

Ministério da Fazenda

Comitê de Gestão de Riscos, Controle e Integridade – CGRCI

Assessoria Especial de Controle Interno – AECI



MANUAL DE GESTÃO DE RISCOS
DO MINISTÉRIO DA FAZENDA

3ª Ed. – Julho 2018

Anexo Único da Resolução CGRCI nº 5, de 25 jul. 2018.

Processo SEI 12100.101934/2018-56



Ministério da Fazenda

CGRCI

Ministro de Estado da Fazenda

Eduardo Refinetti Guardia

Secretária-Executiva

Ana Paula Vitali Janes Vescovi

Presidente do Comitê de Gestão de Riscos, Controle e Integridade

Chefe da Assessoria Especial de Controle Interno

Francisco Eduardo de Holanda Bessa

Elaboração

Thiago Mendes Rodrigues

Colaboração

Comitê de Gestão de Riscos, Controle e Integridade – **CGRCI**

Frente de Gestão de Riscos – **FGR**





PREFÁCIO

A Gestão de Riscos do Ministério da Fazenda é estruturada de forma integrada com base em governança envolvendo normas, instâncias, plataformas e áreas do Ministério. Nesse sentido, destacam-se:

- Comitê Estratégico de Governança – CEG¹ do Ministério da Fazenda, composto pelos titulares da Secretaria Executiva, PFGN, RFB, STN, SPE, SAIN, SEFEL, SEPRAC, SPREV, GMF, ESAF, CARF, COAF, CVM, SUSEP e PREVIC.
- Comitê de Gestão de Riscos, Controle e Integridade – CGRCI², composto por representantes de 24 órgãos e entidades do Ministério da Fazenda: AECI, CARF, COAF, CONFAZ, CRSFN, CRSNSP, CVM, ESAF, GMF, PGFN, PREVIC, RFB, SAIN, Secretaria Executiva, SEAE (SEFEL e SEPRAC), SPE, SPOA, SPREV, STN, SUSEP, Comissão de Ética, Corregedoria e Ouvidoria;
- Modelo de Relacionamento³ para a Gestão de Riscos do MF;
- Política de Gestão de Riscos⁴ do Ministério da Fazenda;
- Programa de Modernização Integrada do Ministério da Fazenda – PMIMF;
- Frente de Gestão de Riscos – FGR⁵ do PMIMF;
- Assessoria Especial de Controle Interno do Ministério da Fazenda – **AECI**; e
- Sistema de Gestão de Riscos e Integridade do Ministério da Fazenda – **GRIFA**.

¹ Cf. Portaria MF nº 267/2018. Cf. <goo.gl/qJKrug>.

² Cf. Resoluções CEG nº 5/2014 – cria o CGIRC; CEG nº 8/2017, Anexo VI – composição do CGRCI; e Resolução CGRCI nº 2/2017: aprova o Regimento Interno do CGRCI. Cf. <goo.gl/Yjk6EG> e <goo.gl/vFdyDT>.

³ Cf. Modelo de Relacionamento em Gestão de Riscos: Resolução CEG nº 9/2017, Anexo V. Cf. <goo.gl/1YxDsD>.

⁴ Cf. Política de Gestão de Riscos: Resolução CGRCI nº 3/2017. Cf. <goo.gl/vFdyDT>.

⁵ Cf. <goo.gl/2vps4H>.



Adicionalmente, ressalta-se a importância de normas como o Acórdão 1273/2015-TCU-Plenário⁶, a Instrução Normativa Conjunta MP/CGU nº 1/2016⁷, o Decreto Federal nº 9.203/2017⁸, e a Portaria CGU nº 1.089/2018⁹.

Nesse sentido, este Manual de Gestão de Riscos, atualizado¹⁰ em sua 3ª Edição, é um guia que apoia e complementa a governança quanto à Gestão de Riscos no Ministério da Fazenda de acordo com as melhores práticas, quanto a análise de contexto; identificação, mensuração e tratamento de riscos; monitoramento; e reporte de resultados.

Conforme dispõe a Política de Gestão de Riscos do Ministério da Fazenda, e em respeito às particularidades dos Órgãos e Entidades, o disposto neste Manual não é de observância obrigatória, mas alvo de gradual convergência:

*“Art. 12. Os Órgãos e Entidades **executarão suas políticas setoriais, normas e metodologias de gestão de riscos buscando gradual convergência** com os princípios, diretrizes e objetivos desta Resolução.”* Política de Gestão de Riscos do MF; grifo nosso.

Controle de Edições:

Manual	Editado em	Coordenador
1ª Edição	Nov. 2015	José Luiz de A. M. Filho
2ª Edição	Dez. 2016	José Luiz de A. M. Filho
3ª Edição	Jul. 2018	Thiago Mendes Rodrigues

⁶ Acórdão 1273/2015-TCU-Plenário, de 27 mai. 2015: recomendou e encaminhou a instâncias do Poder Público elementos de análise e avaliação de temas envolvendo controles internos, gestão de riscos e governanças na administração pública brasileira.

⁷ IN CGU 1, de 10 mai. 2016: dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo Federal.

⁸ Decreto 9.203, de 22 nov. 2017: dispõe sobre a política de governança da administração pública federal – APF direta, autárquica e fundacional.

⁹ Portaria CGU 1.089, de 25 abr. 2018: estabelece orientações a que os órgãos e as entidades da APF federal direta, autárquica e fundacional adotem procedimentos à estruturação, execução e monitoramento de seus programas de integridade e dá outras providências.

¹⁰ Com apoio do CGRCI, e colaboração dos servidores: Joao Batista Ribas de Moura, Alan Ribeiro Milagres, Cesar Almeida de Meneses Silva, Fábio Pinto Coelho, Verochile da Silva Júnior, David Menegon, Gustavo de Oliveira e Silva, Luiz Augusto Barbosa Mozzer, Waldeir Machado da Silva, Iamakaue de Almeida, Mathieu Francois Dunley Corbineau, Fabiano Alves de Oliveira, Eliane de Almeida e Silva Evangelista, e Priscila Gonçalves de Freitas.



SUMÁRIO

Prefácio	3
1 – Introdução.....	6
2 – Gestão de Riscos.....	7
2.1 – Modelo de Gestão de Riscos do Ministério da Fazenda.....	8
2.2 – Contexto	9
2.3 – Gestão de Riscos no Ministério da Fazenda	11
2.4 – Visão Geral dos Conceitos.....	13
3 – Modelo Conceitual do Gerenciamento de Riscos do MF	15
4 – Modelo Operacional do Gerenciamento de Riscos do MF	16
4.1 – Análise de Contexto	17
4.2 – Identificação de Risco	17
4.3 – Mensuração de Risco	18
4.3.1 – Avaliação de Riscos e Controles	19
4.3.1.1 – Controle quanto ao Desenho.....	19
4.3.1.2 – Controle quanto à Operação	20
4.3.2 – Matriz de Riscos	20
4.3.2.1 – Cálculo da Nota de Risco	20
4.4 – Tratamento de Risco	23
4.4.1 – Plano de Implementação de Controles	24
4.4.2 – Mapa de Risco	25
4.5 – Monitoramento e Reporte Gerencial	26
Referências	26
Anexos	27



1. INTRODUÇÃO

A Gestão de Riscos auxilia os órgãos na tomada de decisão, no alcance de seus objetivos, e a evitar que perigos e surpresas ocorram inadvertidamente. Deve ser tratada como componente essencial do sistema de gestão de todo órgão e entidade, e amplia a possibilidade do entendimento prévio de possíveis ameaças, bem como a constatação de fraquezas.

No Brasil a gestão de riscos tem sido considerada mais uma prática da governança corporativa, por força do legislador ou em função da maturidade da organização. A gestão de riscos tem se expandido a setores não-financeiros, inclusive a organizações públicas, como abordagem complementar e de apoio à governança.

No setor público, destaca-se a necessidade real de gerir riscos, evidenciada pela legislação federal e dos órgãos de controle, como o **Acórdão 1273/2015-TCU-Plenário**, de 27 mai. 2015; a **Instrução Normativa Conjunta MP/CGU nº 1/2016**, de 10 mai. 2016; o **Decreto Federal nº 9.203/2017**, de 22 nov. 2017; e a **Portaria CGU nº 1.089/2018**, de 25 abr. 2018.

