementado (se por projeto, melhoria no sistema, criação de norma, plano de contingência, etc.); datas de início e fim.

Em razão das limitações de recursos, devem-se considerar os custos e os benefícios relativos às opções de respostas alternativas ao risco, tanto os custos diretos associados ao estabelecimento de uma

resposta, quanto os indiretos, caso sejam mensuráveis, e, se possível, os custos de oportunidade associados à utilização dos recursos. Com vistas a facilitar esse processo, encontra-se no Anexo VI uma listagem com algumas sugestões de controles básicos.

Quando for risco à integridade ou o risco tiver alguma relação com o tema, a própria unidade poderá desenvolver um plano com ações específicas. Entretanto, caso sejam necessárias medidas transversais que envolvam todo o Ministério, poderá ser feito um contato com a Coordenação-Geral de Governança e Integridade da Assessoria Especial de Controle Interno, uma vez que é responsável pela coordenação e estruturação do Programa de Integridade, bem como pelo monitoramento e revisão do Plano de Integridade.

Após essa etapa, o gestor do processo, que é no mínimo DAS/FCPE 4, fará uma análise, podendo validar ou alterar a resposta a risco, tanto para adotar uma ação em que poderia aceitar o risco e não adotar controle, como deixar de adotar uma ação definida pelos analistas de risco, tudo isso com apresentação de justificativa e validação pela unidade de gestão de risco superior (diretoria ou secretaria). Como no Ágatha há apenas a validação pelo gestor do processo (no mínimo DAS ou FCPE 4), essa concordância das instâncias superiores poderá ser feita formalmente pelo SEI. Não obstante, todos os Secretários Nacionais terão acesso ao Sistema e, a partir da validação do gestor do processo, todo o trabalho ficará disponível para que essas autoridades e o CIGov avaliem a qualquer momento.

MONITORAMENTO E COMUNICAÇÃO

O monitoramento é uma 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, em cada decisão, a compreensão de todos os agentes envolvidos sobre os riscos existentes em cada decisão.

O acesso a informações confiáveis, íntegras e tempestivas é vital para a eficiência da gestão visando facilitar o alcance dos objetivos de cada processo. 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.

O MDR deverá assegurar que os controles permaneçam eficazes e que o ambiente de controle se mantenha efetivo ao longo do tempo. 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 alterações, a administração necessita determinar se o funcionamento do gerenciamento de riscos corporativos permanece eficaz. (COSO ERM)

Cabe destacar que a implementação de atividades relacionadas à gestão de risco e controles, por si só, 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 são essenciais para que cada um dos participantes saiba como seu cargo se encaixa na estrutura corporativa de gestão de riscos e controles. As instâncias e as competências de cada uma estão definidas na Política de Gestão de Riscos do MDR, constante do Anexo III. Além disso, foi elaborada uma matriz de responsabilidades com a descrição das principais tarefas e sua periodicidade, no Anexo II.

A maior parte das informações sobre todas as etapas mencionadas anteriormente estarão registradas no Sistema Ágatha. Também constará no Sistema a validação do gestor do processo (no mínimo DAS/FCPE 4) de todo o trabalho realizado pelos analistas de risco (o grupo que identificou, analisou, avaliou os riscos e definiu os planos de tratamento). Dessa forma, a partir da conclusão do processo e da validação mencionada, considera-se que a comunicação às partes interessadas foi feita.

Contudo, os riscos de nível crítico, considerados intoleráveis, requerem comunicação e ações imediatas, além de ser monitorados de maneira mais atuante. Assim, sugere-se a criação de processo no SEI formalizando o risco e as ações imediatas com encaminhamento às instâncias superiores (diretor, secretário e Comitê Interno de Governança, se for o caso), de modo a compartilhar a responsabilidade pela execução e acompanhamento dessas medidas.

A Coordenação-Geral de Inteligência e Riscos da Assessoria Especial de Controle Interno fará relatórios periódicos ao Comitê Interno de Governança do Ministério, relatando os riscos que atingem ou superam os limites de tolerância definidos pela alta gestão e o monitoramento dos planos de tratamento. Caso sejam percebidas deficiências ou vulnerabilidades, recomendações serão feitas às respectivas unidades para um aperfeiçoamento dos instrumentos de gestão de integridade, riscos e controles.

Não obstante, após implementados os controles operacionais, o gestor deverá **continuamente** avaliar esses controles da mesma forma quanto ao desenho e à operação, assegurando que o controle esteja

presente e funcionando. É importante esse monitoramento contínuo, com vistas a verificar se estão menos eficazes ou obsoletos, tornando-se insuficientes para mitigar o risco. Nesse caso, nova avaliação deve ser feita e, se for o caso, novos planos de controle.

PROGRAMA DE INTEGRIDADE

Segundo a Portaria CGU nº 57/2019, um programa de integridade consiste no conjunto estruturado de medidas institucionais voltadas para a prevenção, detecção, punição e remediação de práticas de corrupção, fraudes, irregularidades e desvios éticos e de conduta.

O programa de integridade do MDR tem como objetivo atuar em temas já conhecidos pela organização, mas de maneira sistematizada. Nesse sentido, o programa de integridade trabalhará em parceria com as atividades, programas e políticas de auditoria interna, correição, ouvidoria, transparência e prevenção à corrupção, organizadas e direcionadas para a promoção da integridade institucional.

O programa de integridade propõe auxiliar os responsáveis pelas atividades acima mencionadas e áreas afins a trabalharem em conjunto e de forma coordenada, a fim de garantir uma atuação íntegra, minimizando os possíveis riscos de corrupção. Esses instrumentos, por serem interdependentes, somente alcançam máxima eficiência e eficácia se utilizados em conjunto.

A formação da gestão da integridade por meio de um programa específico dá maior visibilidade à importância do tema e às medidas propostas para promovê-la. Tal atuação permite que os tomadores de decisão do MDR possam se apoiar nos normativos internos produzidos e numa equipe organizada para auxiliá-los sempre que uma ameaça à integridade for identificada.

Para uma melhor compreensão a respeito do programa de integridade do MDR, é necessário conhecer os quatro pilares do programa, a estrutura de integridade criada no âmbito do Ministério e o Plano de Integridade, que formaliza as ações e medidas que darão o norte ao programa.

OS 4 PILARES DO PROGRAMA

O comprometimento e apoio da alta administração é o 1º Pilar do programa de integridade. A alta direção, composta pelo Ministro, Secretário-Executivo, Secretários e Diretores, deve dar o tom ao órgão,

isto é, conduzi-lo a seguir e respeitar os princípios éticos, caminhando em conformidade com as normas e as boas práticas da administração pública.

A estrutura de funcionamento é o 2º Pilar do Programa de Integridade e oferece as bases para que o Programa seja efetivo. No MDR, a estrutura é composta da seguinte forma:

I – Comitê Interno de Governança (CIGov);

II – Unidade da Gestão da Integridade (UGI)

III – Instâncias Internas de Integridade; e

IV – Agentes de Integridade.

O CIGov atua no nível estratégico e acompanha as atividades do programa de integridade, conforme competências definidas pela Portaria MDR nº 1.079, de 4 de abril de 2019.

A Assessoria Especial de Controle Interno foi designada como Unidade de Gestão da Integridade, responsável pela coordenação e estruturação do programa, bem como sua execução, monitoramento e revisão.

As Instâncias Internas de Integridade atuam de forma organizada e integrada, para atuação permanente, representadas pelos titulares da Ouvidoria, Corregedoria, Comissão de Ética, Assessoria de Comunicação, Coordenação-Geral de Planejamento Institucional e Desenvolvimento, Coordenação-Geral de Gestão de Pessoas e Coordenação-Geral de Gestão de Processos e Inovação.

Os Agentes de Integridade, por sua vez, são servidores que auxiliam a UGI e as Instâncias Internas na disseminação da cultura de integridade no âmbito de cada unidade e na construção do Plano de Integridade.

A gestão de riscos é o 3º Pilar do programa de integridade e consiste na ferramenta que permite aos agentes públicos mapear os processos da organização de forma a identificar fragilidades que possibilitem a ocorrência de fraudes e atos de corrupção. Nesse contexto, alguns dos benefícios decorrentes da realização da gestão de riscos para a integridade são:

- Mantêm as questões de prevenção da corrupção, integridade e boa governança em foco e realiza análises que vão além da abordagem puramente legalista;
- Permite a identificação de riscos que sejam comuns nos setores e que, portanto, exijam ação ou reforma institucional mais ampla;

- Permite partilhar conhecimento e boas práticas na identificação de riscos e, em particular, em medidas de mitigação em determinado setor ou entre setores, projetos ou processos.

A informação, comunicação e o monitoramento, 4º Pilar do programa de integridade, é um processo contínuo e permanente de disponibilização de informação adequada às partes interessadas e de relacionamento entre as instâncias de supervisão e de monitoramento das ações do programa, de forma a avaliar a qualidade do sistema de controle interno ao longo do tempo.

PLANO DE INTEGRIDADE

O Plano de Integridade é o documento que detalha a estrutura, as ações e os prazos necessários para a operacionalização do programa de integridade. Todas as ações devem estar alinhadas ao planejamento estratégico do órgão e à manutenção de uma cultura sustentável de integridade institucional.

A cada ano deve ser realizado um novo Plano de Integridade com o objetivo de apresentar o desenvolvimento e o aprimoramento de ações relacionadas ao tema Integridade já realizadas no atual exercício, como também o plano de ação para o exercício seguinte. Dessa forma, está previsto um ciclo contínuo de análises para possíveis atualizações dos normativos da Instituição com o objetivo de garantir a constante revisão e uniformidade da regulamentação e de todos os processos de atividade que dizem respeito à integridade, da seguinte forma:

- Plano: elaborar um plano com medidas claras e executáveis;
- Execução: implementar e divulgar o plano;
- Checagem: realizar a análise crítica dos resultados do plano; e
- Ação: se necessário, efetuar ajustes e elaborar a documentação do novo padrão operacional.

MEDIDAS E AÇÕES DE INTEGRIDADE

Padrões de Ética e Conduta

O programa de integridade busca disseminar uma cultura de integridade no órgão. Dessa forma, a formalização das expectativas a respeito do comportamento e conduta do agente público é uma medida

que deve ser implementada, sendo necessário comunicar amplamente e com clareza quais valores e princípios deverão orientar a atuação dos servidores.

Nesse sentido, somam-se ao presente Programa as regras operacionais e de conduta estabelecidas, por meio da Comissão de Ética e de um Código de Conduta.

Comunicação e Treinamento

As ações de comunicação e treinamento em um programa de integridade utiliza todas as ferramentas para levar aos agentes públicos informações sobre a correta prestação do serviço público, o que envolve desde campanhas entre os servidores acerca de questões de integridade até treinamentos de qualificação técnica.

Dessa forma, a Unidade de Gestão da Integridade (UGI) em conjunto com a Coordenação-Geral de Gestão de Pessoas promoverão treinamentos periódicos, eventos e palestras com o objetivo de explicar, difundir e incrementar o conteúdo e os aspectos práticos das diretrizes e parâmetros do programa de integridade aos colaboradores do MDR.

Canal de Denúncia

A criação do canal de denúncia por meio do qual todos os colaboradores do órgão e cidadãos possam denunciar desvios cometidos por pessoas da organização, inclusive pela alta direção, é medida indispensável à garantia da manutenção da integridade pública.

Os colaboradores do MDR que identificarem alguma situação de risco ou de ações que destoem da legislação vigente, das normas e políticas internas, têm o dever e responsabilidade de reportar o fato à Ouvidoria, canal único para recebimento e tratamento de denúncias, conforme Instrução Normativa nº 7, de 8 de maio de 2019 e Portaria MDR nº 948, de 8 de abril de 2020.

Assim, caso o colaborador do MDR receba uma denúncia ou outra manifestação de ouvidoria diretamente ou por quaisquer outros meios (SEI, e-mail, telefone, carta, etc.), ele deve realizar o pronto encaminhamento da denúncia à Ouvidoria-Geral, para registro no Fala.BR e envio à unidade responsável para apuração.

Todas as denúncias levadas ao conhecimento dos órgãos apuratórios serão investigadas com a devida diligência e detalhamento das condutas e ocorrências, averiguando-se os fatos para que as medidas de correção e ajustes sejam adotadas, bem como para que eventuais responsáveis sejam punidos.

Medidas de Controles e Disciplinares

Os gestores das unidades do MDR são os responsáveis por implementar as ações corretivas para resolver deficiências em processos e controles. Estes devem ser os primeiros responsáveis por cuidar e fazer cuidar das atividades resultantes de seus processos de atuação.

Ainda no que diz respeito às ações de controle, a Assessoria Especial de Controle Interno (AECI) deve acompanhar a implementação das recomendações da Controladoria-Geral da União e das deliberações do Tribunal de Contas da União relacionadas ao MDR.

Todo sistema de integridade está interligado ao cumprimento das normas e divulgação de padrões de conduta esperados pelos agentes públicos para surtir os efeitos desejados. Se as boas práticas são claras e bem divulgadas, o corpo técnico treinado e, mesmo assim, há violações das regras, sanções fazem-se necessárias para a manutenção da legitimidade do sistema. Nesse contexto, uma atuação correcional, em alguns casos, é necessária e tem efeito desmotivador para o cometimento de novas irregularidades dentro da organização.

Ações de Remediação

Para o funcionamento adequado do programa de integridade não são suficientes controles internos instituídos ou a área disciplinar instaurar procedimentos investigatórios e aplicar penalidades. Os resultados de auditorias, as representações funcionais ou denúncias apresentadas por particulares devem ser utilizadas para retroalimentar o sistema e indicar quais possíveis situações precisam ser tratadas pelo programa.

A Unidade de Gestão da Integridade (UGI) funciona como uma “ponte” entre as áreas do MDR e a alta administração, a qual deve propor mecanismos de controle, aprimoramento de processos, implementação de fluxos de trabalho, entre outras medidas.

RISCOS DE INTEGRIDADE

A Portaria CGU nº 57/2019, define, no inciso II do art. 2º, riscos para a integridade, a saber: *vulnerabilidade que pode favorecer ou facilitar a ocorrência de práticas de corrupções, fraudes, irregularidades e/ou desvios éticos e de conduta, podendo comprometer os objetivos da instituição.*

Essa definição indica que o risco à integridade não deve ser entendido apenas em termos de infração às normas e leis, mas sim de maneira mais ampla, englobando atos de fraudes, abuso de poder/influência, conflito de interesses, uso indevido e vazamento de informação sigilosa, como também práticas antiéticas.

De um modo geral, atos relacionados a quebras de integridade compartilham as seguintes características:

- Derivam da conduta dos colaboradores da organização (servidores, terceirizados ou estagiários, incluindo membros da alta administração);
- São praticados por meio de dolo (intenção ou má-fé) ou culpa (imperícia, imprudência ou negligência comprovada);
- Envolve uma afronta aos princípios da administração pública: legalidade, impessoalidade, moralidade, publicidade e eficiência;
- Implica alguma forma de deturpação, desvio ou negação da finalidade pública ou do serviço público a ser entregue ao cidadão.

A partir dessas características, podemos identificar de **maneira exemplificativa**, alguns riscos para a integridades mais comuns nas organizações públicas e suas possíveis causas.

Possíveis riscos

Uso indevido ou manipulação de dados/informações	• Divulgação ou uso indevido de dados ou informações; • Alteração indevida de dados/informações; • Restrição de publicidade ou de acesso a dados ou informações.
Desvio de pessoal ou de recursos materiais	• Desviar ou utilizar, em obra ou serviço particular, veículos, máquinas, equipamentos ou material de qualquer natureza, de propriedade ou à disposição de entidades públicas, bem como o trabalho de servidores públicos, empregados ou terceiros contratados para fins particulares ou para desempenho de atribuição que seja de sua responsabilidade ou de seu subordinado.
Corrupção, fraude, emprego irregularidade nas verbas públicas	• Crimes contra a administração pública, previstos em leis, tratados, acordos nacionais e internacionais, que representam alto potencial ofensivo às instituições e à sociedade e que demandam custos significativos para recuperação de ativos e para retorno da credibilidade.

Uso indevido de autoridade	• Contra o exercício profissional: atentar contra os direitos e garantias legais assegurados ao exercício profissional com abuso ou desvio do poder hierárquico ou sem competência legal para atender interesse próprio ou de terceiros. Proceder a qualquer tentativa de obrigar o servidor a executar o que evidentemente não está no âmbito das suas atribuições ou a deixar de executar o que está previsto. • Contra a honra e o patrimônio: atentar contra a honra ou o patrimônio de pessoa natural ou jurídica com abuso ou desvio de poder ou sem competência legal para atender interesse próprio ou de terceiros.
Nepotismo	• Nomear, designar, contratar ou alocar familiares para exercício de cargo em comissão, função de confiança ou para a prestação de serviços no MDR.
Conflito de interesses	• Exercício de atividades incompatíveis com as atribuições do cargo; • Intermediação indevida de interesses privados; • Concessão de favores e privilégios ilegais a pessoa jurídica; • Recebimento de presentes/vantagens; • Inobservância da quarentena indicada para aqueles que se desligam de cargos por meio dos quais obtiveram informações privilegiadas no exercício da função.

TABELA 5 - POSSÍVEIS RISCOS

Possíveis causas

Uso indevido ou manipulação de dados ou informações	• Acesso de pessoas não autorizadas aos documentos; • Falta de atenção (não atencional); • Fragilidade no processo e comunicação de informações produzidas ou custodiadas pela organização.
Desvio de pessoal ou de recursos materiais	• Ausência de mecanismos de aferição do desempenho dos servidores da organização; • Falta de comprometimento do servidor da organização com os objetivos institucionais e com o serviço prestado.
Corrupção, fraude, emprego irregularidade nas verbas públicas	• Má-fé do servidor; • Conluio.
Uso indevido de autoridade	• Má fé do superior hierárquico (perseguição, amizade, preferência, etc.); • O normativo favorece a discricionariedade para a prática do ato;

	• Deficiências no desenvolvimento de competências e habilidades do superior hierárquico.
Nepotismo	• Ausência de sistema de informações sobre o quadro de colaboradores da organização; • Solicitações indevidas indiretas ou diretas por autoridades; • Pressão familiar.
Conflito de interesses	• Capacidade operacional insuficiente em relação às demandas; • Falta de comunicação do servidor quanto à sua suspeição; • Trabalhos que demandam competências específicas.

TABELA 6 - POSSÍVEIS CAUSAS

Os tipos mencionados não exaurem todas as possibilidades de ocorrência de riscos para a integridade, tendo como intenção apenas facilitar a identificação dos riscos pelos agentes públicos do MDR.

Os riscos à integridade deverão ser analisados em conjunto com os demais riscos do processo, tais como os riscos operacionais, legais, financeiros, imagem, entre outros.

A Coordenação-Geral de Inteligência e Gestão de Riscos e a Coordenação-Geral de Governança e Integridade da Assessoria Especial de Controle Interno auxiliarão na implementação da gestão de riscos nas unidades, que acontecerá de forma gradual nos processos mais relevantes da área que tenham relação com o planejamento estratégico do MDR.

CONSIDERAÇÕES FINAIS

Como em qualquer iniciativa de implementação e desenvolvimento de metodologias de Gestão de Riscos, é fundamental a realização de ajustes para se adequar ao contexto da organização. Assim, visando adequar-se às necessidades do MDR, este manual estará em constante processo de melhoria, com o objetivo de auxiliar o gestor na gestão de riscos dos processos de suas unidades. Nesse processo, qualquer contribuição de melhoria de todos os colaboradores do MDR será essencial.

Por fim, ressalta-se que o levantamento e gerenciamento de riscos devem fazer parte dos processos das unidades, almejando contribuir para a implantação de boas práticas de gestão de riscos, de integridade, e de Controles Internos e para a tomada de decisões de governança.

REFERÊNCIAS BIBLIOGRÁFICAS

BRASIL. Associação Brasileira de Normas Técnicas - ABNT. **Gestão de Riscos: Princípios e Diretrizes. Norma Brasileira ABNT NBR ISO 31000:2009.** Primeira Edição, 2009. ISBN 978-85-07-01838-4

BRASIL. Associação Brasileira de Normas Técnicas - ABNT. **Gestão de Riscos: Diretrizes. Norma Brasileira ABNT NBR ISO 31000:2018** Segunda Edição, 2018.

