INSTITUTO NACIONAL DO SEGURO SOCIAL

RESOLUÇÃO CEGOV/INSS Nº 50, DE 6 DE FEVEREIRO DE 2025

Aprova a Metodologia de Gestão de Riscos do INSS - Versão 2.0.

O **COMITÊ ESTRATÉGICO DE GOVERNANÇA DO INSTITUTO NACIONAL DO SEGURO SOCIAL – CEGOV/INSS**, no uso das atribuições que lhe foram conferidas pelo art. 5º da Portaria nº 3.213/PRES/INSS, de 10 de dezembro de 2019, e considerando o disposto no Decreto nº 9.203, de 22 de novembro de 2017, na Instrução Normativa Conjunta nº 1/MP/CGU, de 10 de maio de 2016, bem como o contido no Processo Administrativo nº 35014.125444/2021-15,

RESOLVE:

Art. 1º Esta Resolução aprova a Metodologia de Gestão de Riscos do INSS - Versão 2.0, na forma do Anexo.

Parágrafo único. A Metodologia de que trata o *caput* encontra-se em conformidade com a Política de Gestão de Riscos do INSS, instituída pela Resolução nº 5/CEGOV/INSS, de 28 de maio de 2020, e integra o Sistema de Gestão de Riscos do INSS.

Art. 2º Esta Resolução entra em vigor na data de sua publicação.

ALESSANDRO ANTONIO STEFANUTTO
Presidente

ISMÊNIO BEZERRA
Diretor de Governança, Planejamento e Inovação

ROBERTO CARNEIRO DA SILVA
Diretor de Gestão de Pessoas

DÉBORA APARECIDA ANDRADE FLORIANO
Diretora de Orçamento, Finanças e Logística

VANDERLEI BARBOSA DOS SANTOS
Diretor de Benefícios e Relacionamento com o Cidadão

MÁRIO GALVÃO DE SOUZA SÓRIA
Diretor de Tecnologia da Informação

Documento assinado eletronicamente por **Roberto Carneiro da Silva**, **Diretor(a) de Gestão de Pessoas**, em 06/02/2025, às 17:49, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **DEBORA APARECIDA ANDRADE FLORIANO**, **Diretor(a) de Orçamento, Finanças e Logística**, em 06/02/2025, às 18:38, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020 .

Documento assinado eletronicamente por **VANDERLEI BARBOSA DOS SANTOS**, **Diretor(a) de Benefícios e Relacionamento com o Cidadão**, em 07/02/2025, às 10:45, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020 .

Documento assinado eletronicamente por **MARIO GALVAO DE SOUZA SORIA**, **Diretor(a) de Tecnologia da Informação**, em 07/02/2025, às 17:44, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020 .

Documento assinado eletronicamente por **BRUNO BATISTA BARRETO**, **Coordenador(a)-Geral de Governança e Gerenciamento de Riscos**, em 10/02/2025, às 16:12, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020 .

Documento assinado eletronicamente por **ALESSANDRO ANTONIO STEFANUTTO**, **Presidente**, em 11/02/2025, às 20:41, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **19302331** e o código CRC **10ED8D6E**.

ANEXO

RESOLUÇÃO CEGOV/INSS Nº 50, DE 6 DE FEVEREIRO DE 2025

METODOLOGIA DE GESTÃO DE RISCOS DO INSS

Sumário

Controle de Versões

Controle de Versões		
Versão	Data de Revisão	Notas de Revisão
1.0	20 mai. 2022	-
2.0	Setembro de 2024	Lista de abreviaturas e siglas

		-Princípios e Objetivos da Gestão de Riscos no INSS - O Modelo das Três Linhas - Esclarecimentos sobre os referenciais estratégicos - Mapa Estratégico e Cadeia de Valor - Hierarquia dos Processos - Integração da Gestão de Riscos ao Planejamento Estratégico - Inclusão de novas ferramentas/técnicas úteis no processo de gerenciamento de riscos - Tipologia de Riscos e sua Natureza - Identificação e Avaliação dos Controles Internos de Gestão - Apetite a Risco do INSS - Declaração - Indicadores para a Gestão de Riscos - Relatórios Gerenciais - Monitoramento e Efetividade dos Controles

Lista de abreviaturas e siglas:

ABNT - Associação Brasileira de Normas Técnicas

CEGOV - Comitê Estratégico de Governança

CGU - Controladoria Geral da União

COSO - Committee of Sponsoring Organizations of the Treadway Commission

CSGR - Coordenador Setorial de Gestão de Riscos

DIGOV - Diretoria de Governança, Planejamento e Inovação

ICR - Indicador-Chave de Risco

IIA - The Institute of Internal Auditors

INSS - Instituto Nacional do Seguro Social

ISO - International Organization for Standardization

MPOG - Ministério do Planejamento, Orçamento e Gestão

NT - Nota Técnica

RCR - Relatório de Comunicação de Riscos

RRR - Relatório de Risco Residual

SISGR - Sistema de Gerenciamento de Riscos

TCU - Tribunal de Contas da União

1. Introdução

1.1 No âmbito do Poder Executivo Federal, o marco regulatório que dispõe sobre conceitos, princípios, objetivos e responsabilidades relacionados aos controles internos, gestão de riscos e governança é a Instrução Normativa MP/CGU nº 01, de 10 de maio de 2016. Essa instrução aborda como a estruturação desses mecanismos, devem ser adotadas pelos órgãos e entidades do governo, proporcionando sua aplicabilidade de forma sistêmica e eficaz.

1.2 Posteriormente, com o mesmo destaque, foi promulgado 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, conceituando a Gestão de Riscos como o processo de natureza permanente, estabelecido, direcionado e monitorado pela alta administração, que contempla as atividades de identificar, avaliar e gerenciar potenciais eventos que possam afetar a organização, destinado a fornecer segurança razoável quanto à realização de seus objetivos. Nesse contexto, a metodologia de gestão de riscos é instrumento por meio do qual a entidade estabelece e estrutura as etapas necessárias à operacionalização do gerenciamento de riscos, que é parte do processo institucional de gestão de riscos.

1.3 A Metodologia de Gestão de Riscos do INSS objetiva subsidiar a tomada de decisão, baseada em técnicas e ferramentas, preceituando sua aplicabilidade para todas as unidades da Instituição, sem prejuízo da utilização de outras normas complementares específicas, relativas aos processos de trabalho e projetos de cada unidade ou serviços providos pelo INSS.

1.4 Gerenciamento de Riscos no INSS consiste em um processo iterativo e contínuo, realizado por um conjunto de ações destinadas a identificar, analisar, avaliar, priorizar, tratar, comunicar e monitorar riscos. Riscos estes que são capazes de afetar os objetivos dos programas, projetos, processos de trabalho ou serviços, em diferentes níveis hierárquicos da estrutura organizacional.