No Ministério da Fazenda, já em 2002, o Tesouro Nacional – TN iniciou as atividades de Risco Operacional e, em 2006, foi criada área independente para tratar do tema, em cumprimento a uma recomendação do Tribunal de Contas da União - TCU. Em 2007, com a criação da Secretaria da Receita Federal do Brasil – RFB, a competência da gestão de riscos foi atribuída em seu regimento interno. Em 2013, foi instituída a Frente Gestão de Riscos – FGR, vinculada ao PMIMF. E em 2014 foi criado o atual Comitê de Gestão de Riscos, Controle e Integridade – CGRCI, instância de apoio à governança liderada pela Assessoria Especial de Controle Interno do Ministério da Fazenda – AEI, que deliberou e aprovou este manual.

Assim, este Manual é uma guia que auxilia na visão dos conceitos, técnicas e métodos buscando torná-los mais simples ao mapeamento de riscos dos processos de trabalho no dia a dia da unidade, até as decisões mais estratégicas do Ministério da Fazenda.



2. GESTÃO DE RISCOS

A gestão de riscos deve ser capaz de identificar os eventos de riscos em potencial, capazes de afetar a organização, permitir o gerenciamento dos riscos de modo compatível com o tamanho e complexidade da organização e, no caso do setor público, aumentar benefícios e reduzir o custo do valor a ser entregue à sociedade, protegendo os direitos públicos, criando condições à prosperidade econômica, melhorando a prestação dos serviços governamentais, entre outros.

*“O risco é uma precondição essencial para o desenvolvimento humano; se parássemos de assumir riscos, inovações técnicas e sociais necessárias para solucionar muitos dos problemas mundiais desapareceriam. De fato, muitos dos riscos existentes na sociedade moderna resultam de benefícios gerados por inovações sociais e tecnológicas. Por outro lado, a imprudência insensata também não é uma boa ideia. Em vez disso, **precisamos definir um caminho intermediário no qual o acaso – com suas incertezas e ambiguidades inerentes – seja levado em consideração de maneira objetiva, racional e eficiente.**”* Aaron Wildavsky¹¹ (1979, p. 32); grifo nosso.

A gestão de riscos pode ser aplicada a toda organização, em suas várias áreas e níveis, a qualquer momento, bem como a função, atividades e projetos específicos. A adoção de uma abordagem ativa, sistemática, holística e integrada permite gerenciar os riscos, modificando tanto a natureza de suas consequências como a probabilidade de que determinado efeito ocorra, por meio da identificação, compreensão, atuação objetiva e comunicação de questões que envolvam riscos.

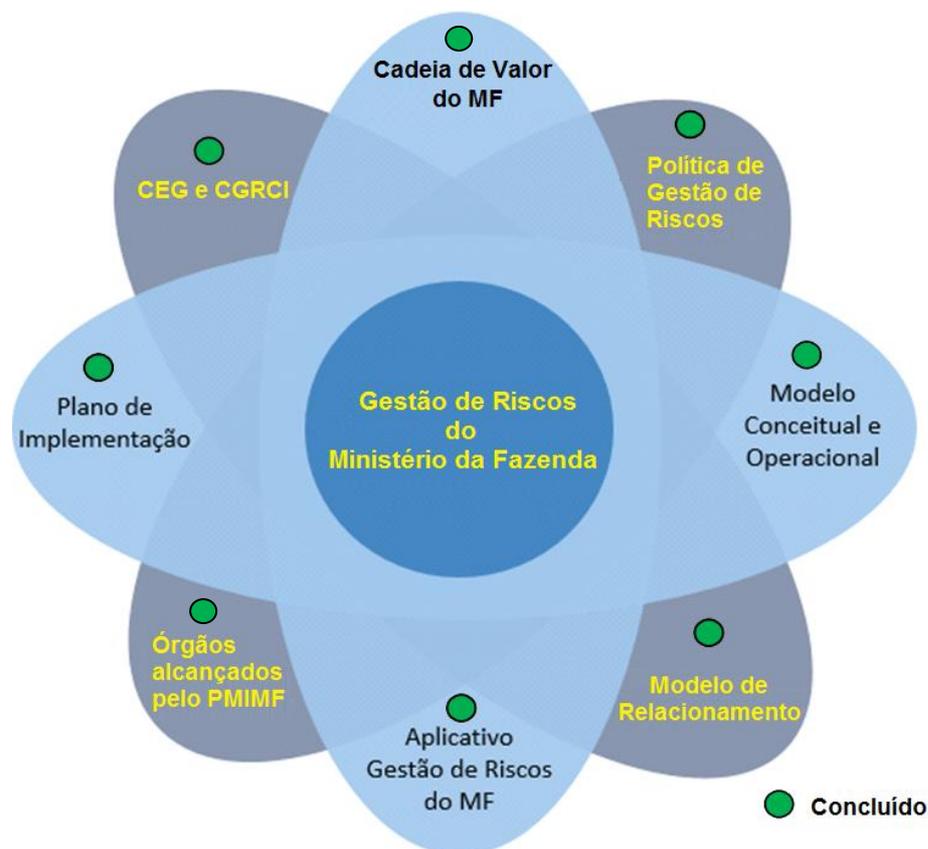
De acordo com ABNT ISO 31000/2018, são utilizadas as expressões “gestão de riscos” e “gerenciamento de riscos”. Em termos gerais, “gestão de riscos” refere-se à arquitetura (princípios, estrutura e processo) a gerenciar riscos eficazmente, enquanto que “gerenciar riscos” refere-se à aplicação dessa arquitetura aos riscos específicos.

¹¹ Cf. Wildavsky (1979, p. 32).



2.1 Modelo de Gestão de Riscos do Ministério da Fazenda

A visão geral do modelo organiza-se da seguinte maneira:



Relativamente à **visão estratégica**:

- O CEG e o CGRCI são órgãos colegiados que têm competências específicas, dentre outras, para elaborar, propor e aprovar política e metodologias relativas à Gestão de Riscos ao Ministério da Fazenda;
- A Política de Gestão de Riscos do Ministério da Fazenda¹² é a norma que estabelecem princípios, diretrizes e responsabilidades a serem observados no processo de gestão de riscos do MF;
- Os Órgãos alcançados pelo PMIMF referem-se às unidades que deverão observar os requisitos mínimos sugeridos à Gestão de Riscos no MF; e

¹² Política de Gestão de Riscos do Ministério da Fazenda: Resolução CGRCI nº 3/2017. Cf. <goo.gl/vFdyDT>.



- d. O Modelo de Relacionamento: descreve os atores e suas atribuições no processo de gestão de riscos integrada.

Quanto ao **gerenciamento riscos**:

- a. A Metodologia estabelece o regramento à identificação, mensuração, tratamento, monitoramento e reporte gerencial do gerenciamento de riscos do MF;
- b. O GRIFA é o aplicativo no âmbito do MF, e é a principal ferramenta eletrônica utilizada no gerenciamento de Risco e Integridade, conforme este Manual;
- c. A Cadeia de Valor Integrada do Ministério da Fazenda¹³: é o conjunto de atividades criadoras de valor, base para aplicação da metodologia;
- d. O Plano de Implementação é a rotina com cronograma de aprovação de normas e modelos previstos na Governança de Riscos do Ministério da Fazenda, bem como suas revisões. É rotina exercida no âmbito das atribuições do CGRCI, sob liderança da Assessoria Especial de Controle Interno – AECI.

2.2 Contexto

As organizações, sejam públicas ou privadas, devem entender quais são os riscos associados às suas decisões, operações, processos e atividades, no intuito de identificar e priorizar as falhas que devem ser corrigidas e, assim, implantar as melhorias necessárias tanto ao aprimoramento do sistema de gestão de riscos, e de ganhos de desempenho e produtividade.

A norma ISO 31000/2018 prevê um conjunto de princípios que devem ser atendidos na gestão eficaz dos riscos. O normativo recomenda que a Gestão de Riscos seja uma parte não separada do propósito organizacional, governança, liderança e comprometimento, estratégia, objetivos e operações.

¹³ Cadeia de Valor Integrada do Ministério da Fazenda. Cf. <goo.gl/mgkFra>.