BRASIL. Ministério do Planejamento. Secretaria de Gestão Pública. **Programa Gespública - O Modelo de Excelência em Gestão Pública**. Brasília, 2014a.

BRASIL. Ministério do Planejamento. Secretaria de Gestão Pública. **Programa Gespública - Instrumento para Avaliação da Gestão Pública**. Brasília, 2014b.

BRASIL. Ministério do Planejamento, Orçamento e Gestão. Secretaria de Gestão Pública. **Programa Gespública - Guia de Orientação para o Gerencimento de Riscos**. Brasília, 2013.

BRASIL. Ministério do Planejamento. Assessoria Especial de Controle Interno. **Manual de Gestão de Integridade, Riscos e Controles Internos da Gestão**. Brasília, 2017.

BRASIL. Ministério da Transparência e Controladoria Geral da União. **Manual para implementação de programas de integridade**. Brasília, 2017.

BRASIL. Ministério da Transparência e Controladoria Geral da União. **Guia Prático para Gestão de Riscos a Integridade**. Brasília, 2018.

BRASIL. Ministério da Transparência e Controladoria Geral da União. **Manual da Metodologia de Gestão de Riscos**. Brasília, 2017.

COSO ERM. **Gerenciamento de Riscos Corporativos - Estrutura Integrada**, 2004.

COSO. **Gerenciamento de Riscos Corporativos – Estrutura Integrada**. 2007. Tradução: Instituto dos Auditores Internos do Brasil (Audibra) e Pricewaterhouse Coopers Governance, Risk and Compliance, Estados Unidos da América, 2007.

ISO (ISO - International Organization for Standardization). **ISO 31000 – Risk Management System – Principles and Guidelines**. Tradução: Associação Brasileira de Normas Técnicas (ABNT) Projeto 63:000.01- 001. Agosto, 2009.

ANEXOS

ANEXO I – TERMOS E DEFINIÇÕES

Accountability: conjunto de procedimentos adotados pelo Ministério e pelos indivíduos que o integram para evidenciar as responsabilidades inerentes por decisões tomadas e ações implementadas, incluindo a salvaguarda de recursos públicos, a imparcialidade e o desempenho;

Alta Administração: Ministros de Estado, ocupantes de cargos de natureza especial, ocupantes de cargo de nível 6 do Grupo-Direção e Assessoramento Superiores – DAS e presidentes e diretores de autarquias, inclusive as especiais, e de fundações públicas ou autoridades de hierarquia equivalente;

Análise do risco: 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: nível de risco que o Ministério está disposto a aceitar;

Atividades de controles internos: são as políticas e os procedimentos estabelecidos para enfrentar os riscos e alcançar os objetivos do Ministério;

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

Consequência: resultado de um evento que afeta positiva ou negativamente os objetivos do Ministério;

Controle: qualquer medida aplicada no âmbito do Ministério, para gerenciar os riscos e aumentar a probabilidade de que os objetivos e metas estabelecidos sejam alcançados;

Controles detectivos: são controles desenhados para detectar erros (intencionais e nãointencionais) 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, de forma integrada pela direção e pelo corpo de servidores das organizações, destinados a enfrentar os riscos e fornecer segurança razoável para a consecução da missão do Ministério;

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 evento é um incidente ou uma ocorrência gerada com base em fontes internas ou externas, que afeta a realização dos objetivos (COSO II).

Fonte de risco: elemento que, individualmente ou combinado, tem o potencial intrínseco de dar origem ao risco;
Fraude: quaisquer atos ilegais caracterizados por desonestidade, dissimulação ou quebra de confiança. Estes atos não implicam o uso de ameaça de violência ou de força física;

Gestão de riscos: processo para identificar, avaliar, administrar e controlar potenciais eventos ou situações, para fornecer razoável certeza no alcance dos objetivos do Ministério do Planejamento, Desenvolvimento e Gestão;

Gestores de riscos: gestor de unidade administrativa responsável pelo gerenciamento de determinado risco;

Gestão da Integridade: conjunto de medidas de prevenção de possíveis desvios na entrega dos resultados esperados pela sociedade;

Governança: combinação de processos e estruturas implantadas pela alta administração do Ministério do Planejamento, Desenvolvimento e Gestão, para informar, dirigir, administrar e monitorar suas atividades, com o intuito de alcançar os seus objetivos;

Governança no setor público: compreende essencialmente os mecanismos de liderança, estratégia e controle postos em prática para avaliar, direcionar e monitorar a atuação da gestão, com vistas à condução de políticas públicas e à prestação de serviços de interesse da sociedade;

Identificação de riscos: processo de busca, reconhecimento e descrição de riscos, que envolve a identificação de suas fontes, causas e consequências potenciais. A identificação de riscos pode envolver dados históricos, análises teóricas, opiniões de pessoas informadas e de especialistas, e as necessidades das partes interessadas;

Incerteza: incapacidade de saber com antecedência a real probabilidade ou impacto de eventos futuros;

Impacto: efeito resultante da ocorrência do evento;

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

Mensuração de risco: significa estimar a importância de um risco e calcular a probabilidade de sua ocorrência;

Monitoramento: é um componente do controle interno que permite avaliar a qualidade do sistema de controle interno ao longo do tempo;

Nível de risco: magnitude de um risco, expressa em termos da combinação de suas consequências e probabilidades de ocorrência;

Operações econômicas: ocorre quando a aquisição dos insumos necessários se der na quantidade e qualidade adequadas, forem entregues no lugar certo e no momento preciso, ao custo mais baixo;

Operações eficientes: ocorre quando consumirem o mínimo de recursos para alcançar uma dada quantidade e qualidade de resultados, ou alcançarem o máximo de resultado com uma dada qualidade e quantidade de recursos empregados;

Política de gestão de riscos: declaração das intenções e diretrizes gerais do Ministério relacionadas à gestão de riscos;

Procedimento de controle: são as políticas e os procedimentos estabelecidos para enfrentar os riscos e alcançar os objetivos do Ministério;

Procedimentos de controle interno: procedimentos que o Ministério executa para o tratamento do risco, projetados para lidar com o nível de incerteza previamente identificado;

Processo: conjunto de ações e atividades inter-relacionadas, que são executadas para alcançar produto, resultado ou serviço predefinido;

Processo de gestão de riscos: aplicação sistemática de políticas, procedimentos e práticas de gestão para as atividades de identificação, avaliação, tratamento e monitoramento de riscos, bem como de comunicação com partes interessadas em assuntos relacionados a risco;

Probabilidade: possibilidade de ocorrência de um evento;

Resposta ao risco: qualquer ação adotada para lidar com risco. As respostas podem se enquadrar num destes tipos: aceitar o risco por uma escolha consciente; transferir/compartilhar o risco a outra parte; evitar o risco pela decisão de não iniciar ou descontinuar a atividade que dá origem ao risco; ou mitigar/reduzir o risco diminuindo sua probabilidade de ocorrência ou minimizando as consequências do risco;

Risco: possibilidade de ocorrer um evento que venha a ter impacto no cumprimento dos objetivos. O risco é medido em termos de impacto e de probabilidade;

Risco inerente: risco a que uma organização está exposta sem considerar quaisquer ações gerenciais que possam reduzir a probabilidade dos riscos ou seu impacto;

Risco residual: risco a que uma organização está exposta após a implementação de ações gerenciais para o tratamento do risco;

Riscos de imagem/reputação do órgão: eventos que podem comprometer a confiança da sociedade (ou de parceiros, de clientes ou de fornecedores) em relação à capacidade do Ministério do Planejamento, Desenvolvimento e Gestão em cumprir sua missão institucional;

Riscos financeiros/orçamentários: eventos que podem comprometer a capacidade do Ministério do Planejamento, Desenvolvimento e Gestão de contar com os recursos orçamentários e financeiros necessários à realização de suas atividades, ou eventos que possam comprometer a própria execução orçamentária, como atrasos no cronograma de licitações;

Riscos legais: eventos derivados de alterações legislativas ou normativas que podem comprometer

as atividades do Ministério do Planejamento, Desenvolvimento e Gestão; e

Riscos operacionais: eventos que podem comprometer as atividades do Ministério do Planejamento, Desenvolvimento e Gestão, normalmente associados a falhas, deficiência ou inadequação de processos internos, pessoas, infraestrutura e sistemas;

Tolerância ao Risco: é o nível de variação aceitável quanto à realização dos objetivos;

Tratamento de riscos: processo de estipular uma resposta a risco;

Categoria de riscos: é a classificação dos tipos de riscos definidos pelo Ministério do Planejamento, Desenvolvimento e Gestão que podem afetar o alcance de seus objetivos estratégicos, observadas as características de sua área de atuação e as particularidades do setor público;

Método de priorização de processos: classificação de processos baseadas em avaliação qualitativa e quantitativa, visando o estabelecimento de prazos para a realização de gerenciamento de riscos.

Sistema de gestão de riscos: refere-se ao modo como os diversos atores se organizam, interagem e procedem para obter uma adequada gestão dos riscos organizacionais.

Unidade organizacional: unidade administrativa do MDR responsável pelo processo organizacional objeto de análise de 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).

ANEXO II – MATRIZ DE RESPONSABILIDADES

Legenda	
A - Aprovador	É quem aprova ou valida formalmente a atividade ou o produto dela resultante.
P - Promotor	É quem promove ou fomenta a execução da atividade.
R - Responsável	É quem executa a atividade formalmente.
C - Consultado	É quem gera uma informação que agrega valor para a execução de uma atividade ou quem apoia sua execução.
I - Informado	É quem precisa ser notificado do resultado da atividade.

Matriz de Responsabilidades

Instâncias de Supervisão						Atribuições e Interelacionamentos	Periodicidade				
Nível Estratégico		Nível Tático	Nível Operacional								
Ministro de Estado	Cigov	Secretaria Executiva	Unidades Organizacionais	Gestores de Riscos	Analistas de Riscos		Mensal	Quadrimestral	Semestral	Quando necessário	Sempre
I	A	P	C			Revisão da Política de Gestão de Riscos.				X	
I	A	P/C				Revisão da Metodologia de Gestão de Riscos.				X	
I	A	P				Níveis de apetite a risco do Ministério.				X	
I	A	P/C	C/R	R	R	Níveis de riscos e a efetividade das medidas de controle implementadas.				X	
I	I	P	P	C/R	R	Identificar e avaliar os riscos dos processos.					X
I	I	I	P/R	C/R	R	Monitoramento do risco ao longo do tempo, de modo a garantir que as respostas adotadas resultem na manutenção do risco em níveis adequados, de acordo com a política e a metodologia de gestão de riscos.					X
I	I	P/C/R				monitorar o desempenho do Sistema de Gestão de Riscos e sua eficácia em relação aos objetivos pretendidos.					X

Matriz de Responsabilidades

Instâncias de Supervisão						Atribuições e Interelacionamentos	Periodicidade				
Nível Estratégico		Nível Tático	Nível Operacional								
Ministro de Estado	Cigov	Secretaria Executiva	Unidades Organizacionais	Gestores de Riscos	Analistas de Riscos		Mensal	Quadrimestral	Semestral	Quando necessário	Sempre
			R	I	I	Indicar os Gestores de Risco.				X	
I	I	P/R	I	I	I	Orientar as unidades organizacionais na aplicação da Metodologia de Gestão de Riscos.					X
I	I	P/C	P/C	P/R	I	Disseminação da cultura de gestão de riscos.					X
I	I	P/R	P	I		monitorar a evolução de níveis de riscos e a efetividade das medidas de controle implementadas.					X
I	P/R	P	P	I	I	estimular a contínua capacitação do corpo funcional em gestão de riscos e em outras competências técnicas correlatas, por meio de palestras, cursos e eventos.			X		
			I	P/R		orientar e acompanhar as ações de identificação, avaliação e tratamento dos riscos.					X
I	R	P/C	P	I	I	garantir o apoio institucional para promover a gestão de riscos, em especial os seus recursos, o relacionamento entre as partes interessadas e o desenvolvimento contínuo dos servidores.					X
I	R	P/C	P	I	I	garantir o alinhamento da gestão de riscos aos padrões de ética e de conduta, em conformidade com o Programa de Integridade do MDR.					X
I	A/P	P/C	P	R	R	Práticas e princípios de conduta e padrões de comportamento.					X
I	C	P/C	P	R	R	Inovação e adoção de boas práticas de governança, integridade, riscos e controles internos da gestão.				X	
I	P	C	R	R	R	Aderências às leis, regulamentações, códigos, normas e padrões na condução de políticas e na prestação de serviços de interesse público.					X
I	A/R	C	R	R		Objetivos estratégicos que norteiam as boas práticas de governança, de integridade, de gestão de riscos e de controles internos.					X
I	P	P/C	P/R	R		Adoção de práticas que institucionalizem a responsabilidade dos agentes públicos na prestação de contas, transparência e efetividade das informações.				X	

Matriz de Responsabilidades

Instâncias de Supervisão						Atribuições e Interelacionamentos	Periodicidade				
Nível Estratégico		Nível Tático	Nível Operacional								
Ministro de Estado	Cigov	Secretaria Executiva	Unidades Organizacionais	Gestores de Riscos	Analistas de Riscos		Mensal	Quadrimestral	Semestral	Quando necessário	Sempre
I	P	P/C	R	R	R	Integração e o desenvolvimento contínuo dos agentes responsáveis pela governança, gestão da integridade, gestão de riscos e controles internos.				X	
I	A/R	C	C			Institucionalização de estruturas adequadas de governança, de gestão da integridade, riscos e controles internos.				X	
I	A	R	C			políticas, diretrizes, metodologias e mecanismos de monitoramento e comunicação para a gestão de integridade, riscos e controles internos.					X
I	A	P/C	P/R			Diretrizes de capacitação dos agentes públicos no exercício do cargo, em gestão de integridade, riscos e controles internos.				X	
I	P	P/C	R	R		Ações para disseminação da cultura de gestão de integridade, riscos e controles internos.				X	
I	A	C				Método de priorização de processos para a gestão de integridade, riscos e controles internos.				X	
I	A	C				Categorias de riscos a serem gerenciados.				X	
I	A/R					Estabelecimento de limites de exposição a riscos e níveis de conformidade.				X	
I	A/R					Estabelecimento de limites de alçada para exposição a riscos de órgãos de assistência direta e imediata ao Ministro de Estado do Desenvolvimento Regional e dos órgãos específicos singulares do Ministério.				X	
I	R					Supervisão dos riscos que podem comprometer o alcance dos objetivos estratégicos e a prestação de serviços de interesse público.	X				
I	A	C				Modelo de gestão de integridade, riscos e controles internos.	X				
I	R	C	C	C		Tomada de decisões considerando as informações sobre gestão de integridade, riscos e controle internos e assegurar que estejam disponíveis em todos os níveis.				X	
I	R	C				Recomendações e orientações para o aprimoramento da gestão de integridade, riscos e controles internos.				X	

Matriz de Responsabilidades

Instâncias de Supervisão						Atribuições e Interelacionamentos	Periodicidade				
Nível Estratégico		Nível Tático	Nível Operacional								
Ministro de Estado	Cigov	Secretaria Executiva	Unidades Organizacionais	Gestores de Riscos	Analistas de Riscos		Mensal	Quadrimestral	Semestral	Quando necessário	Sempre
			I/C	A/R	R	Gerenciamento de riscos dos processos de trabalho priorizados.					X
I	I	I	A	A/R	R	Plano de implementação de controles.				X	
I	I	I	R	C	C	monitoramento dos riscos ao longo do tempo.	X				
I	I	C	P	A/R	R	Implementação de metodologias e instrumentos adequados para a gestão de integridade, riscos e controles internos.				X	
I	I	I	R	C	C	Disponibilidade de informações adequadas sobre gestão de integridade, riscos, e controles internos em todos os níveis, no âmbito das unidades organizacionais.					X

ANEXO III – POLÍTICA DE GESTÃO DE RISCOS

ANEXO DA RESOLUÇÃO CIGOV Nº 07, de 27 de agosto de 2020

Dispõe sobre a Política de Gestão de Riscos do Ministério do Desenvolvimento Regional.

CAPÍTULO I - DISPOSIÇÕES GERAIS

Art. 1º A Política de Gestão de Riscos do Ministério do Desenvolvimento Regional - PGR-MDR tem como finalidade estabelecer conceitos, princípios, objetivos, diretrizes, competências e responsabilidades no âmbito da gestão de riscos.

Art. 2º Para fins desta Portaria, considera-se:

I. alta administração: Ministros de Estado, ocupantes de cargos de natureza especial, ocupantes de cargo de nível 6 do Grupo-Direção e Assessoramento Superiores - DAS e presidentes e diretores de autarquias, inclusive as especiais, e de fundações públicas ou autoridades de hierarquia equivalente;

II. apetite a risco: nível de risco que uma organização está disposta a aceitar;

III. 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 pelo corpo de servidores das organizações, destinados a enfrentar os riscos e fornecer segurança razoável na consecução da missão e do alcance dos objetivos do órgão;

IV. fonte de risco: elemento que, individualmente ou combinado, tem o potencial intrínseco de dar origem ao risco;

V. gestão de riscos: processo para identificar, avaliar, administrar e controlar potenciais eventos ou situações, para fornecer razoável certeza quanto ao alcance dos objetivos da organização;

VI. gestores de risco: gestor de unidade administrativa responsável pelo gerenciamento de determinado risco;

VII. 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;

VIII. nível de risco: magnitude de um risco, expressa como uma combinação entre impacto e probabilidade do risco;

IX. política de gestão de riscos: declaração das intenções, princípios, objetivos, diretrizes, competências e responsabilidades relacionadas à gestão de riscos;

X. processo: conjunto de ações e atividades inter-relacionadas, que são executadas para alcançar produto, resultado ou serviço predefinido;

XI. risco: possibilidade de ocorrência de um evento que venha a ter impacto no cumprimento dos objetivos; e

XII. sistema de gestão de riscos: refere-se ao modo como os diversos atores se organizam, interagem e procedem para obter uma adequada gestão dos riscos organizacionais.

XIII. unidade organizacional: unidade administrativa do Ministério do Desenvolvimento Regional responsável pelo processo organizacional objeto de análise de risco.

CAPÍTULO II - DOS PRINCÍPIOS

Art. 3º A gestão de riscos no MDR deverá observar os seguintes princípios:

I. ser parte integrante dos processos organizacionais;

II. considerar riscos e oportunidades;

III. estabelecer níveis adequados de exposição a riscos;

IV. basear-se nas melhores informações disponíveis;

V. subsidiar a tomada de decisões;

VI. ser sistemática, estruturada e oportuna, subordinada ao interesse público;

VII. agregar valor e observar o estabelecimento de controles internos proporcionais aos riscos, observada a relação custo-benefício;

VIII. apoiar a melhoria contínua dos processos organizacionais;

IX. considerar a importância dos fatores humanos e culturais;

X. ser implantada por meio de ciclos de revisão e melhoria contínua; e

XI. ser dirigida, apoiada e monitorada pela alta administração.

CAPÍTULO III - DOS OBJETIVOS

Art. 4º A gestão de riscos no Ministério do Desenvolvimento Regional tem por objetivos:

I. contribuir para uma cultura de gestão de riscos, chamando a atenção para a importância de se identificar e tratar riscos em todas as áreas e níveis organizacionais do Ministério do Desenvolvimento Regional;

II. fomentar a gestão proativa;

III. facilitar a identificação de oportunidades e ameaças;

IV. aprimorar a governança pública;

V. aprimorar os controles internos da gestão, privilegiando ações de prevenção antes da ocorrência de danos ou de processos sancionadores; e

VI. aumentar a capacidade da organização de se adaptar a mudanças.

CAPÍTULO IV - DAS DIRETRIZES

Art. 5º A Gestão de Riscos deverá se integrar ao planejamento estratégico, aos processos e às políticas do Ministério do Desenvolvimento Regional, sendo implementada de forma gradual em todas as áreas do órgão.

§1º Serão priorizados os processos que impactem diretamente no atingimento das entregas estratégicas definidas no Planejamento Estratégico do Ministério do Desenvolvimento Regional.

§2º O Comitê Interno de Governança – CIGov do Ministério do Desenvolvimento Regional deliberará sobre a inclusão de processos escolhidos como prioritários.