1.5 Os riscos acompanham todas as atividades humanas, com possibilidades de interferência nos resultados desejados. A gestão de riscos está diretamente relacionada aos objetivos estratégicos de uma instituição, favorecendo o cumprimento da sua missão e visão organizacionais, ao antecipar e mitigar situações indesejadas.

1.6 O processo de gestão de riscos do INSS está alicerçado em alguns pilares, que devem ser observados e desenvolvidos continuamente para a qualificação da gestão e governança institucional. São eles:

I - Política de Gestão de Riscos;

II - Metodologia de Gestão de Riscos;

III - Solução Tecnológica e Apoio; e

IV - Capacitação Contínua.

1.7 Este documento tem por objetivo apresentar uma versão atualizada da Metodologia de Gestão de Riscos do INSS, aprovada pela Resolução CEGOV n. 20, de 20 de maio de 2022, prevista pela Política de Gestão de Riscos, instituída pelo Comitê Estratégico de Governança - CEGOV, por meio da Resolução nº 5/CEGOV/INSS, de 28 de maio de 2020.

2. Conceitos da Gestão de Riscos

Para fins desta Metodologia, consideram-se os seguintes conceitos:

I - análise qualitativa: compreender a importância do risco através de escalas médias de impactos e probabilidades;

II - análise quantitativa: investigar o impacto e efeitos do risco com precisão numérica;

III - análise semiquantitativa: associação das duas práticas (métrica e subjetiva) tornando-se um multicritério de apoio à decisão;

IV - apetite a risco: nível de risco que uma organização está disposta a aceitar para atingir seus objetivos organizacionais;

V - causa: condição que dá origem à possibilidade de um evento ocorrer, também chamada de fator de risco e pode ter origem no ambiente interno e externo;

VI - consequência/Impacto: Resultado de um evento que afeta de forma positiva ou negativa os objetivos;

VII - 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, destinados a enfrentar os riscos e fornecer segurança razoável de que os objetivos organizacionais serão alcançados;

VIII - coordenador-setorial de gestão de riscos: agente capacitado em gestão de riscos, que tem a responsabilidade de prover assessoramento no processo de gerenciamento de riscos;

IX - *framework*: conjunto de conceitos e boas práticas usados para orientar nas atividades relacionadas a um domínio específico, que apresenta a estrutura e implementação das estratégias de gerenciamento de riscos;

X - gerenciamento de riscos: aplicação sistemática de políticas, procedimentos e práticas de gestão para identificar, analisar, avaliar, tratar, comunicar e monitorar potenciais eventos ou situações de risco, bem como fornecer segurança razoável no alcance dos objetivos relacionados a processos, projetos e demais objetos avaliados;

XI - gestão de riscos: conjunto de princípios, estruturas, alçadas, processos e atividades coordenadas para dirigir e controlar a organização no que se refere a riscos;

XII - gestor de risco: agente que tem a responsabilidade e a autoridade para gerenciar determinado risco;

XIII - governabilidade: refere-se às condições sistêmicas e institucionais sob as quais se dá o exercício do poder, tais como as características do sistema político, a forma de governo, as relações entre os Poderes, o sistema de intermediação de interesses. É a capacidade do gestor de exercer com autonomia a

implementação de ações de maneira eficaz e legítima;

XIV - governança: combinação de processos e estruturas implantadas pela alta administração da organização, para informar, dirigir, administrar, avaliar e monitorar atividades organizacionais, com o intuito de alcançar os objetivos e prestar contas dessas atividades para a sociedade;

XV - indicador-Chave de Risco (ICR): indicador de desempenho da gestão de riscos diretamente relacionados aos processos, riscos e controles que tenham relevância ao atingimento dos objetivos;

XVI - nível do risco: resultado da aferição da criticidade do risco, considerando aspectos como probabilidade e impacto;

XVII - objeto de gestão: qualquer processo de trabalho, atividade, projeto, iniciativa ou ação de plano institucional do INSS;

XVIII - objetivo organizacional: situação que se deseja alcançar de forma a se evidenciar êxito no cumprimento da missão e no atingimento da visão de futuro;

XIX - plano de ação: é uma ferramenta estratégica, normalmente apresentada em um documento, que detalha os passos necessários para alcançar um ou mais objetivos;

XX - risco: possibilidade de ocorrência de um evento que venha a ter impacto no cumprimento dos objetivos;

XXI - risco-chave: risco que, em função do impacto potencial ao INSS, deve ser conhecido e acompanhado pela alta administração;

XXII - risco inerente: o risco a que o INSS está exposto sem considerar quaisquer ações gerenciais que possam reduzir a probabilidade de sua ocorrência ou seu impacto;

XXIII - risco residual: risco que o INSS está exposto após a implementação de ações gerenciais (controles internos) para o tratamento do risco; e

XXIV - *stakeholders*: “Partes interessadas”. São os grupos e indivíduos cujos interesses são atendidos ou impactados pela organização.

3. Gestão de Riscos no INSS

3.1 A Gestão de Riscos no INSS é o conjunto de princípios, estrutura, alçadas, processos e atividades coordenadas para dirigir, controlar e monitorar a organização no que se refere a riscos, conforme preceitua a Resolução nº 5/CEGOV/INSS, de 2020, sendo os seus pilares representados na figura abaixo:

Figura 1 – Pilares da Gestão de Riscos no INSS

3.2 Princípios da Gestão de Riscos no INSS

3.2.1 Os princípios da Gestão de Riscos desempenham um papel crucial na governança, gestão e tomada de decisões. Eles visam garantir que o órgão atenda aos interesses públicos, se adapte às mudanças, promova a transparência e envolva as partes interessadas de forma inclusiva.

3.2.2 Ao incorporar esses princípios em suas operações, o INSS poderá melhorar sua eficiência, responsabilidade e capacidade de inovação, contribuindo para um impacto positivo na sociedade e potencializando a qualidade dos serviços públicos ofertados. Considerar os riscos é importante, tanto para o estabelecimento de estratégia como melhoria da performance. Nesse contexto, compõe os princípios adotados pelo INSS na sua política de gestão de riscos:

I - criar e proteger valor público: prioriza o interesse público na geração e preservação de valor para a sociedade;

II - subsidiar a tomada de decisões: fornece informações e análise que direcionam a adoção de medidas necessárias;

III - abordar explicitamente a incerteza: reconhece e gerencia a incerteza, preparando a instituição a lidar com os imprevistos;

IV - aplicar-se de forma contínua e integrada a qualquer tipo de atividade, projeto e aos processos de trabalho: integração e aplicação holística, em todas as atividades e projetos, de forma continuada;

V - ser dinâmico, iterativo e capaz de reagir a mudanças: adaptar-se às mudanças e evoluir com base na retroalimentação de dados e no processo de melhoria contínua;

VI - estar integrado às oportunidades e à inovação: preparar a instituição para perceber a aproveitar as oportunidades do ambiente em que está inserida;

VII - basear-se nas melhores informações disponíveis: qualificar as informações, trazendo o conhecimento dos processos internos e do ambiente externo, para que se possa tomar decisões com base em informações precisas e confiáveis;

VIII - ser transparente e inclusivo: divulgação aberta de informações e envolvimento de todas as partes interessadas no processo;

IX - considerar a importância dos fatores humanos e culturais: reconhecer o papel das pessoas e da cultura na eficácia das operações e decisões;

X - facilitar a melhoria contínua da organização: promover um ambiente que incentive a melhoria constante e aprendizado organizacional; e

XI - ser dirigido, apoiado e monitorado pela alta administração: envolver a liderança estratégica no direcionamento, apoio e monitoramento dos princípios.