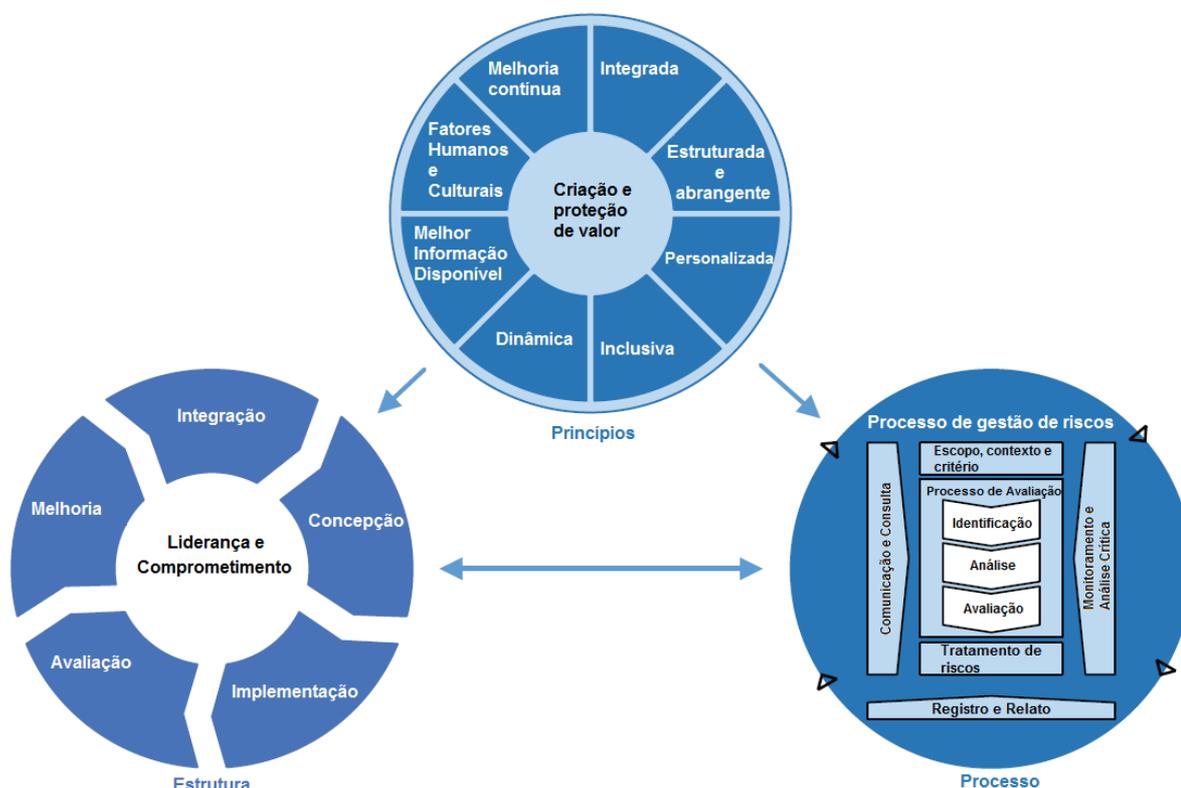


A ISO 31000/2018 apresenta **princípios e diretrizes** ao gerenciamento de qualquer tipo de risco, destacando que na concepção e implementação de planos de gestão de riscos é preciso considerar os contextos externo e interno da organização, como valores, cultura, estratégia, objetivos, políticas.

Assim, a referida norma menciona que para a gestão de riscos ser eficaz, convém que uma organização, em todos os níveis, atenda a três perspectivas: princípios, estrutura e processo.

A figura abaixo demonstra o relacionamento entre os princípios da gestão de riscos, estrutura e processo:

Figura – Princípios, Estrutura e Processos de Gestão de Riscos



Fonte: Princípios, Estrutura e Processo de Gestão de Riscos (ABNT, 2018).



- Na perspectiva princípios, o item 4, da ABNT ISO 31000/2018, estabelece que a Gestão de Riscos cria e protege valor, devendo ser (a) parte integrante de todas as atividades organizacionais; (b) estruturada e abrangente; (c) personalizada; (d) inclusiva; considerando (e) informações históricas e atuais; (f) fatores humanos e culturais; e (g) a melhoria contínua por meio do aprendizado e experiência;
- Na perspectiva estrutura, o item 5, da ABNT ISO 31000/2018, prevê que “a eficácia da gestão de riscos dependerá da sua integração na governança e em todas as atividades da organização, incluindo a tomada de decisão; e
- Na perspectiva processo, o item 6, da ABNT ISO 31000/2018, prevê que convém que o processo de gestão de riscos seja: parte integrante da gestão e da tomada de decisão; incorporado na estrutura, operações e processos da organização.

O modelo proposto neste Manual de Gestão de Riscos observa em parte os princípios, a estrutura e o processo divulgados na norma ISO 31000, por serem menos complexos e mais adequáveis ao contexto do Ministério da Fazenda.

2.3. Gestão de Riscos no Ministério da Fazenda

A norma NBR ISO 31000/2018 recomenda que o comprometimento contínuo com a atividade de gestão de riscos deve ser demonstrado pela organização através de um documento apropriado

Assim, a Gestão de Riscos no Ministério da Fazenda é amparada pela **Política de Gestão de Riscos** do MF¹⁴, pelo **Modelo de Relacionamento**¹⁵, e pelo **Comitê de Gestão de Riscos, Controle e Integridade – CGRCI**.

¹⁴ Resolução CGRCI nº 3/2017: Dispõe sobre a Política de Gestão de Riscos do MF. Cf. <goo.gl/vFdyDT>.

¹⁵ Modelo de Relacionamento para a Gestão de Riscos do Ministério da Fazenda: Resolução CEG nº 9/2017, Anexo V. Cf. <goo.gl/1YxDsD>.



Ministério da Fazenda

CGRCI

Complementarmente, no sentido de atender à IN MP/CGU nº 01/2016, o Regimento Interno do CGRCI (Resolução CGRCI nº 02/2017) define:

“Art. 3º O CGRCI cumpre, no âmbito do Ministério da Fazenda, as funções do comitê previsto pelo art. 23 da Instrução Normativa Conjunta MP/CGU nº 01, de 10 de maio de 2016, que dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo Federal.”

A Política de Gestão de Riscos, por sua vez, estabelece:

“Art. 3º A gestão de riscos deverá alinhar-se:

I - ao planejamento estratégico e à cadeia de valor institucionalizados no âmbito do Programa de Modernização Integrada do Ministério da Fazenda (PMIMF) e dos Órgãos e Entidades;

II - às competências e às atribuições regimentais dos Órgãos e Entidades; e

III - aos modelos de governança corporativa e de gestão institucionalizados no âmbito do PMIMF e dos Órgãos e Entidades.”

O Modelo de Relacionamento, por fim, disciplina o fluxo de informações entre as diversas instâncias e agentes do Ministério da Fazenda.



2.4 Visão Geral dos Conceitos

A seguir são descritos alguns conceitos de termos adotados neste Manual de Gestão de Riscos. Dos termos adotados, alguns são consagrados na literatura relativa à gestão de riscos e outros constam das normas específicas do Ministério da Fazenda.

- **Risco:** efeito da incerteza sobre os objetivos declarados na Cadeia de Valor Integrada do Ministério da Fazenda – CVIMF;
- **Gestão de Riscos:** conjunto de princípios, estruturas, processos e atividades coordenados a dirigir e controlar uma organização no que se refere aos riscos;
- **Processo de Gerenciamento de Riscos:** aplicação sistemática de políticas, procedimentos e práticas de gestão para as atividades de comunicação, consulta, estabelecimento do contexto, identificação, análise, avaliação, tratamento e monitoramento;
- **Estrutura de Gestão de Riscos:** conjunto de componentes que fornecem os fundamentos, metodologias e arranjos organizacionais para a gestão de riscos;
- **Gestor do Risco:** agente que tem a responsabilidade e a autoridade para gerenciar determinado risco;
- **Evento de Risco:** é a materialização do risco que gera algum impacto para a organização.;
- **Risco Inerente:** risco do negócio em si que precede a adoção de controles;
- **Risco Residual:** risco remanescente após a adoção de controles;
- **Tipos de Controles:** controle preventivo e controle corretivo;
- **Controle Preventivo:** são os controles implantados, previstos ou propostos; têm a função de diminuir o nível de risco atuando na redução da probabilidade de ocorrência do risco;
- **Controle Corretivo:** são os procedimentos de acompanhamento implantados, previstos ou propostos; têm a função de possibilitar a diminuição do nível de risco atuando na redução do impacto provocado pela ocorrência do risco;