Art. 6 º O processo de gestão de riscos será detalhado na Metodologia de Gestão de Riscos do Ministério do Desenvolvimento Regional - MGR-MDR, e deverá contemplar, no mínimo, as seguintes etapas:

I. análise de ambiente e dos bjetivos: esta etapa trata do levantamento e registro dos

aspectos externos e internos essenciais ao alcance dos objetivos institucionais, permitindo a compreensão clara do ambiente em que a organização se insere e identificar os fatores que podem influenciar a capacidade da organização de atingir os resultados planejados;

II. identificação dos riscos: esta etapa envolve o reconhecimento, descrição e registro do evento de risco, com a caracterização de suas prováveis causas e possíveis consequências, caso ocorram;

III. avaliação dos riscos: esta etapa visa promover o entendimento do nível do risco e de sua natureza, especialmente quanto à estimação da probabilidade de ocorrência, e do impacto destes eventos identificados como risco nos objetivos dos processos organizacionais;

IV. 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 Plano de Tratamento; e

V. monitoramento e comunicação: etapa contínua em que as instâncias envolvidas com Gestão de Riscos interagem para monitoramento dos riscos. Abrange também 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.

Parágrafo único. A utilização de ferramentas de apoio à gestão de riscos deverá priorizar o uso de software livre ou Software Público Brasileiro.

Art. 7º A metodologia de riscos definirá os critérios de avaliação dos riscos, contemplando as escalas progressivas para avaliação do evento de risco nos parâmetros de probabilidade e impacto, bem como a classficação final na matriz de risco;

CAPÍTULO V - DAS COMPETÊNCIAS E RESPONSABILIDADES

Art. 8º São instâncias responsáveis pelo Sistema de Gestão de Riscos do Ministério do Desenvolvimento Regional - SGR-MDR:

I. Comitê Interno de Governança - CIGov;

II. Secretaria Executiva - SE;

III. Unidades Organizacionais; e

IV. Gestores de risco.

§1º A instância prevista no inciso I representa o nível estratégico da ação, sendo responsável por decisões estratégicas e diretrizes no âmbito da gestão de riscos.

§2º A instância prevista no inciso II representa o nível tático da ação, sendo responsável pela coordenação das ações, monitoramento do SGR-MDR e consolidação de informações estruturadas sobre riscos.

§3º As instâncias previstas nos incisos III e IV representam o nível operacional da ação, sendo responsáveis pelo gerenciamento das ações de identificação, avaliação e tratamento dos riscos.

Art. 9º Compete ao Comitê Interno de Governança, nível estratégico do Sistema de Gestão de Riscos do Ministério do Desenvolvimento Regional:

I. aprovar a presente Política de Gestão de Riscos e suas revisões;

II. definir os níveis de apetite a risco dos processos organizacionais;

III. aprovar a Metodologia de Gestão de Riscos e suas revisões;

IV. avaliar a evolução de níveis de riscos e a efetividade das medidas de controle implementadas;

V. avaliar o desempenho do Sistema de Gestão de Riscos e sua eficácia em relação aos objetivos pretendidos;

VI. garantir o apoio institucional para promover a gestão de riscos, em especial os seus recursos, o relacionamento entre as partes interessadas e o desenvolvimento contínuo dos servidores;

VII. garantir o alinhamento da gestão de riscos aos padrões de ética e de conduta, em conformidade com o Programa de Integridade do Ministério do Desenvolvimento Regional;

VIII. estimular a contínua capacitação do corpo funcional em gestão de riscos e em outras competências técnicas correlatas, por meio de palestras, cursos e eventos; e

IX. incentivar a adoção de boas práticas de governança e de gestão de riscos.

Art. 10. Compete à Secretaria Executiva, nível tático do Sistema de Gestão de Riscos do

Ministério do Desenvolvimento Regional:

I. propor ao CIGov a Política de Gestão de Riscos e suas revisões;

II. propor ao CIGov a Metodologia de Gestão de Riscos e suas revisões;

III. monitorar a evolução de níveis de riscos e a efetividade das medidas de controle implementadas;

IV. orientar as unidades organizacionais na aplicação da Metodologia de Gestão de Riscos; e

V. monitorar o desempenho do Sistema de Gestão de Riscos e sua eficácia em relação aos objetivos pretendidos.

§ 1º A Coordenação-Geral de Inteligência e Riscos deverá subsidiar a Secretaria Executiva no cumprimento das atribuições do caput.

§ 2º A Assessoria Especial de Controle Interno será responsável por coordenar a gestão dos riscos à Integridade, conforme definido no Programa de Integridade do Ministério do Desenvolvimento Regional.

Art. 11. Compete às Unidades Organizacionais do Ministério do Desenvolvimento Regional, níveis operacionais do Sistema de Gestão de Riscos do Ministério do Desenvolvimento Regional:

I. identificar e avaliar os riscos dos processos sob sua responsabilidade, em conformidade ao que define esta PGR;

II. propor respostas e respectivas medidas de controle a serem implementadas nos processos organizacionais sob sua responsabilidade; e

III. indicar os Gestores de Risco.

Art. 12. Compete aos Gestores de Risco, nível operacional do Sistema de Gestão de Riscos do MDR:

I. assegurar que o risco seja gerenciado de acordo com a política e metodologia de gestão de riscos;

II. monitorar o risco ao longo do tempo, de modo a garantir que as respostas adotadas

resultem na manutenção do risco em níveis adequados, de acordo com a política e metodologia de gestão de riscos;

III. garantir que as informações adequadas sobre o risco estejam disponíveis para as instâncias do nível tático da gestão de riscos; e

IV. promover a disseminação da cultura de gestão de riscos.

Parágrafo único. Os Gestores de Risco devem ser chefes de unidade com alçada suficiente para orientar e acompanhar as ações de identificação, avaliação e tratamento dos riscos.

Art. 13. Os demais servidores do MDR deverão colaborar no limite de suas atribuições para o atingimento dos objetivos da gestão de riscos, assessorando no processo de gerenciamento de riscos com a aplicação de técnicas, métodos e instrumentos e comunicando as deficiências identificadas às instâncias superiores.

Art. 14. O Comitê Interno de Governança, a Secretaria Executiva, as Unidade Organizacionais e os Gestores de Risco deverão manter fluxo regular e constante de informações entre si, no limite de suas competências.

Art. 15. Os casos omissos ou as excepcionalidades serão resolvidos pelo Comitê Interno de Governança.

Art. 16. Esta Política de Gestão de Riscos foi aprovada pela Resolução CIGOV nº 7, de 27 de agosto de 2020 e entra em vigor na data de publicação da referida Resolução no Boletim de Serviços Eletrônico.

ROGÉRIO SIMONETTI MARINHO
Ministro de Estado e Presidente do Comitê Interno de Governança

ANEXO IV – METODOLOGIA DE GESTÃO DE RISCOS

METODOLOGIA DE GESTÃO DE RISCOS DO MINISTÉRIO DO DESENVOLVIMENTO REGIONAL

Introdução

O esforço de integração e convergência interna do Ministério do Desenvolvimento Regional – MDR 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 MDR contempla um processo contínuo, desenhado para identificar, responder e monitorar eventos que possam constranger os objetivos definidos ao Ministério, sob liderança da Diretoria de Gestão Estratégica e Coordenação Estrutural - DICOG, em apoio ao Comitê Interno de Governança - CIGov.

Os conceitos, princípios, objetivos, diretrizes e responsabilidades no MDR na Gestão de Riscos estão dispostos na Política de Gestão de Riscos - PGR, aprovada pela Resolução CIGov nº 07/2020.

De forma geral, compreende-se que gerenciar é um processo de melhoria contínua de identificação, avaliação, administração e controle de potenciais eventos de riscos, sejam eles ameaças ou oportunidades. Esta gestão é importante na medida em que permite aos gestores e tomadores de decisão avaliar a factibilidade no alcance dos objetivos organizacionais, e assim decidir pela manutenção ou revisão de procedimentos para garantir o sucesso da organização. O desenvolvimento de uma gestão de riscos eficaz e eficiente, ao aumentar a probabilidade de atingimento dos objetivos do MDR, contribuirá ao cabo para uma condução mais eficiente das políticas públicas.

O processo de gestão de riscos definido nesta Metodologia está aderente às diretrizes definidas na Política de Gestão de Riscos do MDR, em seu artigo 6º, que define, no mínimo, as seguintes etapas:

I. Análise de ambiente e dos objetivos;
II. Identificação dos riscos;
III. Avaliação dos riscos;
IV. Resposta aos riscos;
V. Monitoramento e Comunicação.

Ao longo deste documento será detalhada cada uma destas etapas, com indicação de eventuais técnicas complementares, de forma a estruturar o método de gerenciamento de riscos.

Inicialmente, cumpre informar que para a implementação do gerenciamento de riscos será utilizado o sistema informatizado denominado Agatha para documentar as etapas da gestão de riscos – Agatha. Site: https://agatha.mdr.gov.br.

Análise do Ambiente e dos Objetivos

Esta etapa trata do levantamento e registro dos aspectos externos e internos essenciais ao alcance dos objetivos institucionais, permitindo a compreensão clara do ambiente em que a organização se insere e identificar os fatores que podem influenciar a capacidade da organização de atingir os resultados planejados.

Essa etapa permite priorizar e facilitar a abordagem a partir do processo, projeto, programa, atividade ou iniciativa objeto do gerenciamento de riscos. Poderá ser realizada análise SWOT sobre os pontos fortes e fracos do ambiente interno[1], as oportunidades e ameaças do ambiente externo[2], e a identificação dos principais atores envolvidos no processo referente ao gerenciamento de riscos.

Deverá envolver também 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.

Identificação dos Riscos

A etapa de identificação dos riscos envolve o reconhecimento, descrição e registro do evento de risco, com a caracterização de suas prováveis causas e possíveis consequências, caso ocorra.

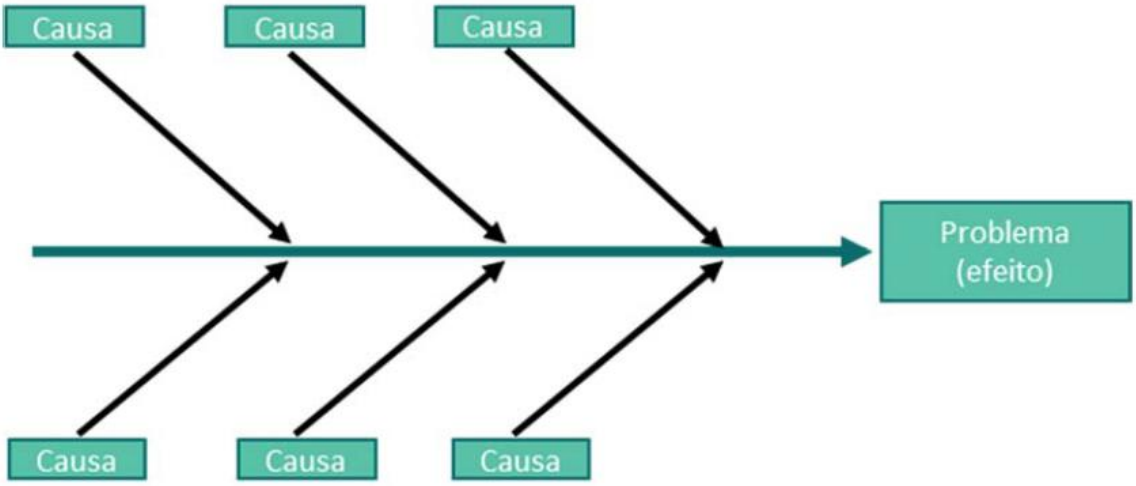
Nesta etapa, deverá ser desenvolvida uma lista de eventos de riscos que podem constranger os resultados e o alcance dos objetivos, afetando o valor público a ser entregue à sociedade.

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 aos processos sob análise.

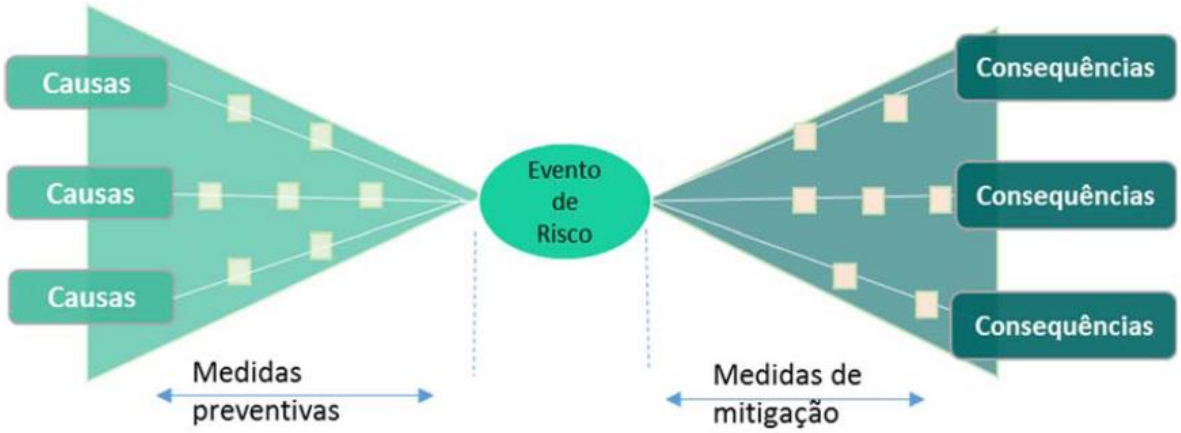
Para cada evento de risco identificado ao longo do processo de gerenciamento, é desejável especificar, explorar e ressaltar suas prováveis causas e possíveis consequências.

O risco não deve ser descrito simplesmente como o "não alcance" do objetivo. A descrição do risco deve prover insights sobre o que pode dar errado no processo.

Como apoio à coleta estruturada de informações, poderão ser utilizadas técnicas[3] como Brainstorming, Diagrama de Ishikawa, Bow Tie, entrevista com especialistas, e análise de cenários.



ANEXO IV - FIGURA 1 - DIAGRAMA DE ISHIKAWA



ANEXO IV - FIGURA 2 - BOW-TIE

[1] Pode envolver aspectos como governança, estrutura organizacional, funções, responsabilidades, políticas, estratégias, capacidades, competência, alçadas, sistemas de informação, processos decisórios, cultura organizacional.

[2] Pode envolver aspectos no âmbito cultural, social, político, regulatório, financeiro, tecnológico, econômico, ambiental. Inicialmente, recomenda-se utilizar a Matriz SWOT: *strengths, weaknesses, opportunities and threats* (forças, fraquezas, oportunidades e ameaças).

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

A sintaxe a seguir para descrição de aspectos envolvendo um evento de risco pode auxiliar na reflexão e desenvolvimento desta etapa:

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

ANEXO IV - FIGURA 3 - SINTAXE DO EVENTO DE RISCO

Já a classificação do evento de risco pode observar aspectos subdivididos em categorias, como:

- **Estratégico:** eventos de potencial impacto na missão, metas ou objetivos estratégicos da unidade/órgão;
- **Operacional:** eventos que podem comprometer as atividades da unidade, normalmente associados a falhas, deficiência ou inadequação de processos internos, pessoas, infraestrutura e sistemas, afetando o esforço da gestão quanto à eficácia e à eficiência dos processos organizacionais;
- **Orçamentário:** eventos que podem comprometer a capacidade da unidade de contar com os recursos orçamentários necessários à realização de suas atividades, ou eventos que possam comprometer a própria execução orçamentária;
- **Reputação:** eventos que podem comprometer a confiança da sociedade em relação à capacidade da unidade em cumprir sua missão institucional; interferem na imagem do órgão;
- **Fiscal:** eventos que podem afetar negativamente o equilíbrio das contas públicas;
- **Conformidade:** eventos que podem afetar o cumprimento de leis e regulamentos aplicáveis;
- **Social:** eventos que podem comprometer o valor público esperado ou percebido pela sociedade em relação ao resultado da prestação de serviços públicos da instituição; e
- **Integridade:** eventos relacionados a corrupção, fraudes, irregularidades e/ou desvios éticos e de conduta, que possa comprometer os valores preconizados pelo Ministério e a realização de seus objetivos.

Caso o evento de risco esteja associado a duas ou mais categorias de classificação, deverá ser escolhida a categoria que reflita o aspecto mais relevante quanto ao impacto que o evento de risco poderá trazer, caso se materialize.

Avaliação dos Riscos

A etapa de **avaliação dos riscos** visa promover o entendimento do nível do risco e de sua natureza, especialmente quanto à estimação da probabilidade de ocorrência, e do impacto destes eventos identificados como risco nos objetivos dos processos organizacionais.

Avaliação do risco inerente

Essa estimação pode ser feita com base em uma escala progressiva de cinco níveis (1 a 5), na forma:

- **Probabilidade**: muito baixa, baixa, média, alta, e muito alta; e
- **Impacto**: muito baixo, baixo, médio, alto, e muito alto.

A probabilidade escala-se em cinco níveis, com base em avaliação quantitativa ou qualitativa que utilizará o conhecimento técnico e experiências vivenciadas dos partícipes no processo a ser avaliado, e sempre que possível, será feita também uma avaliação quantitativa, com base nos dados estatísticos de eventos de riscos já materializados, por determinado período de tempo ou média histórica disponível. Nesse caso, é também possível o uso de técnicas de apoio à coleta estruturada de informações.

A avaliação da probabilidade utiliza da seguinte relação de aspecto avaliativo, frequência e valor do peso para apuração do risco:

- **Muito baixa:**
  - Aspecto avaliativo: evento que pode ocorrer apenas em circunstâncias excepcionais;
  - Frequência observada/esperada: menor ou igual a 20%;
  - Peso na apuração do risco: 1 (um)

- **Baixa:**
  - Aspecto avaliativo: evento pode ocorrer em algum momento;
  - Frequência observada/esperada: maior que 20% e menor ou igual a 40%;
  - Peso na apuração do risco: 2 (dois)

- **Média:**

- Aspecto avaliativo: evento deve ocorrer em algum momento;
- Frequência observada/esperada: maior que 40% e menor ou igual a 60%;
- Peso na apuração do risco: 3 (três)

- **Alta:**
- Aspecto avaliativo: evento deve ocorrer na maioria das circunstâncias;
- Frequência observada/esperada: maior que 60% e menor ou igual a 80%;
- Peso na apuração do risco: 4 (quatro)

- **Muito alta:**
- Aspecto avaliativo: evento com altíssima probabilidade de ocorrência;
- Frequência observada/esperada: maior que 80%;
- Peso na apuração do risco: 5 (cinco)

A avaliação de impacto utilizará os seguintes fatores de análise e pesos de distribuição caso o evento de risco ocorra:

- **Orçamentário/Financeiro**
- Aspecto avaliativo: se evento de risco impacta na gestão orçamentária e financeira do MDR;
- Peso na apuração do risco: 30% (trinta por cento).

- **Resultados nas Políticas Públicas Setoriais**
- Aspecto avaliativo: se evento de risco impacta no atingimento dos resultados das estratégias setoriais expostas nas Políticas e Planos Nacionais de cada uma das políticas setoriais afetas ao MDR;
- Peso na apuração do risco: 25% (vinte e cinco por cento).

- **Resultados Organizacionais**
- Aspecto avaliativo: se evento de risco impacta no atingimento dos resultados definidos pelo próprio órgão em seus instrumentos de planejamento organizacional, tais como Planejamento Estratégico Institucional (PEI) e Plano Plurianual (PPA);
- Peso de 20% (vinte por cento) no cálculo do impacto do evento de risco.