3.3 Objetivos

3.3.1 Definir objetivos é essencial para o sucesso organizacional, pois orienta a tomada de decisões, alinha esforços em um propósito comum e prioriza recursos de maneira eficiente. Esses objetivos promovem coesão e facilitam a comunicação com as partes interessadas, permitindo avaliação do progresso e das ações conforme necessário.

3.3.2 Dentro dessa perspectiva são objetivos da gestão de risco no INSS:

I - aumentar a:

a) probabilidade de atingir os objetivos; e

b) capacidade da organização de se adaptar às mudanças;

II - fomentar uma gestão proativa;

III - preservar a imagem institucional;

IV - facilitar a identificação de oportunidades e ameaças;

V - prezar pelas conformidades legal e normativa dos processos organizacionais;

VI - melhorar:

a) o controle interno da gestão;

b) a prestação de contas à sociedade;

c) a governança;

d) a eficiência operacional;

e) a prevenção de perdas e a gestão de incidentes; e

f) a aprendizagem organizacional;

VII - estabelecer:

a) uma base confiável para a tomada de decisão e o planejamento; e

b) controles proporcionais ao risco, observada a relação custo-benefício;

VIII - alocar e utilizar eficazmente os recursos para o tratamento de riscos; e

IX - minimizar perdas.

3.4 O Modelo das Três Linhas

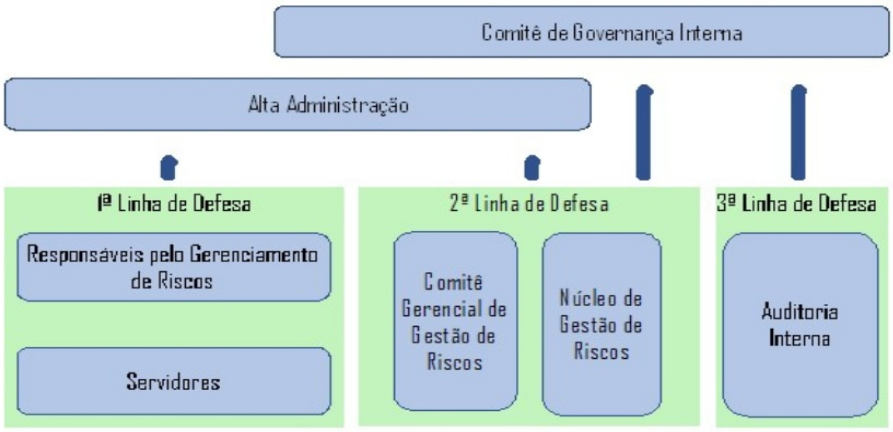
3.4.1 As organizações são empreendimentos humanos operando em um mundo cada vez mais incerto, complexo, interconectado e volátil. Geralmente, elas têm vários *stakeholders* com interesses diversos, mutáveis e, às vezes, concorrentes. Os *stakeholders* confiam a supervisão organizacional a um corpo administrativo,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

3.4.2 O Modelo das Três Linhas (primeira, segunda e terceira linha) implementado pelo The *Institute of Internal Auditors* (IIA), fundado em 1941, ajuda as organizações a identificar estruturas e processos que melhor auxiliam no atingimento dos objetivos e facilitam uma forte governança e gerenciamento de riscos. Além disso, contribui para definir papéis e responsabilidades dentro de uma organização em relação ao gerenciamento de riscos e ao controle interno:

I - 1º linha: gestão operacional, controles internos da gestão executados por todos os agentes públicos responsáveis pela condução de atividades e tarefas, no âmbito dos macroprocessos finalísticos e de sustentação (Apoio) dos órgãos e entidades. É composta pelos servidores e pelos responsáveis pelo gerenciamento de riscos dos processos organizacionais – Gestores de Riscos;

II - 2º linha: funções de gerenciamento de riscos e conformidade, supervisão e monitoramento dos controles internos executados por instâncias específicas, como comitês, diretorias ou assessorias específicas para tratar de riscos, controles internos, integridade e conformidade. É composta pela Diretoria de Governança, Planejamento e Inovação - DIGOV com a colaboração do CSGR; e

III - 3º linha: constituída pelas auditorias internas no âmbito da Administração Pública, uma vez que são responsáveis por aferir a efetividade do gerenciamento de riscos e a adequação dos controles internos, bem como, apoiar a estruturação e efetivo funcionamento da primeira e da segunda linha, por meio da prestação de serviços de consultoria e avaliação dos processos de governança - AUDGER.



Fonte: Declaração de Posicionamento do IIA: as três linhas de defesa no gerenciamento eficaz de riscos e controles (IIA, 2013, adaptado)

3.4.3 Este modelo foi desenvolvido para promover uma governança eficaz e garantir que as responsabilidades sejam claramente definidas e segregadas, sendo aplicável a todas as organizações com as seguintes recomendações:

I - adotar uma abordagem baseada em princípios e adaptar o modelo para atender aos objetivos e circunstâncias organizacionais;

II - focar na contribuição que o gerenciamento de riscos oferece para atingir objetivos e criar valor, bem como questões de "defesa" e proteção de valor;

III - compreender claramente os papéis e responsabilidades representados no modelo e os relacionamentos entre eles; e

IV - implantar medidas para garantir que as atividades e os objetivos estejam alinhados com os interesses priorizados dos *stakeholders*.

3.5 Instâncias e Responsabilidades que compõe o processo de Gestão de Riscos no INSS

A hierarquia de responsabilidades do processo de gestão de risco foi definida de forma que todos os colaboradores compreendam o fluxo de atribuições e responsabilidades, tendo em vista seus respectivos papéis e instância de atuação. Nesse sentido, as instâncias que compõe o processo de gestão de riscos no INSS estão dispostas a seguir:

I - instância superior: composta pelo CEGOV, que tem a responsabilidade de aprovar os referenciais estratégicos para a Gestão de Riscos no INSS, como por exemplo, definir o apetite a riscos da Autarquia, e pelo Presidente do INSS, ao qual compete todas as atividades relacionadas ao patrocínio para as iniciativas desta natureza;

II - instância supervisora: *expertise*, apoio, monitoramento e questionamento sobre questões relacionadas a riscos. Composta pela DIGOV que desempenha o papel de unidade central de coordenação e supervisão da gestão de riscos, com a colaboração dos Coordenadores Setoriais de Gestão de Riscos, atuando como segunda linha;

III - instância avaliadora: Auditoria Interna - atuando como terceira linha - avaliação e assessoria independentes e objetivas sobre questões relativas ao atingimento dos objetivos; e

IV - instância executora: provisão de produtos/serviços aos clientes; gerenciar riscos. Composta por todos os servidores, Gestores de Riscos, responsáveis pela condução e execução de atividades e tarefas, no âmbito dos macroprocessos finalísticos e de sustentação (apoio) dos órgãos e entidades – primeira linha.