- **Natureza dos Controles:** controle manual ou automatizado;
- **Controle Manual:** são controles realizados por pessoas cujas regras não estão em um dispositivo ou sistema;
- **Controle Automatizado:** são controles com regras em dispositivo ou sistema;
- **Valor:** valor declarado na CVIMF a ser entregue à sociedade;
- **Cadeia de Valor Integrada Ministério da Fazenda:** modelo de gestão que pretende estimular algumas sugestões e reflexões de iniciativas de uso da cadeia de valor a que a orientação por processos com foco em resultados seja internalizada na organização;
- **Foco da Análise:** direcionador da análise dos processos dentro de um conjunto de valores definidos para a CVIMF;
- **Dimensão:** agrupamento de alto nível de abstração, que abriga um conjunto de tipos de riscos semelhantes, mas de forma geral;
- **Dimensão Funcional:** o foco da análise são os processos organizacionais associados à geração de valor;
- **Dimensão Econômica:** o foco da análise são as transações financeiras (captação, tributos, orçamento, fluxo de pagamento);
- **Dimensão Estratégica:** o foco da análise são os Projetos Estratégicos Corporativos – PEC e os Objetivos Estratégicos;
- **Tipo de Risco:** um grupamento de fatores de riscos semelhantes, segundo um ou mais critérios, que facilita o entendimento da natureza dos riscos;
- **Fator de Risco:** categorização de riscos mais específica que permite classificar os riscos por temas bem peculiares; e
- **Risco à Integridade:** Efeito da incerteza relacionado a corrupção, fraudes, irregularidades ou desvios éticos e de conduta, que possa comprometer os valores e padrões preconizados pela Instituição e a realização de seus objetivos – Anexo A.



3. Modelo Conceitual do Gerenciamento de Riscos do Ministério da Fazenda

O Modelo Conceitual de Gerenciamento de Riscos foi desenvolvido considerando o foco da análise nas três Dimensões: Funcional, Estratégica e Econômica, detalhadas no Anexo B, e a seguir:





4. Modelo Operacional do Gerenciamento de Riscos do Ministério da Fazenda

O objetivo deste capítulo é fornecer a visão do ciclo do gerenciamento de riscos desenvolvido ao Ministério da Fazenda, bem como contribuir à uniformidade de procedimentos na execução dos trabalhos de mapeamento de riscos nos diversos órgãos, entidades e agentes alcançados pela Governança de Riscos – Política de Gestão de Riscos, Modelo de Relacionamento.

A aplicação do modelo de gerenciamento de riscos tem por base os processos da Cadeia de Valor Integrada do MF. Assim, os processos priorizados serão submetidos ao ciclo de gerenciamento de riscos.

O ciclo foi programado para ser realizado em seis etapas, conforme figura abaixo:





A seguir, estão detalhadas as finalidades de cada etapa do ciclo de gerenciamento de riscos, sugestões de técnicas a serem utilizadas e o sistema operativo específico:

- Sistema de Gestão de Riscos e Integridade do Ministério da Fazenda – [GRIFA](#).

4.1 Análise de Contexto

A iniciar o mapeamento de riscos é desejável que o processo esteja mapeado. Nesse caso, as informações do mapeamento serão utilizadas. Aos casos em que o processo não esteja mapeado, deverá ser realizada a etapa Análise de Contexto, desenvolvida com o objetivo de auxiliar na priorização dos processos que serão objeto da aplicação da metodologia, contribuindo assim ao entendimento e ao o mapeamento de riscos do processo.

Assim, a Análise de Contexto é desenvolvida para registrar as informações coletadas sobre o processo, e seus aspectos afetos, internos e externos, uma vez que as informações obtidas sobre o ambiente, além de contribuir ao entendimento do processo, ajudarão na identificação das fraquezas e riscos, e na escolha das ações para mitigá-los.

Ressalta-se que esta etapa não é obrigatória nos casos em que os processos estiverem mapeados, mas é fundamental aos processos sem mapeamento. O [GRIFA](#) possui aba Análise de Contexto e o seu preenchimento não é condição necessária a passar à etapa seguinte.

4.2 Identificação de Risco

Esta etapa tem por finalidade identificar e registrar os riscos relevantes que comprometem o alcance do objetivo do processo e que afetem a entrega do valor à sociedade, registrado na Cadeia de Valor Integrada do MF.

A auxiliar na condução desta etapa foram elaboradas algumas perguntas, aqui chamadas de “perguntas orientadoras” – Anexo C. Na elaboração dessas perguntas foram considerados os termos e as definições do modelo conceitual



adotado pelo Frente Gestão de Riscos do MF. As perguntas orientadoras estão dispostas na mesma sequência dos termos e definições contidos no modelo conceitual, ou seja, por dimensão, tipo, fatores e subfatores de riscos e ajudarão o gestor ou os especialistas a refletirem sobre os possíveis riscos que podem comprometer o alcance do objetivo do processo em análise e, conseqüentemente, a entrega do valor.

Dessa forma, aplicando-se a técnica Entrevista com Especialistas ou outra mais apropriada para o processo em análise, faz-se as perguntas de forma a identificar os possíveis riscos que afetem a entrega do valor.

Visando ajudar no momento da identificação dos riscos, elaborou-se uma lista¹⁶ de prováveis riscos, considerando os termos e as definições contidos no modelo conceitual, em Anexo D - Taxonomia.

4.3 Mensuração de Risco

Uma vez identificados e registrados, faz-se necessário analisar os riscos sem levar em conta os controles porventura existentes. O processo de compreender a natureza dos riscos fornece base à sua avaliação e às decisões sobre o tratamento.

Em seguida, é importante que se identifiquem os controles existentes e que se faça a verificação de sua qualidade quanto ao desenho e à sua aplicação.

A realização desta etapa tem por finalidade mensurar os riscos identificados, incluindo o levantamento das causas, a existência de controles e, ainda, obter o **nível do risco (probabilidade x impacto)**.

Assim, a cada risco deverá ser identificadas e registradas as possíveis causas e os controles existentes. Em seguida, a cada controle identificado, deverá ser informado se trata de controle preventivo ou corretivo. Esses registros auxiliarão na avaliação dos riscos e dos controles bem como na mensuração do risco, obtendo-se o risco residual e a **Nota de Risco**.

¹⁶ Esta lista não esgota os possíveis riscos, tendo a finalidade de contribuir com a padronização na descrição dos riscos identificados.



Temos que a causa do risco é o fato gerador que motiva a possibilidade da ocorrência do risco e que o controle são procedimentos ou atividades que visam mitigar a possibilidade da ocorrência do risco. O controle reduz o risco inerente. Assim, são exemplos de atividades de controles: aprovações, conferências, autorizações, verificações, validações, conciliações, monitoramento, travas em sistemas, segregação de funções, dentre outras.

Ressalta-se que poderão existir mais de uma causa e mais de um controle relacionado a um mesmo risco. Nesse caso descrever o que for relevante para a análise do risco identificado e, conseqüentemente, para o processo.

4.3.1 Avaliação de Riscos e Controles

Posteriormente, com as causas e os controles listados, é possível que seja aplicado um questionário à verificação da qualidade dos controles. O resultado dessa verificação é importante pelo viés de auditoria mas, pela especificidade, não é obrigatório no Modelo de Gestão de Riscos.

Ressalta-se que a avaliação da eficácia do controle cabe à Auditoria Interna. No mapeamento de riscos a verificação da qualidade do desenho e da aplicação do controle tem a finalidade de subsidiar a mensuração do risco, no momento em que está sendo analisado (risco residual).

4.3.1.1 Controle quanto ao Desenho

Perspectivas do **Desenho do Controle**: o Controle não é sistematizado; Há procedimento de controle para algumas atividades, porém informais; Controles não foram planejados formalmente, mas são executados de acordo com a experiência dos servidores; É desenhado um sistema de controle integrado adequadamente planejado, discutido e documentado. O sistema de controle vigente é eficaz, mas não prevê revisões periódicas; e sistema de controle é eficaz na gestão de riscos. Foi adequadamente planejado, discutido, testado e documentado com correções ou aperfeiçoamentos planejados de forma tempestiva.



4.3.1.2 Controle quanto à operação

Perspectivas da Operação do Controle: Controle não executado; Controle parcialmente executado e com deficiências; Controle parcialmente executado; Controle implantado e executado de maneira periódica e quase sempre uniforme. Avaliação dos controles é feita com alguma periodicidade; e Controle implantado e executado de maneira uniforme pela equipe e na frequência desejada. Periodicamente os controles são testados e aperfeiçoados.