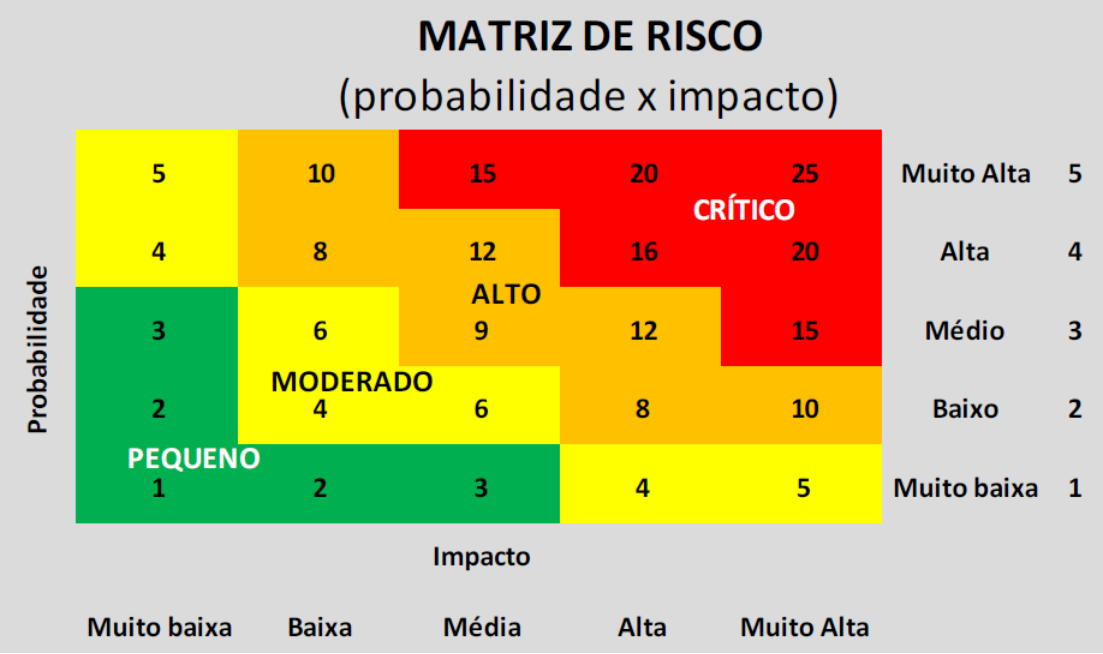
- **Conformidade**

- Aspecto avaliativo: se evento de risco impacta nos atos normativos vigentes que regem o objeto (processo, projeto) da Gestão de Riscos, e medidas correlacionadas determinadas pelos órgãos de controle;
- Peso na apuração do risco: 15% (quinze por cento).

- **Imagem/Reputação**
- Aspecto avaliativo: se evento de risco impacta nos aspectos de confiança da sociedade em relação à capacidade do MDR em cumprir sua missão institucional e que interferem na imagem do órgão;
- Peso na apuração do risco: 10% (dez por cento).

É desejável que a consistência das percepções de probabilidade e impacto seja sustentada pelo registro de **evidências**, como dados, documentos, relatórios, documentos SEI.

A conjunção da avaliação de probabilidade e impacto formam o resultado final da avaliação de risco agrupada em 4 (quatro) níveis, conforme **Matriz de Riscos** abaixo:



ANEXO IV - FIGURA 4 - MATRIZ DE RISCO

- **Nível Pequeno**: é possível conviver com o risco, mantendo as práticas e controles existentes;
- **Nível Moderado**: é possível promover ações que atenuem causas e/ou consequências;
- **Nível Alto**: é necessário a elaboração de plano de ação para evitar ou eliminar as causas e/ou consequências;

- **Nível Crítico**: é necessário a elaboração de plano de ação para evitar ou eliminar as causas e/ou consequências, bem como considerar a necessidade de mobilização imediata de recursos, materiais e pessoal capacitado, com vistas ao tratamento desse risco.

Avaliação do risco residual

Destaca-se que neste momento deve-se avaliar a eficácia dos controles[4] existentes a fim de aferir se o risco residual continua dentro do nível de risco aceitável ao processo em análise, a avaliação será notadamente quanto ao desenho e à operação dos controles existentes, na seguinte forma:

- **Desenho:** há procedimento de controle suficiente e formalizado?

a) Não há procedimento de controle;
b) há procedimentos de controle, mas insuficiente e não formalizado;
c) há procedimentos de controle formalizado, mas insuficientes;
d) há procedimentos de controle suficientes, mas não formalizados; ou
e) há procedimentos de controle suficientes e formalizados.

- **Operação**: há procedimento de controle sendo executado? Há evidências de sua execução?

a) Não há procedimento de controle;
b) há procedimentos de controle, mas não são executados;
c) há procedimentos de controle, mas parcialmente executados;
d) há procedimentos de controle executados, mas não evidenciados; e
e) há procedimentos de controle executados de forma evidenciável.

Orienta-se que todo o processo de Gestão de Riscos observe os controles 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.

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 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 pelo Ministério do Desenvolvimento Regional, todos os riscos com nível de criticidade apurado superior ao nível definido, deverão preferencialmente ser instituídos controles e/ou ações mitigadoras com o objetivo de reduzi-lo ou compartilhá-lo até sua conformidade com o limite de exposição aceitável pelo Ministério.

Os controles propostos podem ser avaliados quanto a:

- **Tipo**:
  - Preventivo: tem como objetivo prevenir a materialização 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 (ex: identificação, pela vigilância, das pessoas que estão no prédio, mas sem credencial).

[4] Controle é a medida que mantém e/ou modifica o risco, e pode estar relacionado a qualquer processo, política, dispositivo, prática, inciativa, entre outras condições e/ou ações, relacionadas ao objeto da Gestão de Riscos.

- **Natureza**:
  - Manual: controle realizado por pessoa (ex: conferência de assinatura);
  - Automático: controle processados 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.

A implementação dos controles pode considerar 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.

Monitoramento e Comunicação

É importante que as informações apresentadas nos meios de monitoramento possuam qualidade contextual e de representação como 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:** volume de informação adequado e suficiente;
- **Concisão:** informação deve ser apresentada de forma compacta;
- **Consistência:** as informações apresentadas devem ser compatíveis;
- **Clareza:** informação deve ser facilmente compreensível; e
- **Padronização:** informação deve ser apresentada no padrão aceitável.

O acesso a informações confiáveis, íntegras e tempestivas é vital para a eficiência da gestão visando facilitar o alcance dos objetivos de cada processo. 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.

O MDR deverá assegurar que os controles permaneçam eficazes e que ambiente de controle se mantenha efetivo ao longo do tempo.

> *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 e 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)*

Cabe destacar que a implementação de atividades relacionadas à gestão de risco e controles, por si só, não é suficiente a 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 são essenciais para que cada um dos participantes saiba como seu cargo se encaixa na estrutura corporativa de gestão de riscos e controles. As instâncias e as competências de cada uma estão definidas na Política de Gestão de Riscos do MDR.

ANEXO V – EVENTOS DE RISCO OPERACIONAL

Segue uma lista sugestiva e não exaustiva de eventos de risco operacional.

Risco Operacional	
Fator	**Subfator e Exemplos de Riscos (Taxonomia)**
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 ▪ 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 ▪ 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 ▪ 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 ▪ 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 ▪ 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 ▪ 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 ▪ 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 ▪ 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
	SOLUÇÃO 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 CATASTROFE**: ▪ *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

ANEXO VI – CONTROLES BÁSICOS

Segue uma lista sugestiva e não exaustiva de controles básicos.

Categoria de Risco	Fatores	Subfatores	Controles Básicos
Risco de Integridade			Postura da alta administração
			Políticas e procedimentos anticorrupção
			Mapeamento dos Riscos de Corrupção
			Criação de indicadores dos riscos de corrupção dos passos decisórios
Risco de Conformidade			Acompanhamento e Análise de Normas e Regulamentos Externos
			Pareceres da Assessoria Jurídica
			Atividades de Treinamento
			Normas e Procedimentos
Risco Operacional	**Pessoas**	Carga de Trabalho	Planejamentos de longo, médio e curto prazos
			Acordo de Trabalho
			Pesquisa de Clima Organizacional
			Reuniões Participativas
		Competências	Identificação da Necessidade de Conhecimento / Habilidades
			Atividades de Treinamento
			Normas e Procedimentos
			Ferramentas de autoavalização de Conhecimentos / Habilidades
		Qualidade de Vida no Trabalho	Pesquisa de Clima Organizacional
			Condições Ambientais
			Comunicação com a Administração
			Processo de Gerenciamento de Equipes
		Conduta	Valores Éticos e Normas de Conduta do Órgão / Unidade
			Alçadas e Limites
			Mecanismos de Motivação / Recompensa / Punição – Práticas de Disciplina e Demissão
			Reconhecimento de Responsabilidade por Escrito
			Conferências e Autorizações
			Rodízio de Funcionários
			Segregação de Funções
			Testes de Conformidade
			Canais de Comunicação – Com a Sociedade
			Normas e Procedimentos

Risco Operacional	**Processos**	Comunicação Interna	Canais de Comunicação – Com os servidores
			Normas e Procedimentos
		Modelagem	Ferramentas para Análise e Melhoria Contínua de Processos
			Metodologia de Autoavalização de Riscos e Controles
			Validações – *Backtesting*
		Segurança Física	Mecanismos de Segurança Física
			Controles de Acesso Físico
			Manutenção de Equipamentos
		Pontos de Controle	Normas e Procedimentos
			Metodologia de Autoavalização de Riscos e Controles
			Mecanismos de Monitoramento e Reporte
		Adequação à Legislação	Testes de Conformidade
			Normas e Procedimentos
	Sistemas	Segurança Lógica	Políticas e Diretrizes
			Controles de Acesso Lógico
			Arquivo e Preservação de Registros
		Hardware e *Software*	Manutenção de Equipamentos
			Layout de formulários e Sistemas
			Planos de Contingência
		Análise e Programação	*Layout* de Formulários e Sistemas
			Validações - *Backtesting*
			Atividades de Treinamento
		Rede de Comunicação	Planos de Contingência
			Manutenção de Equipamentos
	Eventos Externos	Desastres Naturais e Catástrofe	Planos de Contingência
			Atividades de Treinamento
		Ambiente Regulatório	Análise da Conjuntura Política e Econômica Nacional e Internacional
		Ambiente Social	Análise da Conjuntura Política e Econômica Nacional e Internacional
		Fornecedores	Controles de Serviços Terceirizados
			Planos de Contingência
		Clientes	Controles de Acesso Lógico
		Meio Ambiente	Valores Éticos e Normas de Conduta da Empresa
Risco de Imagem			Valores Éticos e Normas de Conduta da Empresa
			Normas e Procedimentos
			Controles de Serviços Terceirizados
			Pesquisa de Satisfação
			Canais de Comunicação - Com a Sociedade
			Canais de Comunicação – Com os Servidores

MANUAL DO SISTEMA AGATHA

Sistema de Gestão de Integridade, Riscos e Controles

SUMÁRIO

Histórico de Versões do manual do Ágatha

Data	Versão do Manual	Descrição	Autor	Versão do Produto
07/12/2017	1.0	Elaboração do documento	Thatyane Costa	1.0
30/07/2020	2.0	Elaboração de documento	Flávia Amaral	2.0

1. Introdução ao sistema

As responsabilidades e deveres do governo em relação ao bem público exigem a adoção de práticas e estratégias eficazes de gestão. Neste contexto, a gestão de riscos, controles internos da gestão e integridade torna-se uma importante ferramenta para ajudar na tomada de decisões baseadas em metodologias e normas que geram, dentre outros benefícios, a redução ou a eliminação de retrabalhos.

O Sistema AGATHA – Sistema de Gestão de Integridade, Riscos e Controles consiste em uma ferramenta automatizada, desenvolvida pelo extinto Ministério do Planejamento, Desenvolvimento e Gestão - MP, para auxiliar no processo de gerenciamento de riscos e controle.

Considerando que o Sistema foi adaptado à metodologia do Ministério do Desenvolvimento Regional – MDR, fizemos algumas alterações e complementamos as informações do manual originalmente elaborado pelo MP, de modo a facilitar o uso do sistema de acordo com a nossa metodologia aprovada pelo Comitê Interno de Governança.

Este manual visa auxiliar o manuseio do sistema, passando por todas as etapas da metodologia, as quais foram detalhadas e explicitadas no Manual de Gestão de Riscos, Controles Internos e Integridade. Dessa forma, para entender melhor a metodologia em si, recomenda-se consultar a esse Manual, o qual apresenta resumidamente os modelos de gestão de riscos existentes, a política e a metodologia do MDR, detalhando todas as etapas do gerenciamento de riscos e, ainda, apresentando o Programa de Integridade do Ministério com as definições e especificações dos riscos à integridade.

2. Como solicitar acesso ao Sistema

O acesso deve ser solicitado por e-mail. A solicitação deve ser feita ao endereço aeci.riscos@mdr.gov.br, por ocupante de, no mínimo, DAS ou FCPE 4 da respectiva secretaria/unidade. Na mensagem, deve ser informado o nome do(s) servidor(es), CPF, e-mail e o perfil que deverá ser concedido, conforme orientações do próximo item.

3. Perfis

No Sistema Ágatha há os seguintes perfis que serão utilizados, nesse momento, pelo MDR:

Analista de Risco: é responsável por iniciar um processo, preencher todas as informações, fazer a identificação e a análise dos riscos e definir os planos de controle. Ele terá acesso apenas aos processos da unidade dele em que está cadastrado como analista responsável. É recomendável que sejam cadastrados pelo menos dois

analistas para cada processo. Esse perfil corresponde ao gestor do risco descrito na Política de Gestão de Riscos do MDR.

Gestor do Processo: é o responsável por aprovar os processos em que está como gestor, os quais foram alimentados pelo(s) analista(s) de risco. Ele consegue visualizar e possui a gestão somente sobre os processos das unidades pelas quais é responsável. Deverá ser ocupante de DAS ou FCPE 4 ou superior.

Núcleo: tem acesso a todas as funcionalidades gerenciais, consulta e emissão de relatórios de todos os processos. A Coordenação-Geral de Inteligência e Riscos da Assessoria Especial de Controle Interno é a unidade responsável por esse perfil.

Comitê: acessam na modalidade consulta e emitem relatórios de todos os processos de todas as unidades do MDR. Quem tem esse perfil são os membros do Comitê Interno de Governança - CIGov.

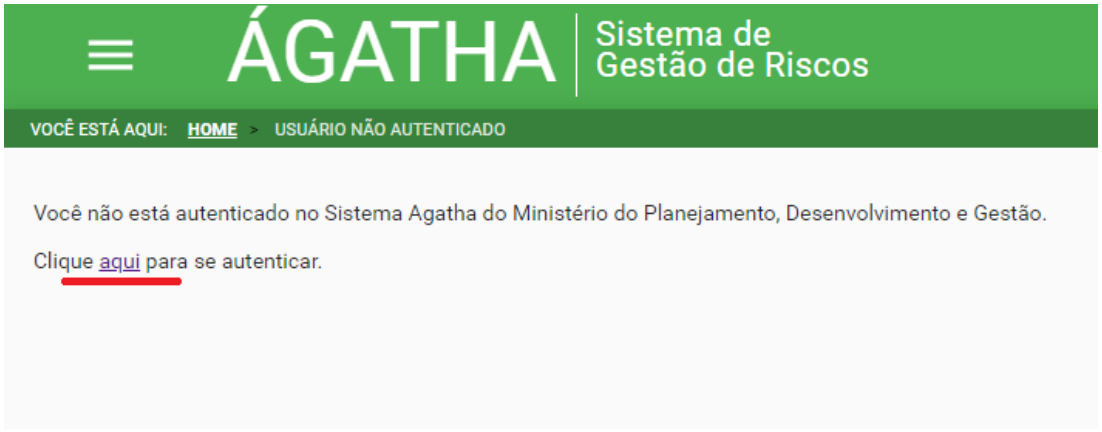
4. Passo a passo para acessar a tela inicial do Sistema

Figura 1 - Navegador

1. Abra o navegador (*browser*) de sua preferência (Internet Explorer, Chrome, Mozilla Firefox, Safari…);

Figura 2 - Barra de Endereço

2. Digite na barra de endereço de seu navegador: https://agatha.mdr.gov.br e pressione "*enter*" em seu teclado;
3. Será carregada a página de login do Sistema Agatha, onde o usuário deverá clicar em "*aqui*", conforme indicado na figura abaixo, para entrar no sistema.



4. O Login corresponde ao CPF do usuário e a Senha é a mesma cadastrada no portal "gov.br". Se for o primeiro acesso ao "gov.br", deverá ser feito o cadastro.
5. Aguarde o carregamento da **Tela Inicial**.

4.1 Tela Inical

Após o login, a **tela inicial** do sistema AGATHA será carregada e o usuário poderá acessar o *Menu* do sistema e, dependendo do perfil cadastrado, poderá ter acesso às ações descritas abaixo:

- Pesquisar macroprocesso /processos,
- Incluir novo mapeamento de risco,
- Visualizar macroprocesso /processos,
- Alterar dados do processo,
- Excluir um processo desejado.

5. Processo – Gerenciar

Para iniciar um **novo mapeamento** de riscos ou verificar os que **já foram lançados** no sistema, deve-se acessar a opção "Processo" e em seguida a opção "Gerenciar" em Gerenciar Processo, conforme figura 3.

Figura 3 – Tela inicial

Para se iniciar um **novo mapeamento** de riscos, clique na opção "+ NOVO MAPEAMENTO" que está circulado de vermelho e, para consultar um **processo já criado**, preencha as informações e clique em "CONSULTAR", também circulado de vermelho ("vide" figura 4).

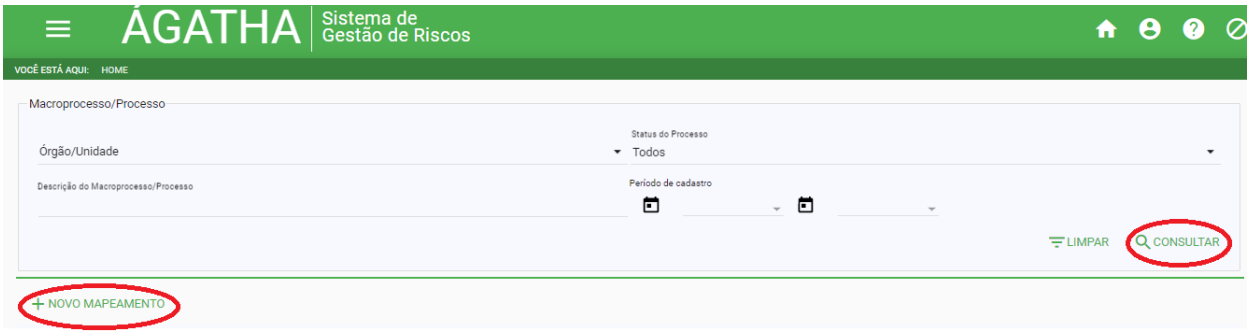


Figura 4 – Mapeamento de processo

6. Análise de Ambiente e de Fixação de Objetivos

Na Aba "ANÁLISE DE AMBIENTE E DE FIXAÇÃO DE OBJETIVOS" preencha o nome da Diretoria ou equivalente e da Coordenação. Em seguida, preencha os campos com as informações a respeito do ambiente e fixação de objetivos, marcando as opções "Sim ou Não", conforme Figura 5 abaixo.

Deve-se selecionar o nome do Macroprocesso e na sequência incluir o nome do processo e seu objetivo. A seguir, informar as Leis e Regulamentos que possuam relação e/ou afetam o processo e quais sistemas, caso existam, são utilizados para a realização do processo.

Na sequência, informar quem é o Gestor Responsável pelo processo, o Responsável pela Análise e o período em que foi realizada a análise. O Gestor Responsável pelo processo visualiza e aprova os processos sob sua supervisão e o Responsável pela Análise é o responsável pelo mapeamento, isto é, é o analista de risco., conforme perfis descritos no item 3.

Conforme explicitado no Manual de Gestão de Riscos, Controles Internos e Integridade, esta é a primeira etapa da gestão de riscos. Todas as informações do processo deverão ser incluídas nesta aba "ANÁLISE DE AMBIENTE E DE FIXAÇÃO DE OBJETIVOS". É possível, inclusive, incluir documentos como anexo, especificando o escopo de análise do processo e o mapa do processo, caso a unidade possua.