3.6 Recursos Operacionais, Tecnológicos e Capacitações

3.6.1 Os recursos operacionais e tecnológicos necessários para apoiar a condução das atividades de Gestão de Riscos do INSS estão definidos na Política de Gestão de Riscos, instituída pela Resolução nº 5/CEGOV/INSS, de 28 de maio de 2020. Compõe o repertório de recursos a serem observados: esta Metodologia, as soluções tecnológicas e de apoio, como o Sistema de Gerenciamento de Riscos (SISGR) e seu Guia, o Painel de Gestão de Riscos e o Manual de Gerenciamento de Riscos.

3.6.2 Dentro desta perspectiva, a Diretoria de Governança, Planejamento e Inovação implementou, por meio da Portaria Conjunta nº 1/DIGOV/DTI/INSS de 28 de março de 2023, o Sistema de Gerenciamento de Riscos – SISGR/INSS, como ferramenta para suporte e registro das etapas do processo de gerenciamento de riscos, objetivando aprimorar a segurança, transparência e a confiabilidade dos dados, criando condições mais adequadas para a produção e a utilização de informações dos riscos mapeados, além de facilitar o acesso às informações e a operacionalização do processo.

3.6.3 O SISGR também alimenta os dados que são enviados ao Painel de Gestão de Riscos do INSS, ferramenta implantada pela DIGOV que permite o acompanhamento dos riscos, mapeados pelo Gerenciamento de Riscos. Esse painel centraliza os dados do SISGR, permitindo o monitoramento dos riscos e das ações implementadas para mitigá-los, além disso, proporciona transparência para a alta administração e Coordenadores Setoriais de Gestão de Riscos, promovendo a clareza e a responsabilidade, ao mesmo tempo que ajuda na identificação de tendências e na tomada de decisões.

3.6.4 Para proporcionar a efetividade do processo, faz-se necessário reunir e utilizar os recursos, preceituados nesta Metodologia, instrumentalizando os servidores na sua práxis, pois estes são os detentores do conhecimento dos processos operacionais. Sendo assim, a execução de capacitações é um fator fundamental para o fomento de um ambiente de melhoria contínua e aprendizado organizacional, permitindo o cumprimento da missão institucional do INSS.

3.6.5 A DIGOV, com o patrocínio do Presidente, Diretores e Superintendentes Regionais, além do apoio da unidade responsável pela capacitação no INSS, ofertará iniciativas para capacitação, com o objetivo de promover o desenvolvimento dos Gestores de Riscos e dos Coordenadores Setoriais de Gestão de Riscos, como mecanismo de incentivo, dotação de recursos para a consecução de boas práticas de governança e de gestão, formando multiplicadores de Gestão de Riscos no INSS.

3.7 Atribuições dos componentes e suas responsabilidades

As atribuições de cada um dos componentes estão normatizadas na Política de Gestão de Riscos do INSS. Oportunamente as descrevemos abaixo:

I - gestores de riscos:

a) identificar, analisar, avaliar e tratar os riscos, conforme a Política de Gestão de Riscos do INSS;

b) definir os indicadores do processo de gerenciamento de riscos, visando à identificação de riscos não mapeados e a exclusão daqueles que, eventualmente, tenham perdido a importância;

c) apresentar à DIGOV os resultados do monitoramento sobre a efetividade do tratamento do risco;

d) acompanhar e monitorar os indicadores-chave de riscos na etapa de monitoramento do processo de gerenciamento de riscos;

e) reportar à DIGOV, com o assessoramento do Coordenador Setorial de Gestão de Riscos, e com a máxima urgência, o surgimento de Riscos-Chave e/ou o incremento de um risco já mapeado;

f) monitorar a evolução dos níveis de riscos e a efetividade das medidas de tratamento implementadas de acordo com a definição do apetite a risco do INSS;

g) registrar e recuperar as informações das ações de tratamento do risco, a fim de monitorar a necessidade de implementar novos controles ou modificar os existentes;

h) informar à DIGOV e a sua instância superior o Plano de Tratamento dos Riscos, em conformidade com as diretrizes estabelecidas por essa Diretoria;

i) identificar a natureza e a extensão do risco residual após o tratamento do risco; e

j) garantir informações relevantes e suficientes sobre o risco, tempestivamente, a fim de subsidiar a tomada de decisão;

II - Coordenadores Setoriais de Gestão de Riscos:

a) apoiar os Gestores de Riscos no desempenho das suas competências, técnica e metodologicamente, conforme definido na Política de Gestão de Riscos;

b) fomentar e assessorar, junto aos Gestores de Riscos, a elaboração e condução dos processos de gerenciamento de riscos da unidade de sua área de atuação;

c) acompanhar:

1. a implementação dos Planos de Tratamento dos Riscos junto aos Gestores de Riscos; e

2. o cumprimento máximo da periodicidade, de 1 (um) ano, após a etapa de tratamento, do ciclo do processo de gerenciamento de riscos dos processos organizacionais, em sua área de atuação;

d) consolidar os resultados das diversas áreas, no âmbito de sua atuação, em relatórios gerenciais e encaminhá-los a DIGOV; e

e) comunicar à DIGOV as mudanças ou fragilidades relacionadas aos riscos-chaves informadas

pelos Gestores de Riscos;

III - demais servidores e colaboradores em geral:

a) conhecer os riscos do seu processo de trabalho;

b) observar a evolução dos níveis de riscos e da efetividade das medidas de controles internos implementadas nos objetos de gestão em que estiverem envolvidos;

c) reportar, imediatamente, ao Gestor de Riscos responsável pelo respectivo objeto de gestão, quando identificar mudanças ou fragilidades em algum risco relacionado a esse objeto;

d) contribuir na execução dos processos de gerenciamento de riscos no âmbito de sua atuação, visando identificar os riscos do seu processo de trabalho; e

e) acionar, inicialmente, a primeira e a segunda linhas de defesa, no âmbito do INSS, antes do ingresso junto à terceira linha de defesa, sob pena de poder acarretar duplos esforços de apuração desnecessariamente, em desfavor do erário e do interesse público (Acordão nº 572/2022 - TCU Plenário).