4.3.2 Matriz de Riscos

4.3.2.1 Cálculo da Nota de Risco

Para auxiliar o gestor na tomada de decisão com base nos resultados da análise dos riscos e definir quais riscos são objeto de tratamento e prioridade para a implementação de ações foi criada a **Nota de Risco**, um vetor que considera o nível de risco (aplicação da Matriz de Risco), o volume de ocorrências e a frequência de execução do processo:

Composição do vetor da Nota de Risco do Ministério da Fazenda

Nota de Risco

Nível de Risco (1º componente do vetor) – severidade resultante da avaliação de **Probabilidade x Impacto** de risco identificado.

Assume **A, B, C**.

Volume de Ocorrências (2º componente do vetor) – avaliação subjetiva do número de ocorrências de um risco no período avaliado (pode ser “um ano”).

Assume: “**a**” (baixo); “**b**” (médio); e “**c**” (alto).

Execução do Processo (3º componente do vetor) – representa a frequência de execução do processo avaliado.

Assume: “**++**” (baixa); “**+**” (média); e “**-**” (alta).



Cada risco avaliado, considerando a apreciação das causas e a qualidade do desenho e da operação do controle, é submetido à **Matriz de Risco** (probabilidade x impacto), afim de definir seu **Nível de Risco**. Nessa etapa, indica-se observar a atuação do controle existente, se é preventivo ou corretivo, fator preponderante na atribuição da probabilidade e do impacto.

Assim, obtém-se o 1º componente da **Nota de Risco** com a aplicação da **Matriz de Riscos**. Já a agregação do 2º e do 3º componente é realizada a partir das informações registradas no sistema quanto ao volume de ocorrências e a frequência de execução do processo.

A **Matriz de Riscos** considera as seguintes possibilidades:

Probabilidade	
RARA	Pode ocorrer em circunstâncias excepcionais
POUCO PROVÁVEL	Pequena possibilidade de ocorrer
PROVÁVEL	Provável que ocorra em várias circunstâncias
ALTA	Deve ocorrer em algum momento
Impacto	
GRANDE	Pode comprometer o alcance total do objetivo do processo
MODERADO	Pode comprometer o alcance de parte relevante do objetivo do processo
PEQUENO	Pode comprometer o alcance de parte não relevante do objetivo do processo
INSIGNIFICANTE	Poderá comprometer de forma insignificante o objetivo do processo



Probabilidade		RARA	POUCO PROVÁVEL	PROVÁVEL	ALTA
Impacto		2	3	4	5
GRANDE	6	12	18	24	30
MODERADO	4	8	12	16	20
PEQUENO	3	6	9	12	15
INSIGNIFICANTE	2	4	6	8	10

Nível de Risco		
A	De 4 a 9	Baixo
B	De 10 a 16	Médio
C	De 18 a 30	Alto

O volume de ocorrências poderá ser obtido por meio de dados históricos, se houver, e/ou com conhecimento do gestor, e a frequência de execução do processo poderá ser obtida com os dados do mapeamento e/ou com o conhecimento dos responsáveis pela execução do processo.

Desta forma, primeiro aplica-se a Matriz de Risco para se obter o nível de risco: **A**, **B** ou **C** (1º componente da Nota), em seguida identifica-se o Volume de Ocorrências: **a**, **b** ou **c** (2º componente da Nota) e, por fim, as informações sobre a frequência de execução do processo: “++”, “+” ou “-” (3º componente da Nota), chegando-se a **Nota de Risco**, instrumento que auxilia o gestor na tomada de decisão quanto ao tratamento a ser dado ao risco identificado, conforme Anexo E.

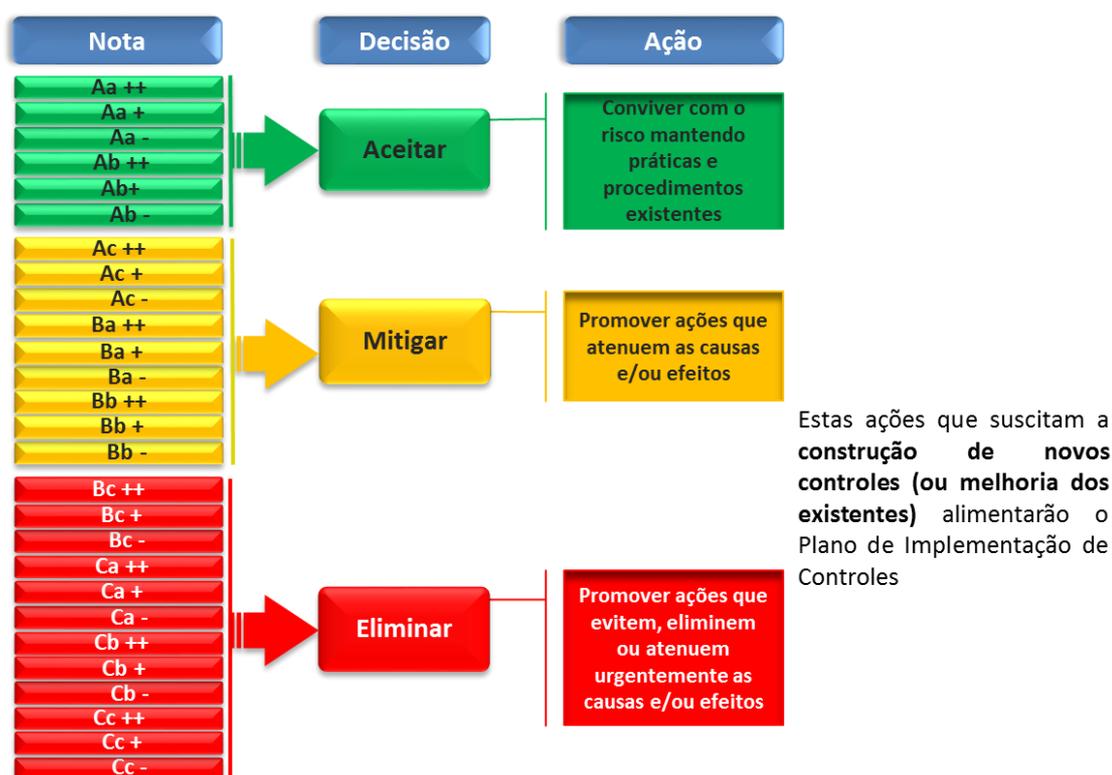


4.4. Tratamento de Risco

Segundo o item 6.5 da ABNT NBR ISO 31000/2018, o tratamento de riscos é o processo para modificar o risco, e pode envolver:

- evitar o risco ao decidir não iniciar, ou descontinuar a atividade que lhe origina;
- assumir ou aumentar o risco;
- remover a fonte de risco;
- mudar a probabilidade;
- mudar a consequência;
- compartilhar o risco; e
- reter o risco por decisão fundamentada.

O modelo desenvolvido pela Frente de Gestão de Riscos sugere três ações (**Aceitar**, **Mitigar** e **Eliminar**) a responder aos riscos, em função da **Nota de Risco** obtida. Essa decisão é discricionária a cada Órgão e Entidade. Abaixo, ilustra-se um exemplo de como essas decisões de Tratamento de Risco podem ser tomadas:





4.4.1 Plano de Implementação de Controles

Após identificados e mensurados, deve-se definir o tratamento a ser dado aos riscos. De acordo com o item 6.5.1 da ABNT NBR ISO 31000/2018, o tratamento de riscos envolve a seleção de uma ou mais opções a modificar os riscos.

As opções previstas no Modelo de Gerenciamento de Riscos do MF (**Aceitar**, **Mitigar** ou **Evitar**), oriundas das **Notas de Risco**, servem de base à tomada de decisão do gestor nas ações a serem adotadas. Entretanto, nos casos em que o gestor decidir por não promover ação ou adotar alguma providência às Notas de Risco que apontam à ação de **Mitigar** ou **Evitar**, essa decisão deverá ser formalmente justificada e documentada. A finalidade da elaboração do Plano de Implementação de Controles é documentar as opções de tratamento que serão adotadas. A tanto, o gestor deverá levar em consideração:

Plano de Implementação de Controles

Aspectos a serem observados na implementação dos controles

Os custos e esforços (diretos ou de oportunidade) de implementação, bem como os benefícios decorrentes

Os requisitos legais, normativos e regulatórios

Os responsáveis por aprovar e implementar as ações

Recursos necessários

Cronograma e Programação

O gestor deverá adotar ações – controle novo ou melhorar controle existente, e registrá-las em formulário eletrônico, como o disponibilizado no [GRIFA](#).