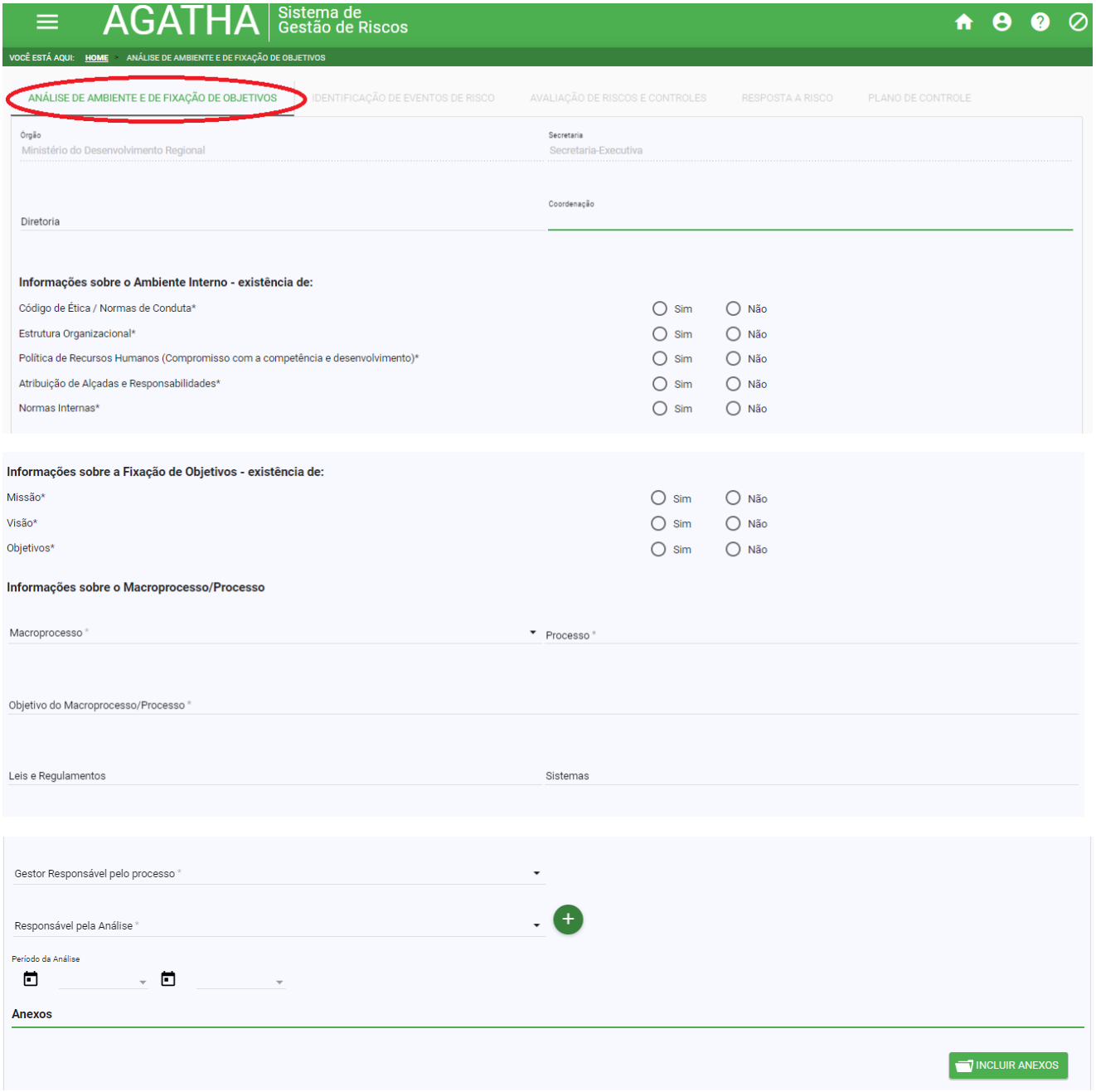


Figura 5 - Análise de Ambiente e de Fixação de Objetivos

Além dessas informações, nesta aba, há a matriz Swot, em que deverão ser identificadas as forças e as fraquezas (ambiente interno); as oportunidades e as ameaças (ambiente externo), conforme detalhamento na figura abaixo. Cabe esclarecer que o ambiente externo é sempre **externo ao MDR**, sendo que o ambiente interno pode ser a **própria secretaria ou o Ministério como todo**.

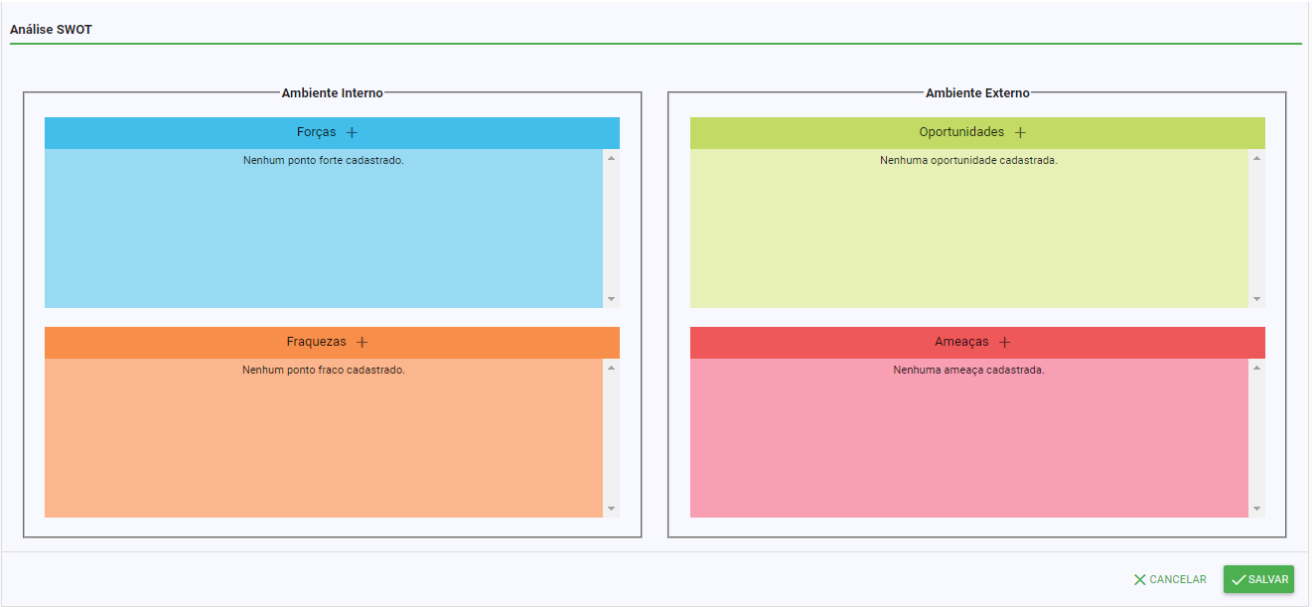


Figura 6 - Análise Swot

7. Identificação de Eventos de Risco

Após o preenchimento das informações na Aba “ANÁLISE DE AMBIENTE E DE FIXAÇÃO DE OBJETIVOS” deve-se passar para a próxima etapa na gestão de riscos que é a fase de identificação do evento de risco. Para isso, basta clicar na Aba “IDENTIFICAÇÃO DO EVENTO DE RISCO”, conforme a figura 7.

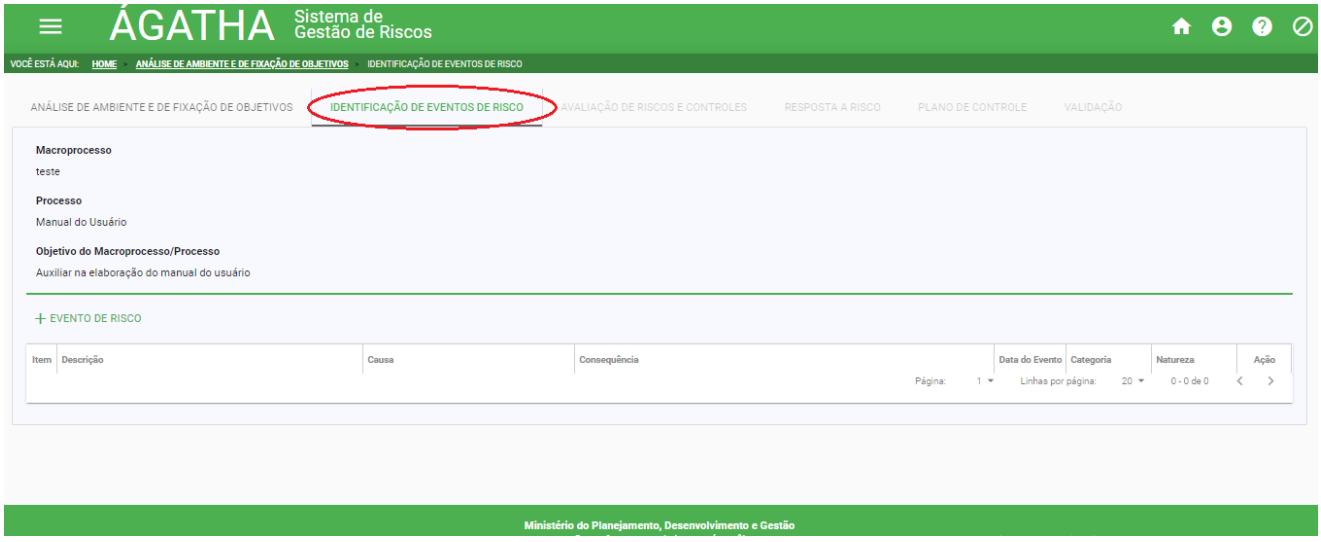


Figura 7 - Identificação de Eventos de Risco

A etapa de identificação dos riscos envolve reconhecimento, descrição e registro do evento de risco, com a caracterização de suas prováveis causas e possíveis consequências, caso o evento ocorra. No Manual de Riscos,

Controles Internos e Integridade, há descrição do que deve ser feito nesta etapa, portanto, sugere-se que esse Manual seja consultado.

7.1 Incluir Evento de Risco

Descrever o risco identificado no espaço destinado a “Evento de Risco”, conforme tela abaixo.

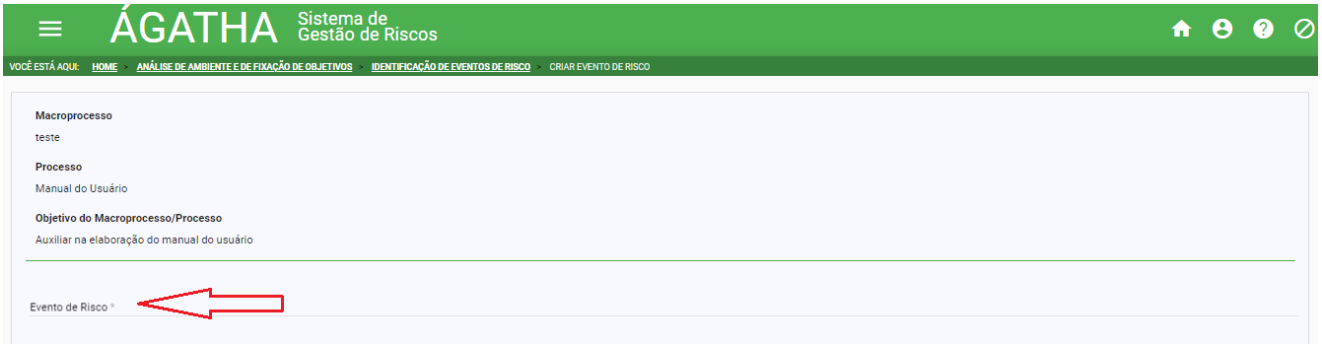


Figura 8 - Identificação de Eventos de Risco

No Manual já mencionado, há orientações sobre a melhor forma de identificar o risco.

Em seguida, deverão ser incluídas tantas causas desse risco, quanto for necessário. Para incluir a primeira causa do risco, clique na opção “Causa” e, depois de digitar o texto, clique em confirmar para salvar. Para incluir novas causas, basta clicar na opção “+ Causa”, até que todas as causas identificadas estejam lançadas.

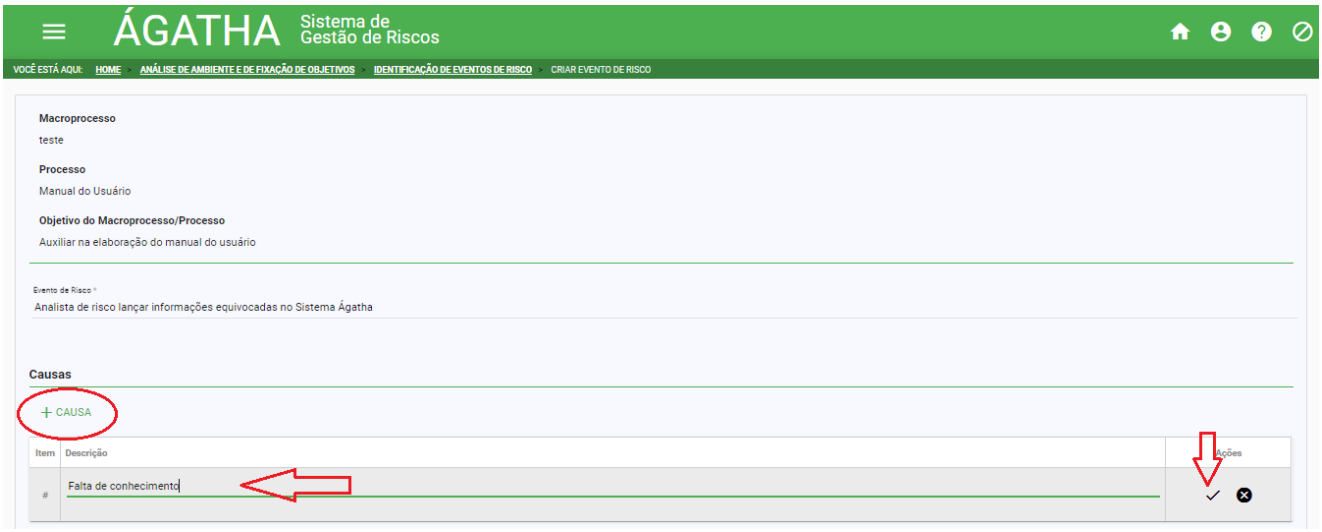


Figura 9 - Identificação das Causas do Evento de Risco

O mesmo procedimento é necessário para o lançamento das consequências. Para incluir a primeira consequência clicar na opção “Consequência” e para incluir outras consequências clicar na opção “+ Consequência”, até todas as consequências identificadas estejam lançadas.

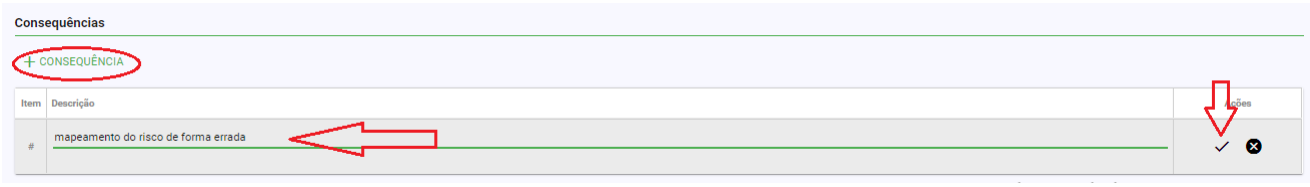


Figura 10 - Identificação das Consequências do Evento de Risco

Na sequência, deve-se selecionar a Categoria e a Natureza do Risco, conforme definições descritas no Manual de Riscos, Controles Internos e Integridade, clicar em “SALVAR” ao final do preenchimento das informações.

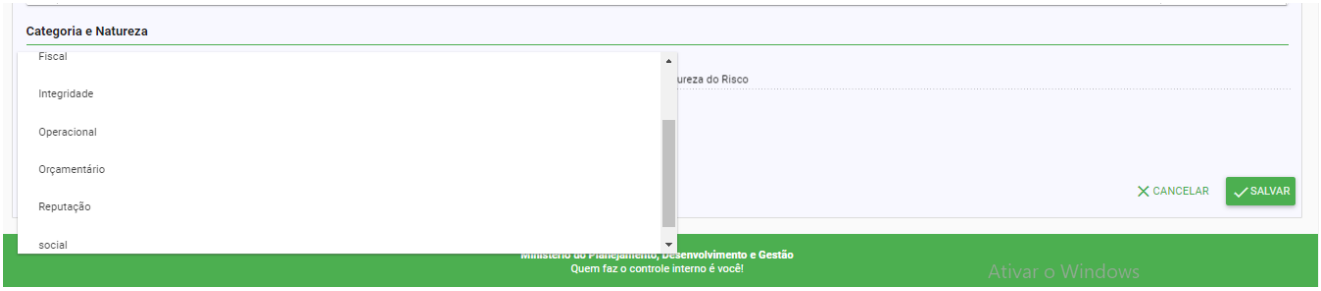


Figura 11 - Incluir Categoria do Risco

Caso o evento de risco esteja associado a duas ou mais categorias de classificação, deverá ser escolhida a categoria que reflita o aspecto mais relevante quanto ao impacto que o evento de risco poderá trazer, caso se materialize.

Importante ressaltar também que alguns riscos poderão ser categorizados, por exemplo, como operacional, mas há causas ou consequências relacionadas à integridade. É o caso, por exemplo, de conluio entre o servidor e a empresa contratada ou pressão externa ou interna sofrida pelo servidor para aprovar um documento. Nesses casos, deve-se marcar o “box” indicado na figura abaixo. Lembrando que no Manual já mencionado, há maiores explicações para riscos à integridade.

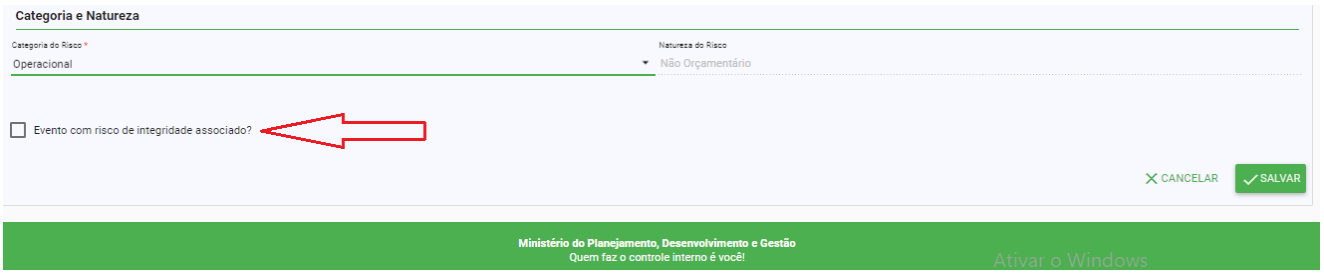


Figura 12 – Evento com risco de integridade associado

8. Avaliação de Riscos e Controles

Após o preenchimento das informações na Aba “IDENTIFICAÇÃO DO EVENTO DE RISCO” deve-se passar para a próxima etapa da gestão de riscos que é a avaliação dos riscos. Para isso, deve-se clicar na Aba “AVALIAÇÃO DE RISCOS E CONTROLES”.

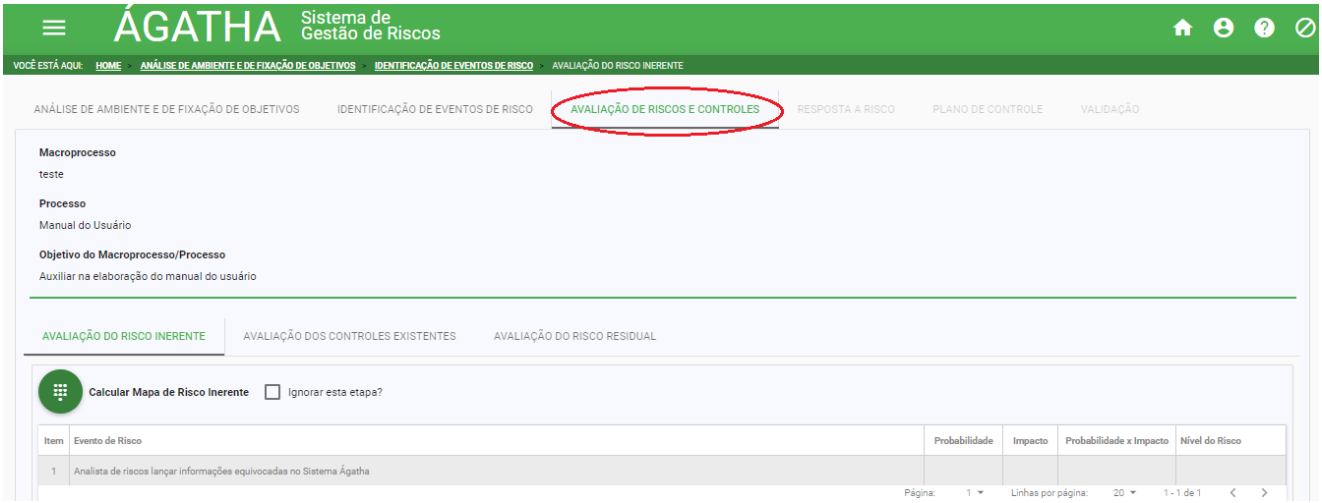


Figura 13 – Avaliação de Riscos e Controles

A etapa de avaliação dos riscos visa promover o entendimento do nível do risco e de sua natureza, especialmente quanto à estimativa da probabilidade de ocorrência e do impacto destes eventos identificados como risco nos objetivos dos processos organizacionais. Normalmente as causas se relacionam à probabilidade de o evento ocorrer e, as consequências ao impacto, caso o evento se materialize.