4. Metodologia de Gestão de Riscos

4.1 A Metodologia de Gestão de Riscos é baseada em técnicas e ferramentas específicas que ajudam no alcance dos objetivos da organização, proporcionando a antecipação de possíveis eventos que possam afetar seu sucesso, promovendo a melhoria contínua dos processos de trabalho, reduzindo ou eliminando retrabalho e aumentando a assertividade para a implementação de estratégias para solução de problemas, entre outros benefícios.

4.1.1 Todas as unidades organizacionais devem executar os procedimentos previstos no processo de gerenciamento de riscos, em processos sob sua responsabilidade, obedecendo as diretrizes e orientações apresentadas neste documento, pois a política instituída pela Autarquia pressupõe um modelo de aplicação integrada e descentralizada. Ainda, deverá contemplar critérios predefinidos de avaliação continuada, de forma a permitir a comparabilidade entre os riscos, em todas as etapas.

4.1.2 No INSS a gestão de riscos está intrinsecamente relacionada aos referenciais estratégicos, Mapa Estratégico e a Cadeia de Valor. Para subsidiar a tomada de decisões e aplicá-las de forma contínua e integrada a qualquer tipo de atividade, projeto e processo de trabalho, deverão ser considerados os princípios da Gestão de Riscos do INSS, fundamentais para garantir a integração e o alinhamento das ações e projetos conduzidos.

4.1.3 O Mapa Estratégico é uma representação gráfica que comunica a estratégia de forma clara, alinhando objetivos estratégicos de longo prazo com ações específicas. Identifica e ilustra objetivos principais e suas inter-relações, abrangendo processos internos, perspectiva dos cidadãos, aprendizado, crescimento e resultados. Essa visão integrada facilita o alinhamento dos esforços de todos os níveis da organização, promovendo a comunicação e ajudando a monitorar o progresso em direção às metas estabelecidas.

4.1.4. O planejamento estratégico consolida-se graficamente no Mapa Estratégico, onde consta a missão, visão de futuro, direcionadores e objetivos estratégicos do INSS e cuja materialização ocorre por meio de iniciativas concretas, estruturadas na forma de Planos de Ação anuais.

4.1.5 O êxito na realização do planejamento estratégico está diretamente ligado ao bom desempenho na execução dos processos de negócio e à realização de iniciativas de melhorias contínuas através de projetos.

4.1.6 A Cadeia de Valor é uma representação gráfica dos principais processos da organização que agregam valor em seus resultados (Porter, 1985). Constitui em um alinhamento dos processos aos objetivos estratégicos da instituição, com base nos macroprocessos e processos principais, que são classificados como finalístico, sustentação ou gerencial:

I - Processos Finalísticos são também chamados de processos essenciais ou primários, pois representam as atividades essenciais que as organizações realizam para cumprir sua missão. Geralmente eles detêm características interfuncionais ponta a ponta que agrega valor diretamente para o cliente tipicamente externo;

II - Processos de Sustentação são também chamados de processos de apoio, pois agregam valor a outros processos e não diretamente aos clientes externos, podendo ser tanto os processos primários, como outros de suporte ou mesmo os gerenciais. São reconhecidos por fornecerem os recursos necessários para a execução das atividades de uma organização, os processos de suporte podem ser fundamentais e estratégicos para uma organização na medida que aumentam a sua capacidade de efetivamente realizar os processos primários. Podem ter a natureza funcionais ou interfuncionais; e

III - Processos Gerenciais, de Gestão ou de Gerenciamento têm a finalidade de coordenar, medir, monitorar e controlar as atividades de negócio de forma contínua. Assim como os processos de suporte, não agregam valor diretamente aos clientes externos, mas são essenciais para a busca da eficácia e eficiência, assim como para assegurar que a organização opere de acordo com seus objetivos e metas de desempenho. Podem ter a natureza funcionais ou interfuncionais.

4.1.7 Os referenciais estratégicos, demonstram a importância dos processos organizacionais, série de atividades relacionadas entre si, que promovem a transformação dos insumos em produtos ou serviços, que destinam atender às demandas e necessidades dos cidadãos, o que contribui para gerar valor aos usuários finais (clientes, cidadão, sociedade).

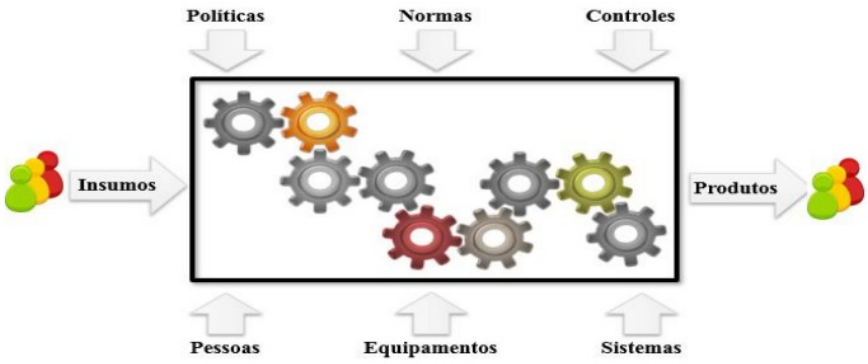


Figura 3 - Representação gráfica de processo

4.1.8 A construção da Cadeia de Valor ocorre a partir da identificação e ordenamento lógico dos processos de negócio de modo a apresentar a arquitetura organizacional.

4.1.9 Hierarquia dos Processos. Conforme o Guia Gerenciamento de Processo do INSS (2023), a hierarquia de processos é uma perspectiva que permite à organização visualizar como seus processos se desdobram de um nível de detalhamento da “visão do todo” (cadeia de valor) até uma “visão operacional” (mapa de processo e procedimentos). Para a classificação do processo é atribuída uma hierarquia, que

contempla os seguintes níveis:

I - macroprocesso representa a visão mais ampla de um processo que geralmente envolve mais de uma função da organização, cuja operação tem impactos significativos nas demais funções. Dependendo da complexidade, o macroprocesso é dividido em processos;

II - processo representa o conjunto de atividades que transformam insumos em resultados que representam agregação de valor. Dependendo da complexidade, o processo é dividido em subprocessos; e

III - Subprocesso representa uma divisão do processo com objetivos específicos, organizada seguindo linhas funcionais. Os subprocessos recebem entradas e geram suas saídas em um único departamento, podem apresentar uma etapa.