O formulário permitirá ao gestor informar o tipo de plano (adotar um controle novo ou melhorar um controle existente); descrever a ação; informar o responsável pela implementação da ação; como se dará a implementação da ação, início e fim, bem como estabelecer sua Meta de Nota de Risco.



Visando auxiliar o gestor na quanto às ações de tratamento constantes do Plano de Implementação de Controles, foi disponibilizada uma lista de controles básicos – Anexo F. É essencial que os gestores, tomadores de decisão, ter ciências da natureza e da extensão do risco após seu tratamento. Assim, o modelo prevê o registro da Meta de Nota de Risco. Esta Meta representa a nota que o gestor espera atingir com as ações propostas em seu Plano.

4.4.2 Mapa de Risco

Para permitir ao gestor e às partes interessadas conhecerem o resultado do mapeamento de riscos foi desenvolvido o Mapa de Risco, disponibilizado no [GRIFA](#).

A sequência dos dados no Mapa de Risco é a seguinte:

- os riscos são vinculados ao processo, macroprocesso, valor da Cadeia de Valor integrada do Ministério da Fazenda;
- foco da análise;
- o resultado da avaliação dos riscos;
- o resultado da mensuração dos riscos – Nota de Risco;
- as evidências;
- as ações de tratamento; e
- a meta de Nota de Risco estabelecida pelo gestor.



4.5. Monitoramento e Reporte Gerencial

O monitoramento e o reporte gerencial atualmente são atividades debatidas no âmbito do [Comitê de Gestão de Riscos, Controle e Integridade – CGRCI](#), conforme a **Política de Gestão de Riscos** do Ministério da Fazenda, e o **Modelo de Relacionamento** para a Gestão de Riscos do Ministério da Fazenda. Normas e diretrizes complementares podem ser editadas nesse sentido.

Por fim, destaca-se que foi lançado o Programa de Integridade do Ministério da Fazenda – PREVENIR¹⁷, com a finalidade de promover a prevenção, detecção e correção da prática de desvios éticos, ilícitos administrativos, fraude e corrupção no âmbito do MF. Assim, este Manual pode auxiliar ainda os órgãos e entidades do MF no sentido de tratar dos Riscos à Integridade.

REFERÊNCIAS

ISO 31000:2018 – Gestão de Riscos: Diretrizes. Associação Brasileira de Normas Técnicas – ABNT. Fev. 2018.

WILDAVSKY, Aaron. “**No Risk is the Highest Risk of All**”. American Scientist nº. 67. P. 32-37. 1979.

¹⁷ Portaria MF nº 116, de 3 abr. 2018.



ANEXO A – Exemplos de Medidas de Tratamento a Riscos à Integridade

Exemplos de Medidas de Tratamento a Riscos à Integridade
Atualização do Banco de Talentos da entidade pelos servidores, como estímulo para processos de solicitação de capacitação e promoção na carreira
Ações de sensibilização voltadas à prevenção de condutas antiéticas
Estudo sobre critérios para identificação e avaliação de líderes da entidade, para atualização da Política de Gestão de Pessoas
Revisão do Código de Conduta Profissional do Servidor da entidade
Ações permanentes de monitoramento de acesso a sistemas e pastas de rede
Adoção de postura pró-ativa para identificação de temas específicos com vistas a fomentar a capacitação interna
Implantação da Base de Conhecimento da entidade
Mapeamento e divulgação dos Canais de Denúncia e de fluxos dos processos da Comissão de Ética
Elaboração de normativo que trate sobre a omissão de irregularidades de forma intencional
Projeto “Programa de Valores da Entidade”
Programa de Desenvolvimento de Líderes
Aperfeiçoamento de ferramentas de trabalho e comunicação interna, que possibilitam a edição de trabalhos de maneira colaborativa
Procedimentos e trilhas para identificação de casos de nepotismo na entidade
Exigência de declaração de parentesco no momento da posse para cargos em comissão, funções e confiança, terceirizados ou estagiários
Orientação contínua reforçando a obrigatoriedade de utilização dos controles existentes nos processos de auditoria
Metodologia para implementação das revisões de qualidade no âmbito do Programa de Avaliação e Melhoria da Qualidade das Ações de Controle
Política de rotação periódica de servidores / coordenadores
Política que impeça que auditores da entidade que estavam atuando na gestão em unidades auditadas realizem trabalhos de auditoria sobre a mesma unidade pelo período de 2 anos

Fonte: Adaptado de “Programa de Integridade da CGU: Eixo 3 – Riscos à Integridade”.

**ANEXO B – Dimensões do Modelo Conceitual de Gerenciamento**

Dimensão	Tipo de Risco	Fator de Risco	Subfatores
Funcional	Risco Operacional ¹⁸	Processos	<ul style="list-style-type: none">▪ Comunicação Interna: comunicação apropriada, clara, objetiva e de fácil acesso para consulta.▪ Modelagem: desenho, redesenho e documentação de processos com seus controles e instrumentos de mitigação.▪ Segurança Física: segurança de pessoas e equipamentos.▪ Adequação à legislação: leis e jurisprudências vigentes no país – <i>compliance</i>.
		Pessoas	<ul style="list-style-type: none">▪ Carga de Trabalho: compatibilização das demandas de trabalho à capacidade operacional e à jornada de trabalho.▪ Competência: autoridade, habilidade e conhecimento para execução do processo.▪ Ambiente Organizacional: clima organizacional e infraestrutura adequada para execução do processo.▪ Conduta: postura ética nos relacionamentos interpessoais, atenção e zelo, imparcialidade, confidencialidade e comprometimento para a execução do processo.
		Ambiente Tecnológico	<ul style="list-style-type: none">▪ Segurança Lógica: acesso aos sistemas de TI pelos servidores, usuários externos, contratados, fornecedores e parceiros para a execução do processo.▪ Infraestrutura Tecnológica: disponibilidade de <i>hardware</i> e <i>software</i> para a execução do processo.▪ Solução de TI: especificação, desenvolvimento, manutenção, homologação e implantação de soluções de TI em consonância à necessidade de execução do processo.▪ Comunicação: disponibilidade de rede física e lógica com acesso aos usuários internos e externos para a execução do processo.
		Eventos Externos	<ul style="list-style-type: none">▪ Desastres Naturais e Catástrofes: eventos naturais ou catástrofes que provoque dano à continuidade das operações.▪ Ambiente Regulatório: mudanças políticas, legislação e regulamentação que interfira na execução do processo, inclui o risco de imagem.

¹⁸ É o risco associado à possibilidade de perda resultante da ocorrência de falha, deficiência ou inadequação de processos internos, pessoas e ambiente tecnológico, ou de eventos externos (Resolução CMN 3380/2006).



Dimensão	Tipo de Risco	Fator de Risco	Subfatores
			<ul style="list-style-type: none">▪ Ambiente Social: situação econômico-social que interfira na execução do processo, inclui o risco de imagem.▪ Fornecedores: desempenho e qualidade dos fornecedores de produtos e serviços que interfira na execução do processo.
Estratégica	Risco Estratégico ¹⁹	Descontinuidade	Desempenho inadequado do processo em função de tomada de decisão do gestor que afete a realização das diretrizes estratégicas.
		Indisponibilidade de Recursos	Alteração de recursos previstos que afetem a realização dos objetivos dos processos estratégicos.
	Risco de Projeto ²⁰	Atraso	Não cumprimento das entregas de produtos previstas nos projetos estratégicos, que, ocasionando atrasos, afetem a realização dos objetivos do projeto.
		Indisponibilidade de Recursos	Alteração de recursos previstos que afetem a realização dos objetivos dos processos estratégicos.
		Perda de Patrocínio	Falta de apoio político à realização do projeto estratégico que afete o alcance dos seus objetivos.
	Risco de Conjuntura ²¹	Mudanças Internas	Condições políticas, culturais, sociais, econômicas ou financeiras do Brasil.
		Mudanças Externas	Condições políticas, culturais, sociais, econômicas ou financeiras de outros países.

¹⁹ É o risco associado à possibilidade de perda resultante do insucesso das estratégias adotadas, levando-se em conta os negócios (clientes, concorrência, fornecedores e investimentos) e as alterações políticas e econômicas no contexto de atuação, ou seja, qualquer incerteza que afete os objetivos.