Inicialmente, deverá ser feita uma avaliação do risco inerente (risco bruto, sem considerar qualquer controle), em seguida, será feita uma análise do(s) controle(s) já existente(s) e, por fim, do risco residual (considerando os controles identificados e avaliados quanto ao desenho e a sua execução). Novamente, todas essas etapas estão explicitadas no Manual de Riscos, Controles Internos e Integridade.

8.1 Avaliação do risco Inerente

Na aba “AVALIAÇÃO DE RISCOS E CONTROLES”, clicar na opção “AVALIAÇÃO DO RISCO INERENTE” e em seguida, para iniciar o preenchimento, clicar no ícone “Calcular Mapa de Risco Inerente”, conforme figura abaixo.

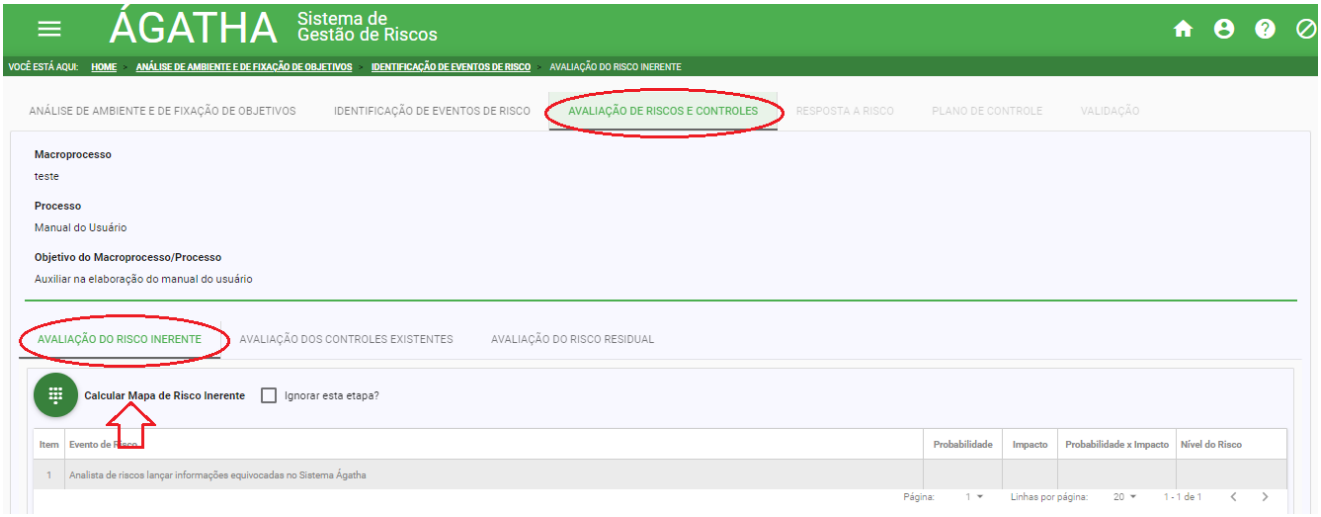


Figura 14 - Avaliação de Risco Inerente

Vale salientar que o “box” Ignorar esta etapa? apenas será marcado quando já estiver sendo feita uma segunda análise do processo, ou seja, em um primeiro momento, foram feitas todas as etapas de identificação e avaliação dos riscos do processo sob análise e, posteriormente, no segundo momento, devido a algumas modificações no cenário ou no processo, tornou-se necessário reavaliar os riscos do processo. Para essa segunda avaliação, poderá ser feito o trabalho apenas quanto ao risco residual, sem passar pela etapa do risco inerente.

8.1.1. Calcular mapa de risco inerente – Probabilidade

Na aba “PROBABILIDADE”, conforme figura 15, deve-se selecionar o nível de probabilidade de a causa do evento de risco acontecer, sem considerar os controles existentes.

Figura 15 - Risco Inerente – Probabilidade

A escala da probabilidade, de acordo com a metodologia do MDR, a qual se encontra explicitada no Manual já mencionado, é a seguinte:

Peso	Faixa	Aspecto avaliativo	Frequência
1	Muito baixa	evento que pode ocorrer apenas em circunstâncias excepcionais	≤ 20%
2	Baixa	evento pode ocorrer em algum momento	> 20% e ≤ 40%
3	Média	evento deve ocorrer em algum momento	> 40% e ≤ 60%
4	Alta	evento deve ocorrer na maioria das circunstâncias	> 60% e ≤ 80%
5	Muito alta	evento com altíssima probabilidade de ocorrência	> 80%

Tabela 7 - Dados da Probabilidade

O mesmo procedimento deverá ser executado para cada evento de risco que estiver lançado e, após a inclusão das informações clique em “SALVAR”.

8.1.2. Calcular mapa de risco inerente – Impacto

Na aba “IMPACTO”, deve-se selecionar o nível de impacto para cada consequência do evento de risco acontecer, sem considerar os controles existentes, de acordo com os aspectos avaliativos da metodologia do MDR.

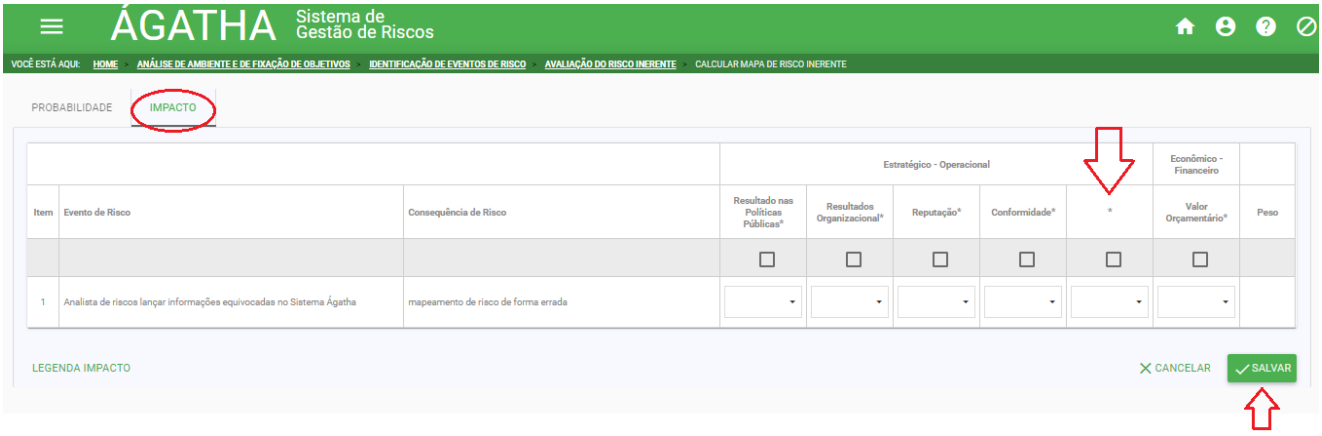


Figura 16 - Risco Inerente – Impacto

Nesta etapa, deverá ser selecionada a coluna em branco, conforme apontado na figura acima. Este fato se deve à adaptação da metodologia do extinto Ministério do Planejamento que possuía um critério de impacto a mais.

Para cada critério, deverá ser feita a análise de 1 a 5, conforme escala constante da tabela abaixo:

Impacto - Fatores para Análise						
	Estratégico-Operacional				Econômico-Financeiro	Peso
	Resultados nas Políticas Públicas Setoriais	Resultados Organizacionais (entregas estratégicas e PPA)	Conformidade / Regulação	Imagem / Reputação	Orçamentário / Financeiro	
	25%	20%	15%	10%	30%	100%
Orientações para atribuição de pesos	Impacto muito alto nas políticas públicas	Impacto muito alto nas metas estratégicas ou do PPA	Pode acarretar interrupção das atividades	Com destaque na mídia nacional e internacional, podendo atingir os objetivos estratégicos e a missão	> = 25%	5-Muito alto
	Impacto alto nas políticas públicas	Impacto alto nas metas estratégicas ou do PPA	Pode acarretar ações de caráter pecuniários (multas/dano ao erário)	Com algum destaque na mídia nacional, provocando exposição significativa	> = 10% < 25%	4-alto
	Impacto moderado nas políticas públicas	Impacto moderado nas metas estratégicas ou do PPA	Pode acarretar ações de caráter corretivo (determinação)	Pode chegar à mídia provocando a exposição por um curto período de tempo	> = 3% < 10%	3-Moderado
	Impacto baixo nas políticas públicas	Impacto baixo nas metas estratégicas ou do PPA	Pode acarretar ações de caráter orientativo (recomendação)	Tende a limitar-se às partes envolvidas	> = 1% < 3%	2-Baixo
	Pouco ou nenhum impacto	Pouco ou nenhum impacto nas metas estratégicas ou do PPA	Pouco ou nenhum impacto	Impacto apenas interno/sem impacto	< 1%	1-Muito baixo

Tabela 2 - Dados do Impacto

No contexto do aspecto avaliativo do “Valor Orçamentário”, o analista deverá analisar o impacto do evento de risco, considerando o orçamento anual do Ministério.

O mesmo procedimento deverá ser executado para cada evento de risco que estiver lançado e, após a inclusão das informações, clique em “SALVAR”.

É desejável que a consistência das percepções de probabilidade e impacto seja sustentada pelo registro de evidências, como dados, documentos, relatórios, documentos SEI, os quais poderão ser incluídos nos anexos da aba “ANÁLISE DE AMBIENTE E DE FIXAÇÃO DE OBJETIVOS”.

8.2 Avaliação dos controles existentes

Ainda na mesma aba “AVALIAÇÃO DE RISCOS E CONTROLES”, deve-se clicar na opção “AVALIAÇÃO DOS CONTROLES EXISTENTES” e na caneta  para alterar.

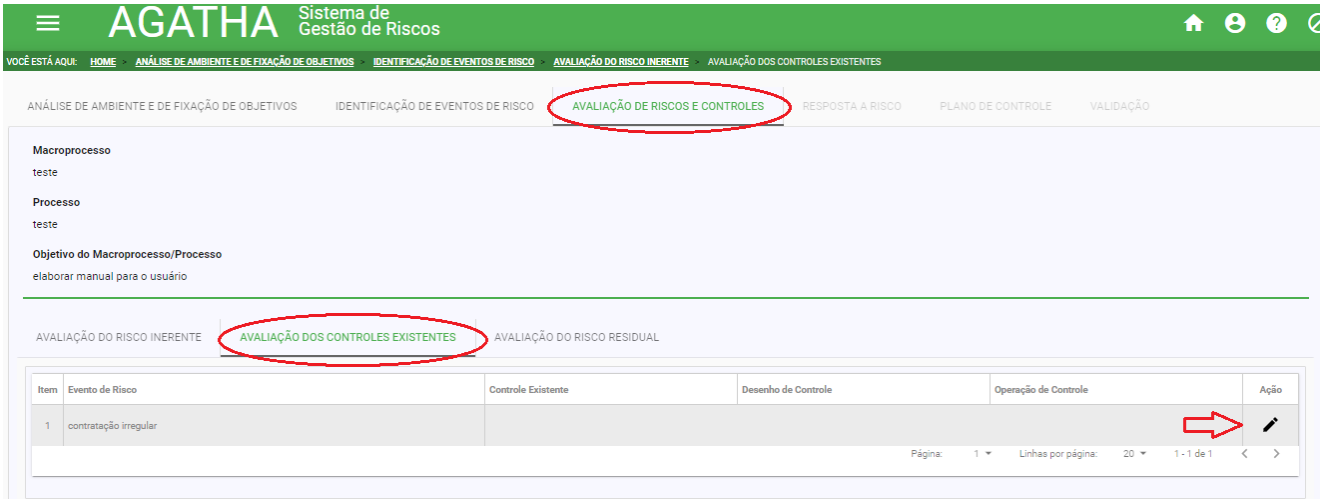


Figura 17 – Avaliação dos Controles Existentes

Para inserir o controle, deve-se clicar em +CONTROLE EXISTENTE, conforme figura abaixo:

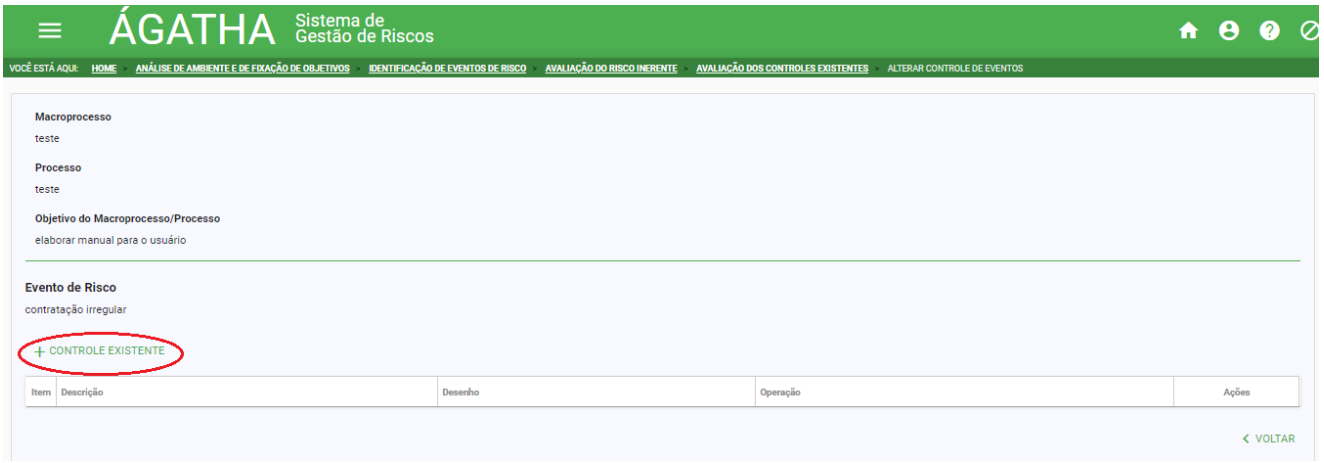


Figura 18 – Inserir Controles Existentes

Para cada evento de risco identificado, deve ser descrito o controle existente ou informar que não há controle no campo “Descrição”. Em seguida, deve-se selecionar as opções de acordo com o controle descrito, considerando a avaliação do desenho e da operação do controle. Por fim, clique no ícone ✓, da coluna Ações para salvar, conforme imagem a seguir.

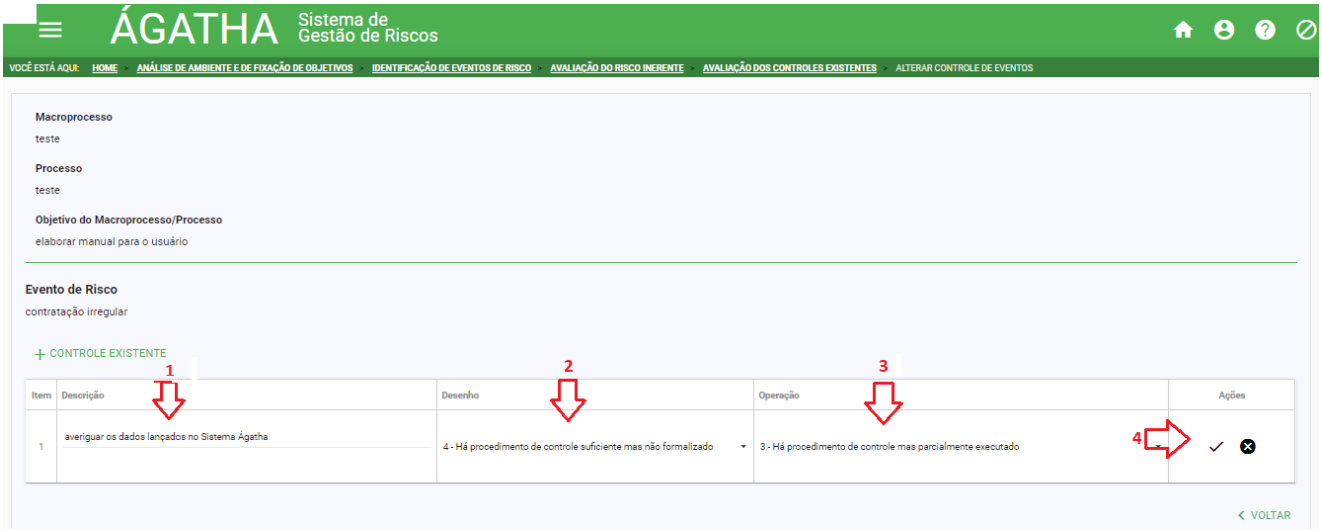


Figura 19 - Avaliação dos Controles Existentes

Caso haja necessidade de incluir mais de um controle, clicar na opção "+CONTROLE EXISTENTE" e proceder como descrito anteriormente.

8.3 Avaliação do Risco Residual

Na mesma aba "AVALIAÇÃO DE RISCOS E CONTROLES", clicar na opção "AVALIAÇÃO DO RISCO RESIDUAL".

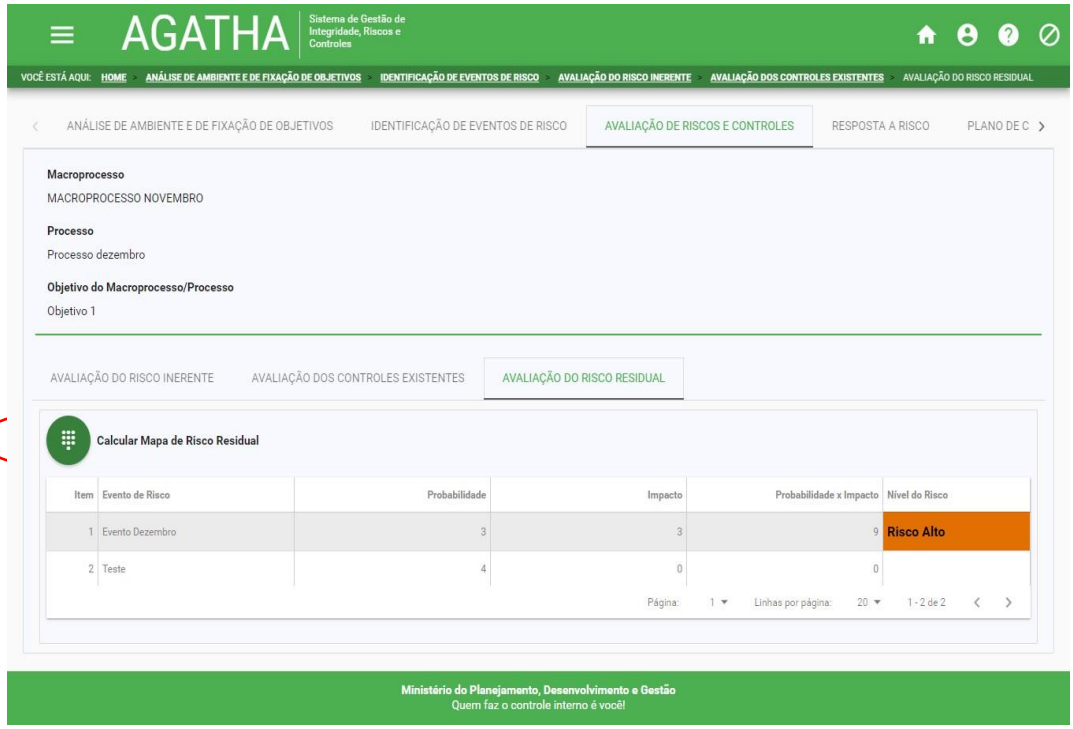


Figura 20 - Avaliação do Risco Residual

Após avaliar a eficácia dos controles existentes, deve-se aferir o nível de risco residual indicando os novos pesos relativos à probabilidade e ao impacto, levando-se sempre em consideração como os controles foram avaliados. Os controle preventivos são relacionados às causas (probabilidade) e os corretivos às consequências (impacto).