4.1.10 Assim, considerando a conceituação de hierarquia de processos, no INSS, recomenda-se que a avaliação dos riscos aconteça na instância subprocesso, que pode ser visualizada na figura a seguir:

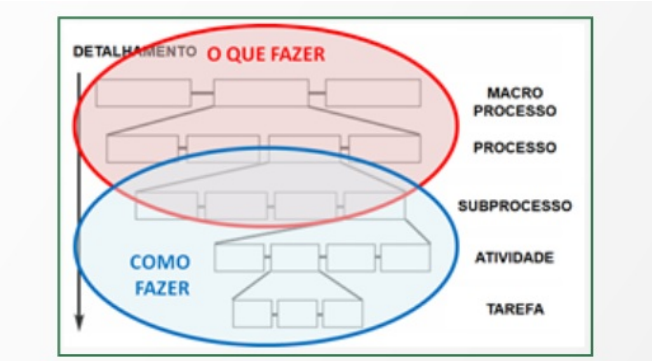


Figura 3: Nível de detalhamento dos processos.
Fonte: https://www.allankern.com.br/blog/2021/01/13/o-que-e-hierarquia-de-processos/

4.1.11 Integração da Gestão de Riscos ao Planejamento Estratégico

4.1.11.1 Melhores estruturas de governança, como o incentivo à gestão de riscos, podem potencializar a eficiência da prestação de serviços públicos. A gestão de riscos preserva e agrega valor à organização, contribuindo fundamentalmente para a realização de suas metas de desempenho, objetivos e cumprimento de sua missão. Para facilitar e orientar o processo de reconhecimento e administração dos riscos, estruturas e modelos foram criados e planejados para a redução de incertezas na tomada de ações e decisões por parte dos gestores (Giestosa, 2023).

4.1.11.2 A revisão do Coso ERM: Enterprise Risk Management: *Integrating with Strategy and Performance* (COSO, 2017), 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.

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

I - possibilidade de os objetivos estratégicos e de negócios não se alinharem com a missão, a visão e os valores fundamentais da organização;

II - as implicações da estratégica escolhida; e

III - os riscos na execução da estratégia.

4.1.11.4 Os riscos constituem insumo para o diagnóstico institucional do processo de planejamento estratégico. Ao se formular a estratégia institucional, deverão ser considerados os riscos intrínsecos àquela estratégia (COSO 2017). Deve ser considerado, também, o risco de a estratégia não estar alinhada à missão, à visão e às competências constitucionais do INSS.

4.1.11.5 Depois de estabelecida a estratégia, as possíveis medidas mitigadoras, submetidas ao processo decisório devido, constituirão ações constantes dos planos operacionais ordinários, sem necessidade de produção de planos de resposta a risco específicos.

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

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

4.1.11.6 O gerenciamento de riscos não depende, exclusivamente, do mapeamento dos processos de trabalho. A realização de oficinas com servidores que possuem profundo conhecimento do processo é geralmente suficiente para identificar os principais riscos e as respectivas medidas mitigadoras.

4.1.11.7 Com base nas indicações dos Gestores de Riscos, o CEGOV definirá a priorização dos processos que deverão ser objeto de gestão de riscos, levando em consideração a transversalidade e o impacto nos objetivos estratégicos do INSS. Essa priorização não impede que os gestores de riscos optem por gerir riscos de outros processos de trabalho sob sua responsabilidade.

4.2 Etapas do Gerenciamento de Riscos

4.2.1 A compreensão das atividades que envolve o gerenciamento de riscos será descrita como subprocesso (processo de trabalho), com as ações que deverão ser realizadas pelos gestores de riscos.

4.2.2 Dada a transversalidade da matéria, que requer conhecimento multidisciplinar de temas, o processo de gerenciamento de riscos deve ser conduzido, preferencialmente, de forma coletiva, por meio de oficinas ou reuniões, com pessoas que conhecem do processo, além dos atores envolvidos na tomada de decisão ao longo da cadeia de responsabilidades. Esta orientação deve ser aplicada em todas as etapas desta metodologia. Após a escolha dos projetos, processos de trabalhos e serviços, dar-se-á início ao processo de gerenciamento de riscos.

4.2.3 O gerenciamento de risco tem sua operacionalização contemplada nas seguintes etapas:

I - estabelecimento de contexto;

II - identificação de riscos;

III - análise e avaliação de riscos;

IV - tratamento dos riscos;

V - comunicação e consulta; e

VI - monitoramento e melhoria contínua.

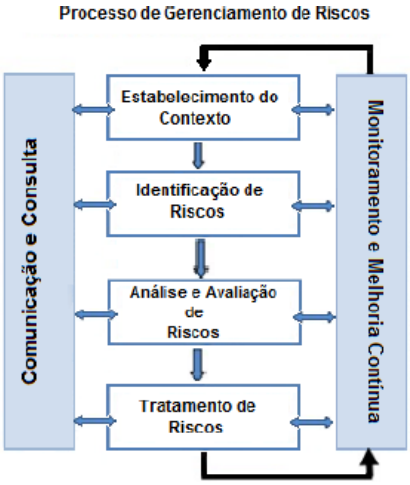


Figura 04 – Fonte: Norma ABNT NBR ISO 31000:2009 – Adaptado.

4.3 Estabelecimento de Contexto

4.3.1 Consiste em compreender o ambiente externo e interno no qual o objeto da gestão encontra-se inserido e em identificar parâmetros e critérios a serem considerados no processo de gestão de riscos.

4.3.2 O contexto para gestão de riscos refere-se ao entendimento do histórico da organização, considera os elementos da estratégia, relaciona-os aos fatores correspondentes ao ambiente interno e externo em que está inserido, e dos riscos envolvidos em suas tomadas de decisão a fim de utilizá-los nas etapas de identificação, análise, avaliação e tratamento dos riscos.

4.3.3 Em outras palavras, é preciso considerar os objetivos da organização, sua cadeia de valor (processos) e registrar os fatores correspondentes ao ambiente interno que estão sob sua governabilidade e o ambiente externo que não estão, que impactam os objetivos, resultados e partes interessadas.

4.3.4 O estabelecimento do contexto visa personalizar o objeto da gestão de riscos, com informações básicas. Nesta etapa é possível obter uma visão minuciosa e integral do objeto em estudo, onde deverão ser identificados:

I - órgão/Unidade do objeto;

II - informações:

a) quanto a existência de: Código de Ética, estrutura organizacional, políticas de recursos humanos, atribuição de alçadas e responsabilidades;

b) sobre a fixação de objetivos: missão, visão e objetivos da instituição; e

c) sobre o macroprocesso, processo e processo de trabalho: registrar sua descrição, objetivos, leis, regulamentos e sistemas associados.

4.3.5 Após a personalização do objeto de gestão é necessária a identificação dos atributos internos e externos relacionados ao objeto em estudo. Para execução desse procedimento, recomenda-se a utilização de ferramentas gerenciais estruturadas, como por exemplo a matriz *SWOT*. A palavra *SWOT* é um acrônimo formado pelas palavras inglesas *Strengths* (forças), *Weaknesses* (fraquezas), *Opportunities* (oportunidades) e *Threats* (ameaças), que permite a análise e registro dos fatores que se apresentam, como pontos fortes e fracos dentro do ambiente interno e oportunidades e ameaças, dentro do ambiente externo, ambos relacionados ao macroprocesso/processo/processo de trabalho.

4.3.6 A estruturação da *SWOT* baseia-se em uma matriz com quatro quadrantes e sua formulação deverá ser realizada e registada dentro do sistema SISGR.