²⁰ É o risco associado à possibilidade de perda resultante da ocorrência de um conjunto de eventos sob a forma de ameaças que, caso se concretizem, afetem a realização dos objetivos do projeto.

²¹ É o risco associado à possibilidade de perda resultante de mudanças verificadas nas condições políticas, culturais, sociais, econômicas ou financeiras do Brasil ou de outros países.



Dimensão	Tipo de Risco	Fator de Risco	Subfatores
Econômica	Risco de Mercado ²²	Taxa de Juros	Mudanças adversas nas taxas de juros e/ou em seus derivativos.
		Taxa de Câmbio	Mudanças adversas nas taxas de câmbio e/ou em seus derivativos.
		Títulos Públicos	Mudanças adversas na precificação dos títulos públicos.
		Participações Societárias	Efeitos dos preços das ações da União sobre a posição financeira, desempenho financeiro e fluxos de caixa.
		Indicadores Econômicos	Flutuações nos preços dos ativos indexados por índices de preços, índices de bolsas.
	Risco de Crédito ²³	Inadimplência	Incerteza no recebimento por incapacidade de pagamento do tomador de empréstimo, contraparte de um contrato ou de um emissor de título.
		Garantias Associadas	Suficiência e liquidez das garantias associadas aos débitos e ações de execução.
		Litígio	Atrasos ou não recebimento de créditos concedidos em função de contestação judicial.
		Entrada de Recursos	Captação no mercado, arrecadação de tributos e outras receitas, obtenção de crédito junto a organismos.
		Exigência de	Atendimento/cumprimento de obrigações/compromissos

²² É o risco associado à possibilidade de perda resultante de movimentação de preços de mercado, notadamente de flutuações de taxas de juros, câmbio, preços de ações e commodities ou indicadores econômicos que impactem a captação/desembolso de recursos.

²³ É o risco associado à possibilidade de perda resultante da incerteza quanto ao recebimento de valores pactuados com tomadores de financiamentos e tributos inscritos na dívida ativa.



Dimensão	Tipo de Risco	Fator de Risco	Subfatores
	Risco de Liquidez²⁴	Caixa	programados.
		Desvalorização de Ativos	Condições em que o valor contábil do ativo excede seu valor recuperável.
	Risco de Conjuntura	Mudanças Internas	Condições políticas, culturais, sociais, econômicas ou financeiras do Brasil.
		Mudanças Externas	Condições políticas, culturais, sociais, econômicas ou financeiras de outros países.

²⁴ é o risco associado à possibilidade de perda resultante do descasamento entre a entrada de recursos (captação no mercado, arrecadação de tributos/outras receitas e obtenção de crédito junto a organismos) para atender às exigências de caixa que impactem o cumprimento de obrigações/compromissos programados.

**ANEXO C – Identificação de Risco: Perguntas Orientadoras**

Dimensão	Tipo de Risco	Fator de Risco	Perguntas Orientadoras
Funcional	Risco Operacional	Processos	Existem ameaças associadas à possibilidade de perda resultante da ocorrência de falha, deficiência ou inadequação de processos ?
		Pessoas	Existem ameaças associadas à possibilidade de perda resultante da ocorrência de falha, deficiência ou inadequação de pessoas ?
		Ambiente Tecnológico	Existem ameaças associadas à possibilidade de perda resultante da ocorrência de falha, deficiência ou inadequação de ambiente tecnológico ?
		Eventos Externos	Existem ameaças associadas à possibilidade de perda resultante da ocorrência de falha, deficiência ou inadequação de eventos externos ?
Estratégica	Risco Estratégico	Descontinuidade de	Existe o risco de descontinuidade neste processo ao ponto de comprometer o alcance deste valor?
		Indisponibilidade de Recursos	Existe o risco de indisponibilidade de recursos neste processo ao ponto de comprometer o alcance deste valor?
	Risco de Projeto (Existe PROJETO vinculado a este processo para atingimento do valor?)	Atraso	Existe o risco de atraso no PROJETO vinculado a este processo ao ponto de comprometer o alcance deste valor?
		Indisponibilidade de Recursos	Existe o risco de indisponibilidade de recursos no PROJETO vinculado a este processo ao ponto de comprometer o alcance deste valor?
		Perda de Patrocínio	Existe o risco de perda de patrocínio no PROJETO vinculado a este processo ao ponto de comprometer o alcance deste valor?
	Risco de Conjuntura	Mudanças Internas	Existe risco de mudanças internas neste processo ao ponto de comprometer o alcance deste valor?
		Mudanças Externas	Existe risco de mudanças externas neste processo ao ponto de comprometer o alcance deste valor?
Econômica	Risco de Mercado	Taxa de Juros	Existe o risco de flutuações de mercado na taxa de juros neste processo ao ponto de comprometer o alcance deste valor?
		Taxa de Câmbio	Existe o risco de flutuações de mercado na taxa de câmbio neste processo ao ponto de comprometer o alcance deste valor?



Dimensão	Tipo de Risco	Fator de Risco	Perguntas Orientadoras
		Títulos Públicos	Existe o risco de flutuações de mercado nos preços dos títulos públicos neste processo ao ponto de comprometer o alcance deste valor?
		Participações Societárias	Existe o risco de flutuações de mercado no preço das ações da união neste processo ao ponto de comprometer o alcance deste valor?
		Indicadores Econômicos	Existe o risco de variações nos indicadores econômicos neste processo ao ponto de comprometer o alcance deste valor?
	Risco de Crédito	Inadimplência	Existe risco de default neste processo ao ponto de comprometer o alcance deste valor?
		Garantias Associadas	Existe risco de default na execução das garantias associadas neste processo ao ponto de comprometer o alcance deste valor?
		Litígio	Existe risco de litígio de créditos neste processo ao ponto de comprometer o alcance deste valor?
	Risco de Liquidez	Entrada de Recursos	Existe risco de descasamento entre a entrada de recursos e obrigações a pagar originado pela incerteza acerca da entrada de recursos ao ponto de comprometer o alcance deste valor?
		Exigência de Caixa	Existe risco de descasamento entre a entrada de recursos e obrigações a pagar originado pela incerteza de caixa ao ponto de comprometer o alcance deste valor?
		Desvalorização de Ativos	Existe risco de descasamento entre a entrada de recursos e obrigações a pagar originado pela desvalorização de ativos ao ponto de comprometer o alcance deste valor?
	Risco de Conjuntura	Mudanças Internas	Existe risco de mudanças internas neste processo ao ponto de comprometer o alcance deste valor?
		Mudanças Externas	Existe risco de mudanças externas neste processo ao ponto de comprometer o alcance deste valor?

**ANEXO D – Identificação de Risco: Taxonomia de Riscos**

Risco Operacional	
Fator	Subfator e Exemplos de Riscos (Taxonomia)
PROCESSOS	<p>COMUNICAÇÃO INTERNA:</p> <ul style="list-style-type: none">Os insumos e as informações não são recebidos em tempo adequado para a execução do processoAusência de padrões mínimos definidos para a execução do processoErros e falhas de informações que afetam a execução do processo <p>MODELAGEM:</p> <ul style="list-style-type: none">Fluxo desatualizado e não reflete a prática atual utilizada na execução do processoAusência de avaliações periódica sobre a adequabilidade do desenho do processoAusência ferramenta para análise e melhoria contínua do processoFalha ou falta de metodologia que auxilie no mapeamento do processo <p>SEGURANÇA FÍSICA:</p> <ul style="list-style-type: none">Falha ou falta de segurança no ambiente de trabalho que afeta a execução do processoAcesso a áreas consideradas como críticas sem que as pessoas estejam devidamente credenciadas e identificadas <p>ADEQUAÇÃO À LEGISLAÇÃO:</p> <ul style="list-style-type: none">Descumprimento de prazos legais na execução do processoAusência de compilação e distribuição de legislação pertinente ao processo em execuçãoExecução do processo em desacordo com o regimento interno/normasDescumprimento de prazo judicial na execução do processoDescumprimento de obrigação regulatória na execução do processo
PESSOAS	<p>CARGA DE TRABALHO:</p> <ul style="list-style-type: none">Rotatividade (<i>turnover</i>) de pessoal acima do esperado que afeta a execução do processoCapacidade operacional insuficiente para a execução do processoFalha ou falta de dimensionamento da capacidade operacional com impacto na execução do processo <p>COMPETÊNCIAS:</p> <ul style="list-style-type: none">Capacitação da equipe é insatisfatória para a execução do processoConcentração de conhecimentos em determinados servidores afetando a execução do processoFalha ou falta de disseminação de conhecimento afetando a execução do processoFalha ou falta de capacitação que afeta a execução do processo <p>AMBIENTE ORGANIZACIONAL:</p> <ul style="list-style-type: none">Ausência de satisfação e/ou de bem-estar do servidor na execução de sua tarefaDesconhecimento dos objetivos do processo por parte dos ServidoresServidores desconhecem as suas responsabilidades individuais na execução do