Qualquer dúvida, sugerimos consultar o Manual de Riscos, Controles Internos e Integridade.

8.3.1. Calcular Risco Residual – Probabilidade

Na aba "PROBABILIDADE", conforme figura abaixo, deve-se selecionar o nível de probabilidade da causa do evento de risco acontecer, considerando neste momento os controles existentes, de acordo com a possibilidade de ocorrência.

O mesmo procedimento deverá ser executado para cada evento de risco que estiver lançado. Após a inclusão das informações clicar em "SALVAR".

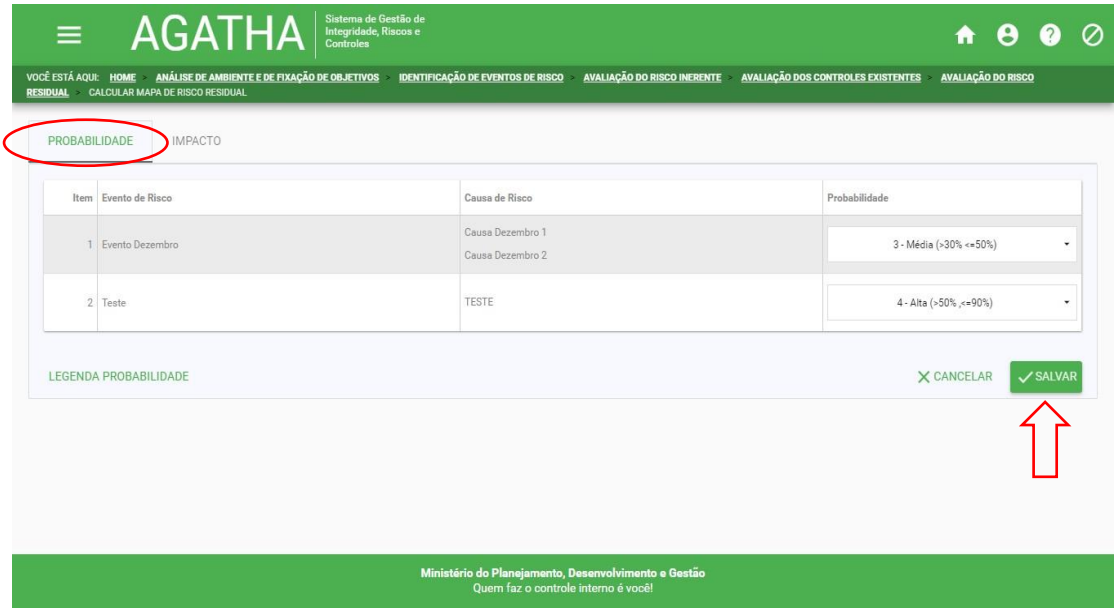


Figura 21 - Risco Residual – Probabilidade

8.3.2. Calcular risco residual – Impacto

Na aba "IMPACTO" selecionar o nível de impacto, considerando neste momento os controles existentes, de acordo com os aspectos avaliativos.

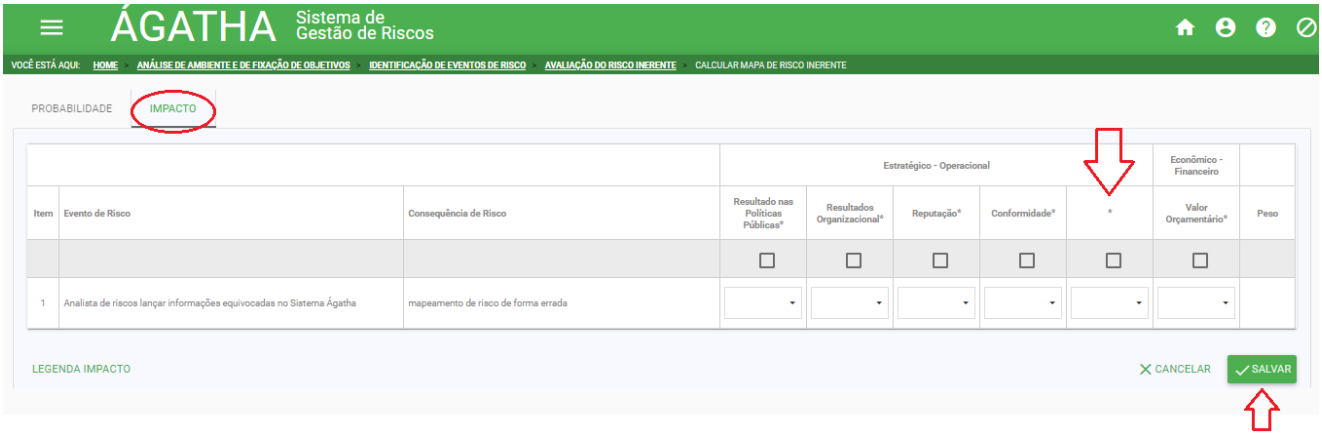


Figura 22 - Risco Residual – Impacto

Nesta etapa, deverá ser selecionada a coluna em branco, conforme apontado na figura acima. Este fato se deve à adapção da metodologia do extinto Ministério do Planejamento, conforme explicado na avaliação do impacto do risco inerente.

Para cada critério, deverá ser feita a análise de 1 a 5, conforme escala constante da tabela abaixo:

Impacto - Fatores para Análise						
	Estratégico-Operacional				Econômico-Financeiro	Peso
	Resultados nas Políticas Públicas Setoriais	Resultados Organizacionais (entregas estratégicas e PPA)	Conformidade / Regulação	Imagem / Reputação	Orçamentário / Financeiro	
	25%	20%	15%	10%	30%	100%
Orientações para atribuição de pesos	Impacto muito alto nas políticas públicas	Impacto muito alto nas metas estratégicas ou do PPA	Pode acarretar interrupção das atividades	Com destaque na mídia nacional e internacional, podendo atingir os objetivos estratégicos e a missão	> = 25%	5-Muito alto
	Impacto alto nas políticas públicas	Impacto alto nas metas estratégicas ou do PPA	Pode acarretar ações de caráter pecuniários (multas/dano ao erário)	Com algum destaque na mídia nacional, provocando exposição significativa	> = 10% < 25%	4-alto
	Impacto moderado nas políticas públicas	Impacto moderado nas metas estratégicas ou do PPA	Pode acarretar ações de caráter corretivo (determinação)	Pode chegar à mídia provocando a exposição por um curto período de tempo	> = 3% < 10%	3-Moderado
	Impacto baixo nas políticas públicas	Impacto baixo nas metas estratégicas ou do PPA	Pode acarretar ações de caráter orientativo (recomendação)	Tende a limitar-se às partes envolvidas	> = 1% < 3%	2-Baixo
	Pouco ou nenhum impacto	Pouco ou nenhum impacto nas metas estratégicas ou do PPA	Pouco ou nenhum impacto	Impacto apenas interno/sem impacto	< 1%	1-Muito baixo

Tabela 02 – Dados do Impacto

No contexto do aspecto avaliativo do “Valor Orçamentário”, o analista deverá analisar o impacto do evento de risco, considerando o orçamento anual do Ministério.

O mesmo procedimento deverá ser executado para cada evento de risco que estiver lançado. Após a inclusão das informações clicar em “SALVAR”.

Antes de prosseguir, pode-se validar os níveis dos riscos residuais, definidos pelos analistas dos riscos, com o gestor do processo que seria, no mínimo, o DAS/FCPE 4 da sua unidade. Ou, se a unidade preferir, os analistas poderão fazer todo o processo e o gestor fazer a validação apenas no final, conforme explicitado neste Manual. Alertando que, no Sistema, há apenas a opção de encaminhar para validação do gestor após o estabelecimento do(s) plano(s) de controle, então, se for decidido fazer essa validação também antes de definir esses planos e após o estabelecimento dos níveis dos riscos residuais, poderá ser feita por meio do SEI ou por e-mail.

9. Resposta a risco

Conhecido o nível do risco residual, verifique qual estratégia a ser adotada para responder ao evento de risco. A escolha da estratégia dependerá do nível de exposição a riscos previamente estabelecido em confronto com a avaliação que se fez do risco (matriz de riscos). No Manual de Gestão de Riscos, Controles Internos e Integridade, há detalhamento sobre essa matriz.

Clicar na aba “RESPOSTA A RISCO”. Os campos Macroprocesso, Processo, Objetivo do Macroprocesso/Processo e o Evento de Risco já deverão estar preenchidos. No campo “Nível de Risco” aparecerá o nível de risco residual que aquele evento apresenta. Clique no ícone “Ações”.

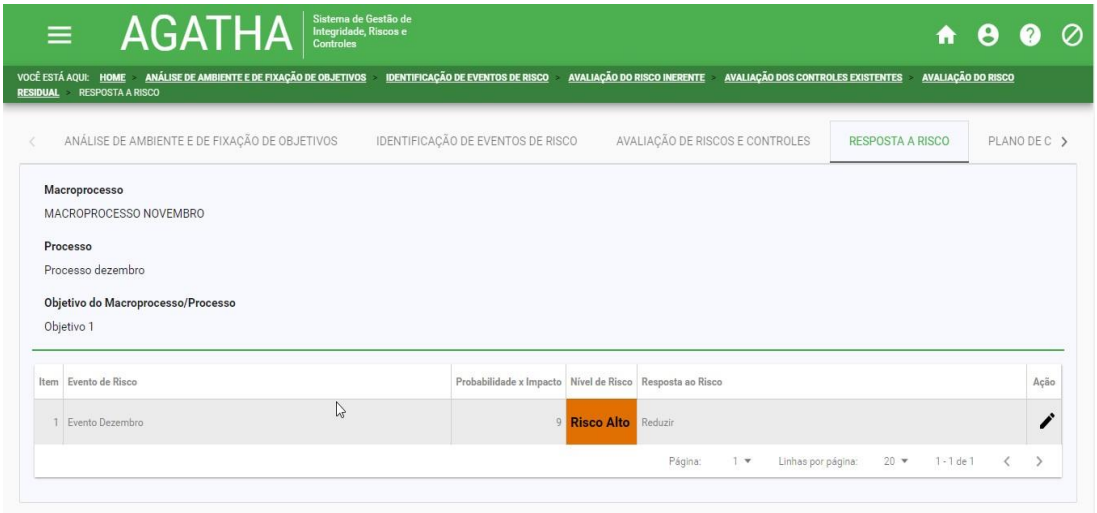


Figura 23 - Resposta a Risco

No campo Resposta ao Risco, deve-se selecionar a opção que indique qual a ação será tomada para representar a resposta para aquele evento de risco, dentre as opções possíveis. Na sequência, deve ser apresentada a justificativa para referenciar a resposta ao risco a ser adotada. Após a inclusão das informações clicar em “SALVAR”.

9.1 Alterar Resposta a Risco

Após essa etapa, o gestor do processo, que é, no mínimo DAS/FCPE 4, fará uma análise, podendo validar ou alterar a resposta a risco definida pelos analistas de risco, tanto para adotar uma ação em que poderia aceitar o risco e não adotar controle, como deixar de adotar uma ação em que deveria adotar uma ação de controle, tudo isso com apresentação de justificativa, conforme definido pela Política de Gestão de Riscos do MDR. Ou, se a unidade preferir, os anailtas poderão fazer todo o processo e o gestor validar apenas no final, conforme explicitado neste Manual.

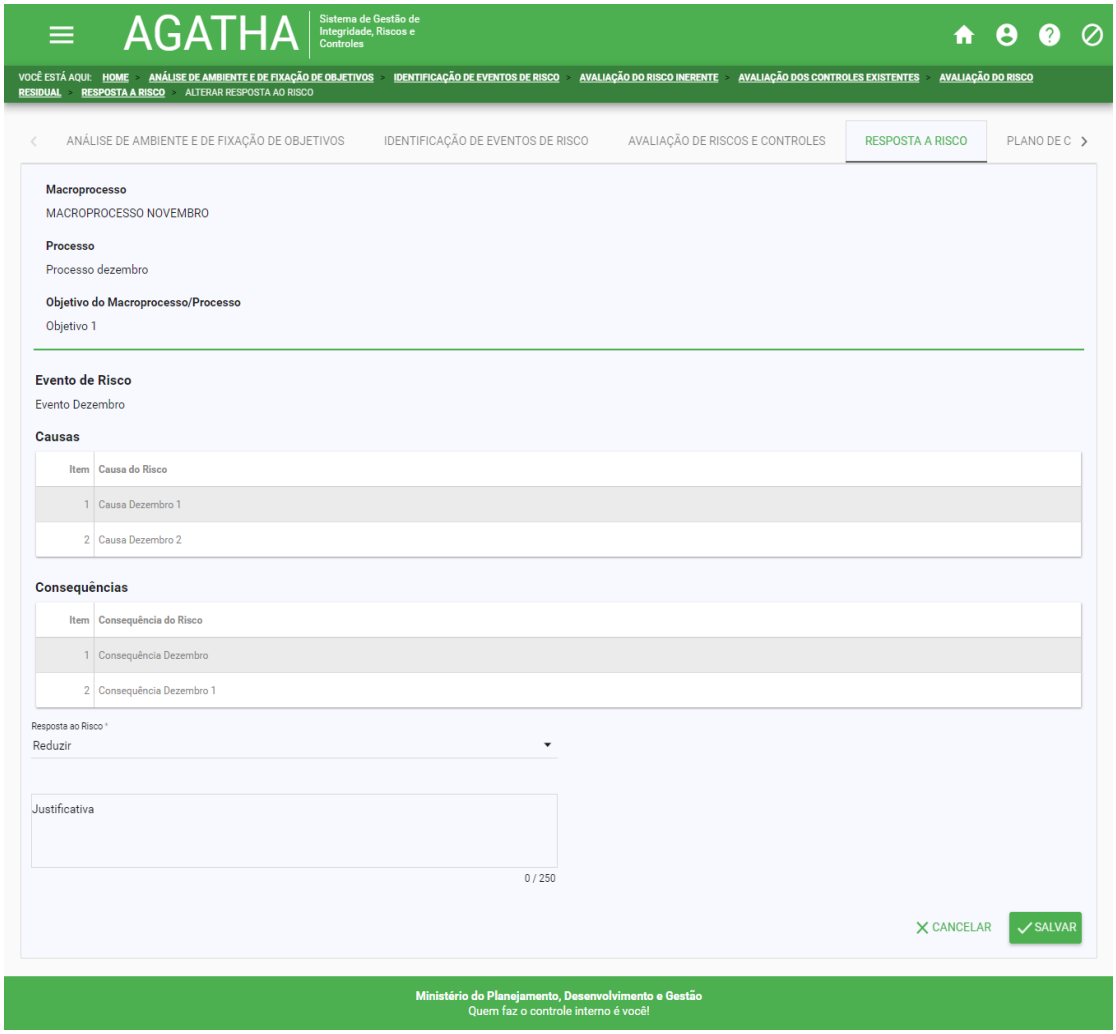


Figura 24 - Alterar Resposta a Risco

9.2 Plano de Controle

A próxima etapa é definir os planos de tratamento ou planos de controle. Para isso, basta clicar na aba “PLANO DE CONTROLE”. Os campos Macroprocesso, Processo, Objetivo do Macroprocesso/Processo e o Evento de Risco já deverão se apresentar preenchidos. No campo Nível de Risco aparecerá que tipo de nível de risco residual aquele evento apresenta. Em seguida, clicar no ícone “Ações”.

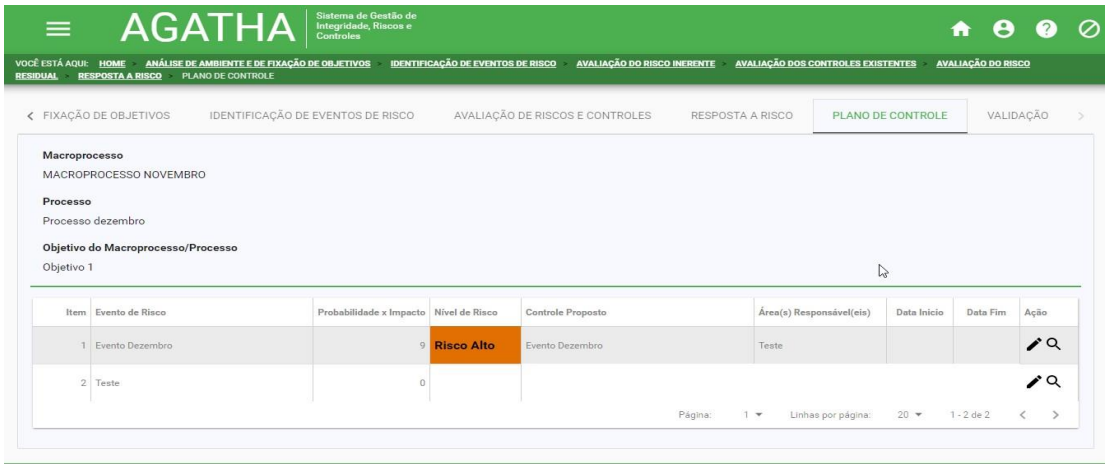


Figura 25 - Plano de Controle

Os analistas de risco deverão preencher o campo “Controle Proposto” com informações do tipo de controle que será aplicado para este evento de risco. Para os campos “Tipo de Controle” e Objetivo do Controle” deverá ser selecionado a opção que reflete o controle que deverá ser aplicado ao evento de risco. No Manual de Riscos, Controles Internos e Integridade, há as explicações sobre os tipos de controles.

É importante retomar as informações preenchidas na avaliação do controle, caso o controle seja existente. Então, por exemplo, se foi feita uma avaliação de que o controle não está formalizado, a proposta no plano pode ser a formalização. Ou, se ele não é comunicado, a proposição de ações de comunicação.

Na sequência, preencher os campos “Área responsável” e “Responsável” com os dados da área e do responsável pela efetivação da aplicação dos controles propostos. Recomenda-se incluir o cargo do responsável e não o nome, pois, se houver alteração, não terá impacto ou descontinuidade no desenvolvimento do plano.

Além disso, há o campo “Intervenientes”, em que é possível se estabelecer outras unidades que poderão auxiliar na elaboração e no cumprimento do plano. No entanto, sempre que se envolver outras unidades, antes deve

haver uma negociação com concordância e definição dos papéis. Se possível, essas definições poderão ser feitas ou por e-mail ou em um processo formal no SEI.

Também será necessário preencher o campo “Como será implementado”, com informações dos passos e procedimentos adotados para implantação do controle proposto. Deve-se tentar ser o mais claro possível, pois, depois da validação do processo, esses planos serão acompanhados pela Coordenação-Geral de Inteligência e Riscos da Assessoria Especial de Controle Interno e, também, poderão ser auditados pelos órgãos de controle interno e externo.

No tocante à data de início e à data prevista para conclusão, deve-se estimar todo o período de planejamento e execução do plano. Por exemplo, se o plano for para realizar uma capacitação, a data deverá ser de todo o processo e não somente a capacitação em si. Após a inclusão das informações, clicar em “SALVAR”.

Conforme mencionado anteriormente, o processo de Mapeamento de Risco desenvolvido pelos analistas de risco deverá ser encaminhado para validação do Gestor do Processo, que é, no mínimo ocupante de DAS ou FCPE 4, o qual foi informado nos dados iniciais da aba “ANÁLISE DE AMBIENTE E DE FIXAÇÃO DE OBJETIVOS”.

Para tanto, deverá selecionar a opção “Voltar” e em seguida a opção “Solicitar Validação” ao final da tela, conforme figura abaixo.