4.3.7 As informações obtidas desta aplicação contribuem para a identificação dos riscos e se tornam um forte aliado de apoio estratégico à tomada de decisão, à medida que os pontos estabelecidos para análise passam a ser alvo da aplicação dos mecanismos de avaliação e controle de risco, resultando em uma estratégia que fomenta a tomada de decisão e provém elementos para seguir à segunda etapa.

4.3.8 Nesta altura, os pontos fortes e fracos estarão evidenciados e será possível testar os possíveis riscos ou ameaças que serão listados, a fim de serem posteriormente classificados, analisados e avaliados quanto aos eventuais impactos à tomada de decisão.

4.4 Identificação de Riscos

4.4.1 Essa etapa compreende o reconhecimento e a descrição dos riscos relacionados a um objeto de gestão, envolvendo a identificação de possíveis fontes de riscos e seus efeitos.

4.4.2 Consiste em encontrar, reconhecer e registrar os riscos. Envolve a identificação das fontes de risco, eventos, suas causas e suas consequências potenciais, dados históricos, análises teóricas, opiniões de pessoas informadas e especialistas, e as necessidades das partes interessadas.

4.4.3 A finalidade é mapear onde, o porquê e como os eventos de risco poderão impedir, inibir ou atrasar a consecução dos objetivos dos processos, ou quais situações que poderiam existir e afetar o alcance dos objetivos da organização.

4.4.4 Desta forma, a especificação de um risco é realizada pela associação de um evento de risco com uma causa. Para isso, é necessário identificar todos os eventos de riscos e suas respectivas consequências.

4.4.5 Todas as informações da gestão deverão ser tratadas de tal forma que tragam, com clareza, o objetivo ou resultado que se deseja alcançar, listando para cada objetivo os eventos que possam impactá-lo negativamente e descrevendo-os, a fim de que possam ser objeto de avaliação e tratamento nas fases seguintes do processo de gerenciamento de riscos.

4.4.6 Para facilitar a identificação dos eventos de riscos, sugere-se a utilização de algumas ferramentas que auxiliam nesse processo, como a realização de *brainstorm, brainwriting*, listas de verificação,

entrevistas, visitas técnicas, bem como a aplicação da técnica de *Bow Tie* ou Diagrama de *Ishikawa*.

4.4.7 A norma ABNT ISO/IEC 31010:2021 recomenda uma séria de técnicas e estratégias que poderão ser utilizadas durante esse processo. Destacamos algumas delas nessa metodologia, mas reforçamos que a sua utilização não é restritiva, sendo assim, a opção pela adoção de uma ou mais técnicas poderá ser feita ao longo dessa etapa.

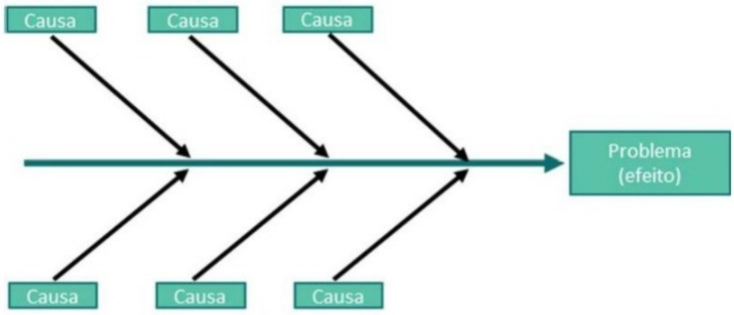
4.4.8 *Brainstorming* é um processo usado para estimular e encorajar um grupo de pessoas a desenvolver ideias relacionadas a um ou mais tópicos de qualquer natureza. *Brainwriting* é uma técnica similar ao *Brainstorming*, entretanto, em vez de utilizar o meio oral, as pessoas expõem suas ideias por escrito.

4.4.9 O diagrama que representa a técnica *Bow Tie*, por sua vez, está representado conforme figura abaixo:

Figura extraída da Metodologia da Antaq

4.4.10 Essa técnica, utilizada no SISGR, permite uma visualização sistêmica dos eventos de risco, correlacionando causa e consequência, de uma forma a possibilitar a investigação de medidas preventivas e de recuperação.

4.4.11 Ainda na avaliação de causa e efeito, também é comumente utilizado na análise sistemática das causas raiz o diagrama de *Ishikawa*, também conhecido como diagrama de espinha de peixe. Ao categorizar causas potenciais em diferentes ramos, o diagrama ajuda a compreender melhor as inter-relações entre fatores que podem estar contribuindo para o problema em questão.



4.4.12 Independentemente de as fontes estarem ou não sob controle, é adequado que se identifique os riscos. Convém considerar que pode haver mais de um tipo de resultado, o que pode resultar em uma variedade de consequências tangíveis ou intangíveis que deverão ser objeto de priorização de impacto ou relevância ao(s) objetivo(s) que se deseja alcançar.

4.4.13 A realização de algumas perguntas-chaves, nessa fase, também poderá ajudar a evidenciar os riscos possíveis, tais como:

I - quais situações ou elementos podem atrapalhar nesta fase ou em qualquer outra o cumprimento do objetivo almejado?

II - existem fatores críticos de sucesso e quais são?

III - quais as principais fontes de riscos ao longo do processo para atingimento do objetivo? Pessoas, processos, sistemas, legislação e eventos externos.

4.4.14 Para facilitar o entendimento dos elementos que compõem o gerenciamento dos riscos dos processos, recomenda-se utilizar a sintaxe abaixo, adaptada do TCU, inserindo os componentes dos riscos identificados, nos campos destacados, como forma de se obter sentido para a afirmação:

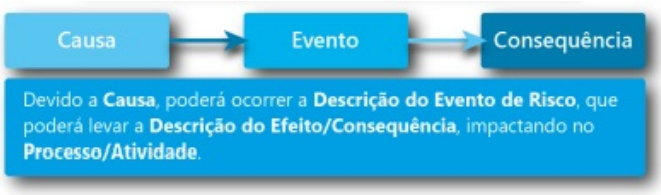


Figura 6. Sintaxe para o entendimento do processo de gestão de riscos.

Devido a <CAUSA/FONTE>,
Poderá acontecer <EVENTO DE RISCOS>,
O que poderá levar a <CONSEQUÊNCIA>,
Impactando no <OBJETIVO DO PROCESSO>

Fonte: TCU, 2017

4.4.15 A identificação de riscos está diretamente ligada às suas causas fundamentais e fragilidades, independentemente de suas fontes estarem ou não sob seu controle. Compreender os fatores subjacentes que originam os riscos, como falhas em processos ou vulnerabilidades, e as fragilidades que tornam uma organização mais suscetível, é crucial para desenvolver estratégias eficazes de prevenção e resposta.