Risco Operacional	
Fator	Subfator e Exemplos de Riscos (Taxonomia)
	<p>processo</p> <ul style="list-style-type: none">Ausência de recursos necessários para execução das tarefasResistência de Servidores em promover alterações nas condições de trabalho <p>CONDUTA:</p> <ul style="list-style-type: none">Ausência de postura ética nas atividades e nos relacionamentos interpessoaisFalta de atenção e zelo na execução do processoAusência de imparcialidade, cumprimento das leis e normas/regulamentares, confidencialidade e comprometimento na execução do processoQuebra de sigilo e confidencialidade
AMBIENTE TECNOLÓGICO	<p>SEGURANÇA LÓGICA:</p> <ul style="list-style-type: none">Ausência de estrutura de perfis de acesso aos sistemas para execução do processoAusência de controle de acesso lógicoAusência de <i>logon</i> próprio na rede institucionalFalha ou falta de meios seguros de acesso aos sistemasInexistência de registro nos sistemas (<i>log</i>) das transações críticasAusência de formalização que defina as responsabilidades do usuário externo do sistemaIncapacidade do sistema de prover informações confiáveis e suficientes sobre o processo em execução <p>INFRAESTRUTURA TECNOLÓGICA:</p> <ul style="list-style-type: none">Grau de informatização do processo inadequado para execução do processoInformações e dados armazenados em diretórios não protegidos e sem controle de acessoAusência de backup de arquivos, planilhas e bancos de dados essenciais à execução do processoA estação de trabalho não possui acionado dispositivo de <i>time-out</i>Descarte de mídias sem antes terem apagados os com conteúdo reservadoSobrecarga de sistemas de processamento de dados no momento da execução do processoInadequação de sistemas operacionais/aplicativos para execução do processoFalhas de hardware, faltas de backup e de legalização do software afetando a execução do processoObsolescência dos sistemas e equipamentos afetando a execução do processoAtaques lógicos à rede de computadores afetando a execução do processo <p>SOLUÇÃO DE TI:</p> <ul style="list-style-type: none">Inexistência de controle nas requisições e nas melhorias requeridas nos sistemas cuja falta de implementação afeta a execução do processoFalha ou falta de homologação de sistema impedindo a execução do processo de forma automatizada <p>COMUNICAÇÃO:</p>



Risco Operacional	
Fator	Subfator e Exemplos de Riscos (Taxonomia)
	<ul style="list-style-type: none">▪ Instabilidade nos sistemas operacionais que afeta a execução do processo▪ Incompatibilidade e/ou indisponibilidade de informações afetando a execução do processo
EVENTOS EXTERNOS	<p>DESASTRES NATURAIS E CATASTROFE:</p> <ul style="list-style-type: none">▪ <i>Ação Humana:</i> 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▪ <i>Força Maior:</i> (i) enchentes, terremotos, catástrofes (queda de prédio) e outros desastres naturais <p>AMBIENTE REGULATÓRIO:</p> <ul style="list-style-type: none">▪ Alterações inesperadas na legislação ou em marcos regulatórios pelos órgãos fiscalizadores e reguladores <p>AMBIENTE SOCIAL:</p> <ul style="list-style-type: none">▪ 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 <p>FORNECEDORES:</p> <ul style="list-style-type: none">▪ 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 E – Descrição da Nota de Risco**

Nota	Descrição da Nota de Risco
Aa++	Baixo nível de risco, baixo volume de ocorrências risco e baixa frequência de execução
Aa+	Baixo nível de risco, baixo volume de ocorrências risco e média frequência de execução
Aa-	Baixo nível de risco, baixo volume de ocorrências risco e alta frequência de execução
Ab++	Baixo nível de risco, médio volume de ocorrências risco e baixa frequência de execução
Ab+	Baixo nível de risco, médio volume de ocorrências risco e média frequência de execução
Ab-	Baixo nível de risco, médio volume de ocorrências risco e alta frequência de execução
Ac++	Baixo nível de risco, alto volume de ocorrências risco e baixa frequência de execução
Ac+	Baixo nível de risco, alto volume de ocorrências risco e média frequência de execução
Ac-	Baixo nível de risco, alto volume de ocorrências risco e alta frequência de execução
Ba++	Médio nível de risco, baixo volume de ocorrências risco e baixa frequência de execução
Ba+	Médio nível de risco, baixo volume de ocorrências risco e média frequência de execução
Ba-	Médio nível de risco, baixo volume de ocorrências risco e alta frequência de execução
Bb++	Médio nível de risco, médio volume de ocorrências risco e baixa frequência de execução
Bb+	Médio nível de risco, médio volume de ocorrências risco e média frequência de execução
Bb-	Médio nível de risco, médio volume de ocorrências risco e alta frequência de execução
Bc++	Médio nível de risco, alto volume de ocorrências risco e baixa frequência de execução
Bc+	Médio nível de risco, alto volume de ocorrências risco e média frequência de execução
Bc-	Médio nível de risco, alto volume de ocorrências risco e alta frequência de execução
Ca++	Alto nível de risco, baixo volume de ocorrências risco e baixa frequência de execução
Ca+	Alto nível de risco, baixo volume de ocorrências risco e média frequência de execução
Ca-	Alto nível de risco, baixo volume de ocorrências risco e alta frequência de execução
Cb++	Alto nível de risco, médio volume de ocorrências risco e baixa frequência de execução
Cb+	Alto nível de risco, médio volume de ocorrências risco e média frequência de execução
Cb-	Alto nível de risco, médio volume de ocorrências risco e alta frequência de execução
Cc++	Alto nível de risco, alto volume de ocorrências risco e baixa frequência de execução
Cc+	Alto nível de risco, alto volume de ocorrências risco e média frequência de execução
Cc-	Alto nível de risco, alto volume de ocorrências risco e alta frequência de execução



ANEXO F – Exemplos de Controles Básicos

Fator	Subfator	Controles Básicos	
Pessoas	Carga de Trabalho	Planejamentos de longo, médio e curto prazos	
		Acordo de Trabalho	
		Pesquisa de Clima Organizacional	
		Reuniões Participativas	
	Competência	Identificação da Necessidade de Conhecimento / Habilidades	
		Atividades de Treinamento	
		Normas e Procedimentos Internos	
		Ferramentas de autoavaliação de Conhecimento / Habilidades	
	Ambiente Organizacional	Pesquisa de Clima Organizacional	
		Condições Ambientais	
		Comunicação com a Administração	
		Processo de Gerenciamento de Equipes	
	Conduta	Valores Éticos e Normas de Conduta da Empresa	
		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 clientes			
Processos	Comunicação Interna	Canais de Comunicação – Com funcionários	
		Normas e Procedimentos Internos	
	Modelagem	Ferramentas para Análise e Melhoria Contínua de Processos	
		Metodologia de Autoavaliação de Riscos e Controles	
		Metodologia de Desenvolvimento de Produtos e Serviços – CARPIS	
		Validações – <i>Backtesting</i>	
		Normas e Procedimentos Internos	
		Metodologia de Autoavaliação de Riscos e Controles	
		Mecanismos de Monitoramento e Reporte	
	Segurança Física	Mecanismos de Segurança Física	
		Controles de Acesso Físico	
		Manutenção de Equipamentos	
	Adequação à Legislação	Testes de Conformidade	
Ambiente Tecnológico	Segurança Lógica	Políticas e Diretrizes	
		Controles de Acesso Lógico	
		Arquivo e Preservação de Registros	
	Infraestrutura e Tecnologia	Manutenção de Equipamentos	
		<i>Layout</i> de formulários e Sistemas	
		Planos de Contingência	
		<i>Layout</i> de Formulários e Sistemas	
		Validações - <i>Backtesting</i>	
		Atividades de Treinamento	
	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	