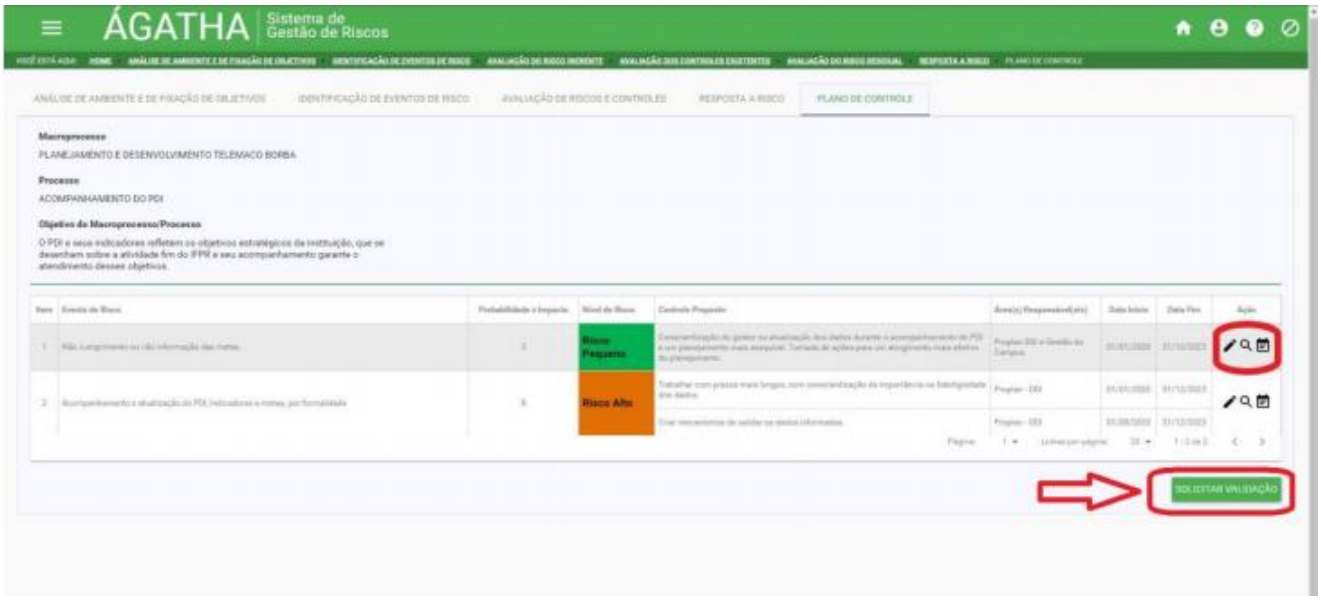


Figura 26 – Envio para validação

9.2.1. Acompanhamento do Plano de Controle

O analista de risco poderá realizar e registrar o acompanhamento das ações do controle propostas no “Plano de Controle”. Para isso, o analista de risco deverá clicar na opção “Ações de Acompanhamento”, conforme figura abaixo.

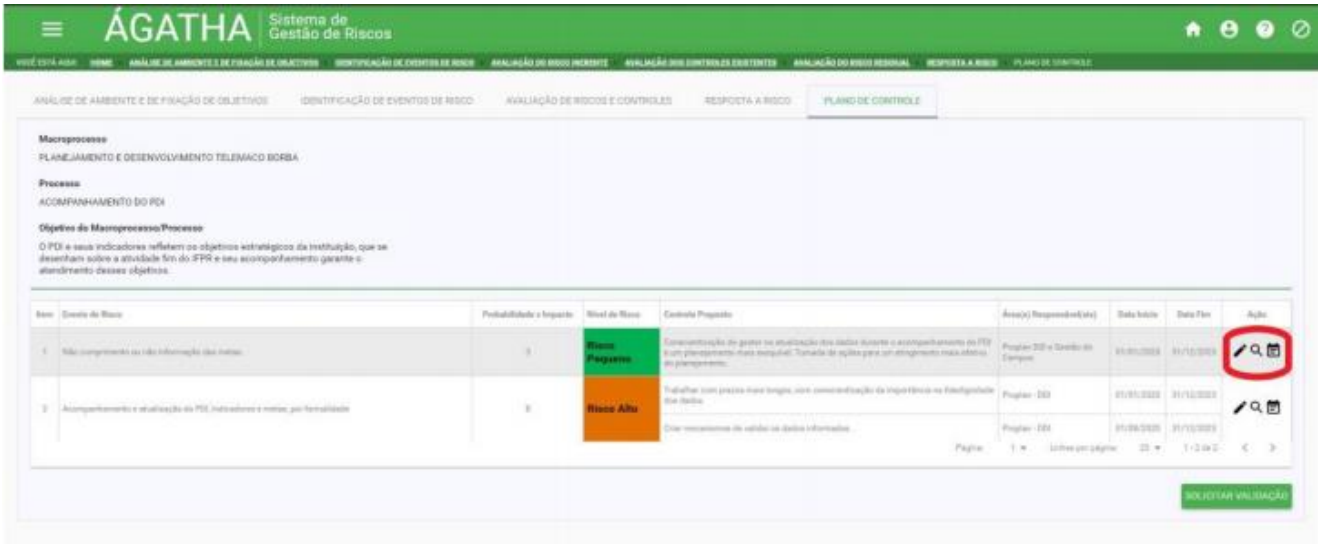


Figura 27 – Acompanhamento do Plano de Controle

Em seguida clicar na opção “+ Novo Acompanhamento”, conforme figura a seguir:

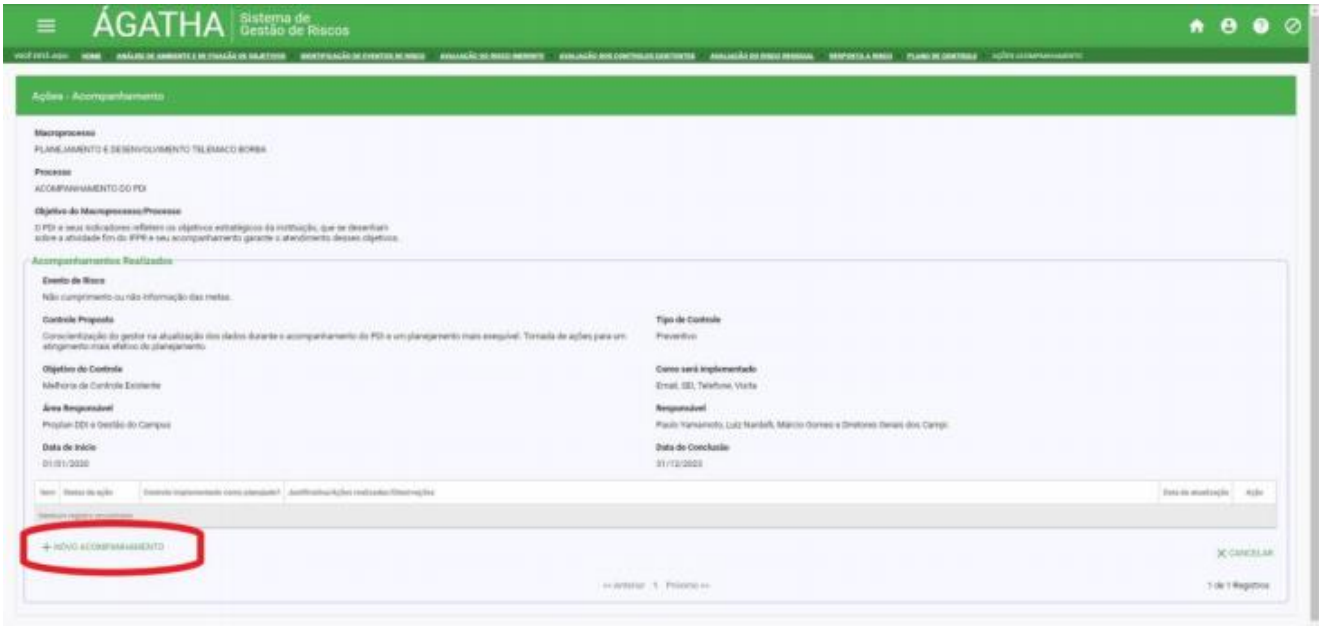


Figura 28 – Inserir novo Acompanhamento do Plano de Controle

Será apresentada uma tela em que será possível informar qual o “status” do Plano de Controle, se o controle está implantado conforme foi planejado, justificativa, ações e/ou observações a respeito da implantação.

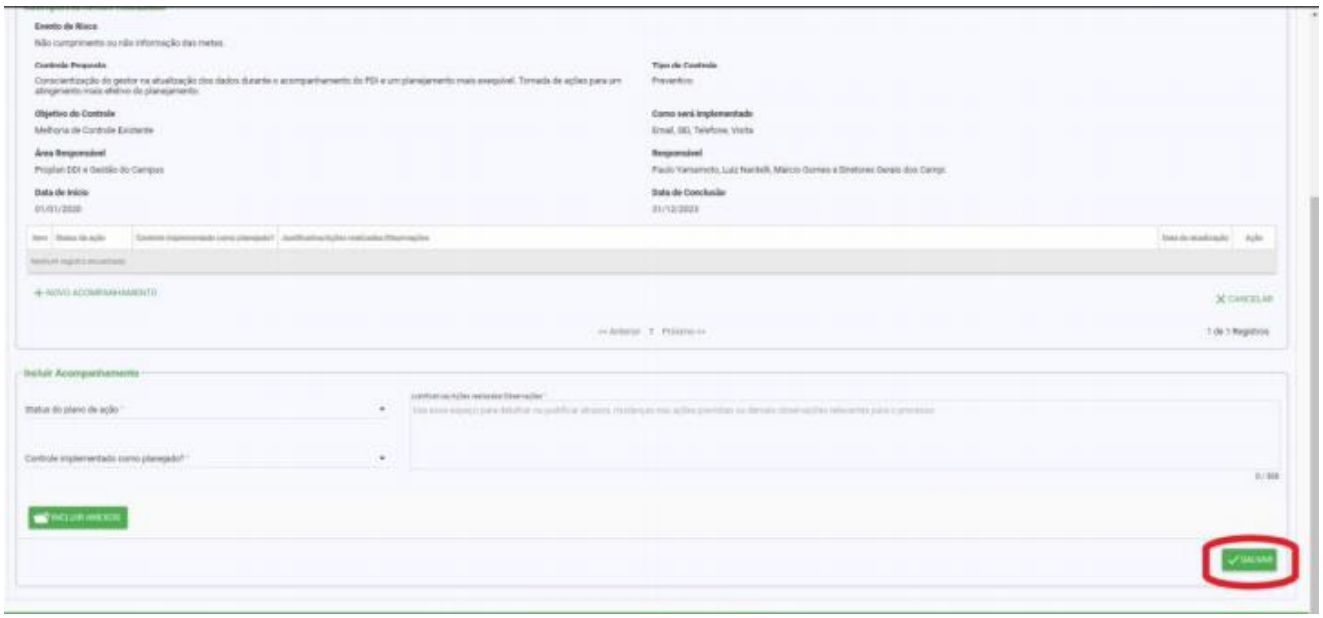


Figura 29 – Informações sobre o Acompanhamento do Plano de Controle

Se necessário, também é possível incluir documentos anexos com vistas à comprovação das ações realizadas. Após a conclusão, não esquecer de clicar em “Salvar”.

10. Validação

Para validação do Mapeamento de Risco, o Gestor do Processo deverá selecionar a opção “Processo” e em seguida a opção “Gerenciar” em Gerenciar Processo.

Na tela, serão apresentados os processos mapeados, seus status e as possibilidades de ações (visualizar, alterar ou gerar relatório). O Gestor de Processo poderá alterar qualquer etapa do mapeamento dos eventos de risco. Como destacado anteriormente, pode-se escolher validar apenas ao final do processo ou o gestor poderá, à medida que o processo for evoluindo, analisar e, se não concordar, alterar as informações. Saliente-se que todas as alterações ficarão registradas no Sistema.

Na fase de validação, o gestor de processo deve clicar no ícone “Alterar” na opção Ações, conforme figura abaixo, abrir a aba “VALIDAÇÃO” e selecionar o evento de risco a ser avaliado. Os campos Macroprocesso, Processo e Objetivo do Macroprocesso/Processo já deverão se apresentar preenchidos. No campo “Decisão” o Gestor do Processo deverá selecionar a opção de validar ou não o mapeamento do evento de risco realizado e “SALVAR”. Concluída a validação o mapeamento estará terminado e pronto para acompanhamento dos demais perfis.

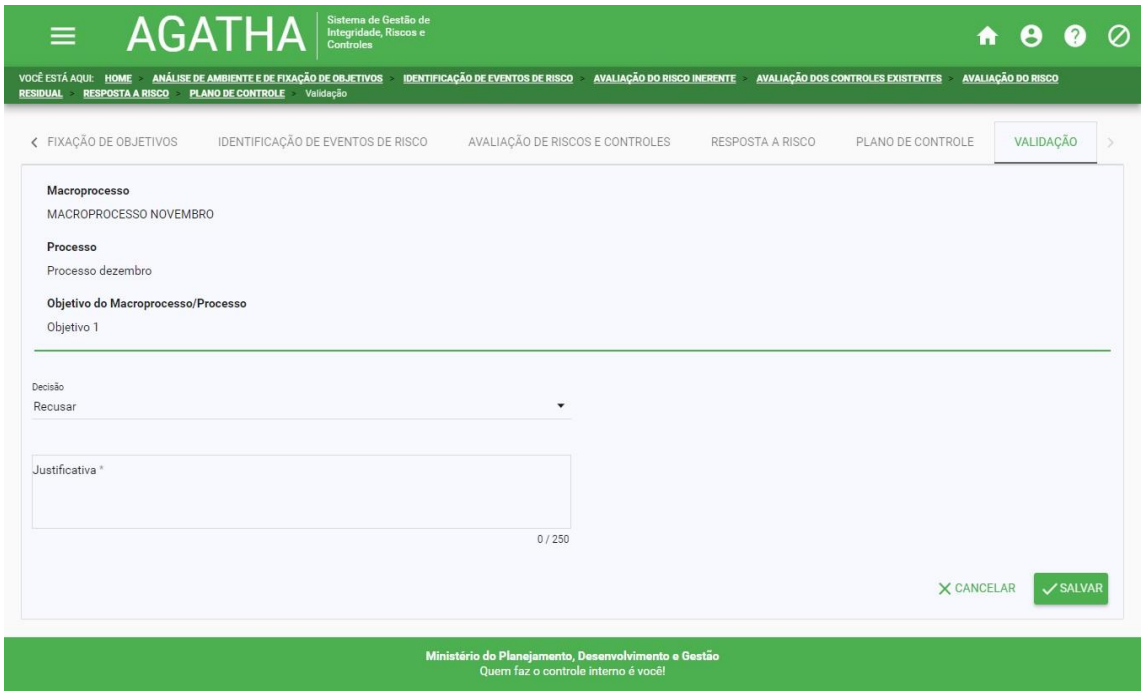


Figura 30 - Validação

11. Relatórios

Os perfis de GESTOR DO PROCESSO, NÚCLEO E COMITÊ poderão acompanhar o status, consultar ou emitir relatórios dos processos e eventos de riscos mapeados, bem como suas tratativas. Na opção “Processos”/“Relatórios” é apresentado um painel com as informações compactadas dos processos com os riscos mapeados e validados.

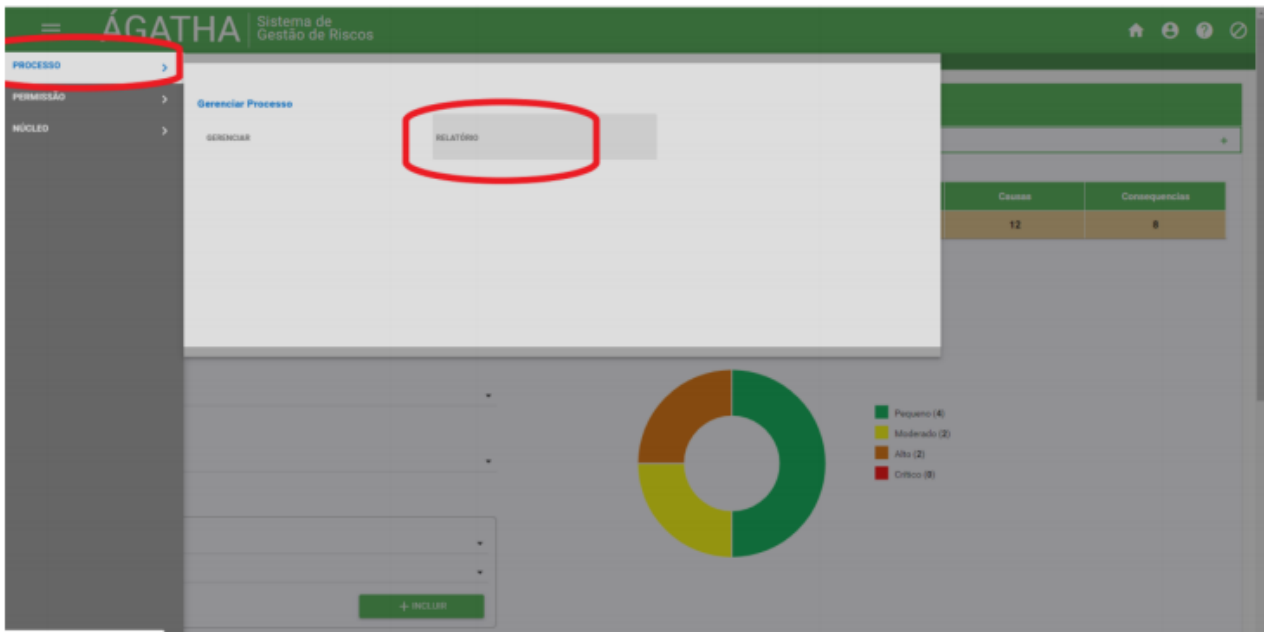


Figura 31 - Relatórios

A opção permite monitorar os indicadores e aplicar filtros de acordo com a necessidade. Na opção “Processos” / “Gerenciar” é possível visualizar o mapeamento de risco de um processo específico. Clique no ícone “Visualizar (lupa)” para visualizar e para emitir relatório basta clicar no ícone “Gerar Relatório do Processo”, ambos na opção Ações.

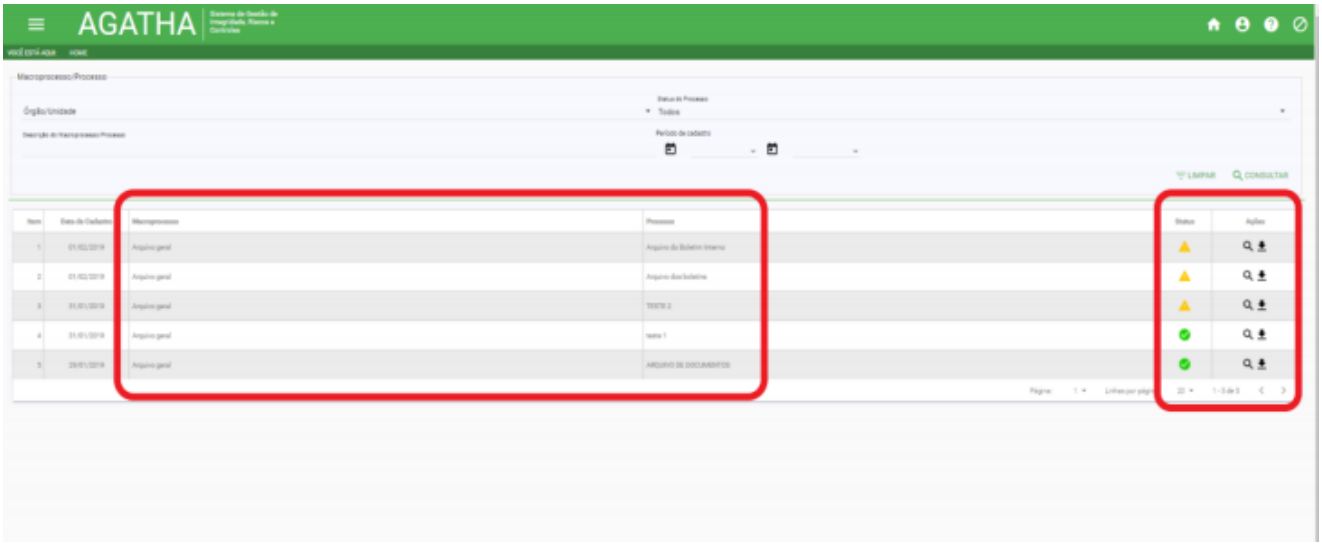


Figura 32 – Ações da tela de Relatórios

12. Conclusão

Portanto, o Sistema acompanha todas as fase de mapeamento dos riscos, incluisive de monitoramento dos controles. Espera-se que este Manual auxilie o usuário a executar todas as ações.

Qualquer dúvida durante o processo, entre em contato com a Coordenação-Geral de Inteligência e Riscos no e-mail aeci.riscos@mdr.gov.br ou no ramal 5700.