4.4.16 A tabela abaixo apresenta alguns exemplos de fontes de riscos e suas fragilidades:

4.4.17 Tipologia de Riscos e sua Natureza

4.4.17.1 A tipologia dos riscos refere-se à classificação ou categorização dos diferentes tipos de riscos que uma organização ou projeto pode enfrentar. Esses riscos podem ser classificados de diversas maneiras, dependendo de sua origem, impacto ou natureza. A categorização desses riscos não é consensual na literatura, sendo assim, cabe a cada organização o desenvolvimento de suas categorias de acordo com suas peculiaridades.

4.4.17.2 A natureza dos riscos está relacionada à categoria de risco escolhida. Se a categoria de risco for orçamentária, a natureza do risco será orçamentário-financeira. As demais categorias de risco são consideradas não orçamentário-financeira. Sobre a classificação dos eventos de riscos quanto à sua natureza, vale esclarecer que esta metodologia adotará as seguintes tipologias de riscos:

I - riscos de conformidade: eventos que podem afetar o cumprimento de leis e regulamentos aplicáveis;

II - riscos de reputação: eventos que podem comprometer a confiança da sociedade (ou de parceiros, de clientes ou de fornecedores) em relação à capacidade do INSS em cumprir sua missão institucional;

III - riscos estratégicos: eventos que possam impactar na missão, nas metas ou nos objetivos estratégicos do INSS. Estes riscos deverão ser informados, de forma imediata, às instâncias superiores e à DIGOV que informará ao CEGOV;

IV - riscos orçamentários: eventos que podem comprometer a capacidade da iniciativa de contar com os recursos orçamentários necessários à realização de suas atividades, ou eventos que possam comprometer a própria execução orçamentária;

V - riscos operacionais: eventos que podem comprometer as atividades do órgão ou entidade, normalmente associados às falhas, deficiência ou inadequação de processos internos, pessoas, infraestrutura e sistemas, afetando o esforço da gestão quanto à eficácia e a eficiência dos processos organizacionais; e

VI - riscos à integridade: eventos que podem afetar a probidade da gestão dos recursos públicos e

das atividades do INSS, causados pela falta de honestidade e desvios éticos. Estes riscos deverão ser informados, às instâncias superiores e à DIGOV que informará ao CEGOV.

4.4.17.3 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 apresenta a seguinte definição sobre riscos de integridade:

> Art. 2º.....
>
> .....
>
> II - Riscos para a integridade: riscos que configurem ações ou omissões que possam favorecer a ocorrência de fraudes ou atos de corrupção.
>
> Parágrafo único. Os riscos para a integridade podem ser causa, evento ou consequência de outros riscos, tais como financeiros, operacionais ou de imagem.

4.4.17.4 A Organização para a Cooperação e Desenvolvimento Econômico (OCDE) define integridade pública como o alinhamento consistente e a adesão a normas, valores, princípios éticos compartilhados para defender e priorizar o interesse público sobre os interesses privados no setor público.

4.4.17.5 Desse modo, no INSS, a integridade é componente fundamental da boa governança que busca direcionar condutas, valores, princípios e normas na construção de ambientes cada vez mais transparentes, éticos e íntegros.

4.4.17.6 A partir desse entendimento, elencamos alguns tipos de riscos para a integridade mais relevantes e comuns nas organizações públicas, conforme exposto a seguir:

I - fraude: quaisquer atos ilegais caracterizados por desonestidade, dissimulação ou quebra de confiança. Estes atos não implicam o uso de ameaça de violência física ou de força física;

II - abuso de posição ou poder em favor de interesses privados: conduta contrária ao interesse público, valendo-se da sua condição para atender interesse privado, em benefício próprio ou de terceiros;

III - nepotismo: o nepotismo pode ser entendido como uma das formas de abuso de posição ou poder em favor de interesses privados, em que se favorecem familiares, nos termos da Súmula Vinculante nº 13 do Supremo Tribunal Federal;

IV - conflito de interesses: de acordo com a Lei nº 12.813, de 16 de maio de 2013, conflito de interesses trata da situação gerada pelo confronto entre interesses públicos e privados, que possa comprometer o interesse coletivo ou influenciar, de maneira imprópria, o desempenho da função pública;

V - pressão interna ou externa ilegal ou antiética para influenciar agente público: pressões explícitas ou implícitas de natureza hierárquica (interna), de colegas de trabalho (organizacional), política ou social (externa), que podem influenciar indevidamente atuação do agente público;

VI - solicitação ou recebimento de vantagem indevida: caracteriza-se por qualquer tipo de enriquecimento ilícito, seja dinheiro ou outra utilidade, dado que ao agente público não se permite colher vantagens em virtude do exercício de suas atividades;

VII - utilização de recursos públicos em favor de interesses privados: algumas das formas de utilização de verbas e fundos públicos em favor de interesses privados são:

a) apropriação indevida;

b) irregularidades em contratações públicas; e

c) outras formas de utilização de recursos públicos para uso privado (ex.: carros, tempo de trabalho, equipamentos do escritório etc.).

4.4.17.7 Ressalta-se que os riscos associados à integridade apurados durante o processo de gerenciamento de riscos das unidades institucionais, contribuirão para a elaboração e aprimoramento do código de ética e do Plano de Integridade, conforme disposto no Programa de Integridade do INSS e terão monitoramento diferenciado, uma vez que o conceito de integridade, não se limita apenas a evitar práticas corruptas, mas abrange a promoção de uma abordagem ética em todas as ações e decisões, garantindo que os processos sejam justos e que a confiança pública seja mantida.

4.5 Análise e Avaliação de Riscos

4.5.1 É o processo que estima o nível do risco, considerando a probabilidade e o impacto, e que compara o nível com critérios, a fim de determinar se o risco exige tratamento e outras providências, como o escalamento às instâncias decisórias superiores.

4.5.2 Análise, na fase de análise, após levantamento e identificação dos eventos de riscos, busca-se desenvolver sua compreensão, a observação das correspondentes fontes de risco, suas causas e consequências, medindo a probabilidade de ocorrência do evento de risco e em termos da magnitude do impacto sobre os objetivos. Leva-se também em consideração a presença ou não de quaisquer controles existentes e sua eficácia (Risco Inerente – Risco Residual).

4.5.3 Trata-se da realização da estimativa, do registro e classificação da probabilidade e impacto, para as especificações de riscos feitas na etapa de identificação.

4.5.4 Dependendo das circunstâncias, a análise de riscos pode ser qualitativa, semiquantitativa ou quantitativa, ou, ainda, uma combinação destas, e ser mais ou menos detalhada. A avaliação qualitativa define consequência, probabilidade e nível de risco por níveis de significância, tais como "alto", "médio" e ``baixo", pode combinar consequência e probabilidade, e avalia o nível de risco resultante em comparação com os critérios qualitativos (ABNT, 2009).

4.5.5 Os métodos semiquantitativos utilizam escalas de classificação numérica para consequência e probabilidade de forma combinada. As escalas podem ser lineares ou logarítmicas, ou podem ter alguma outra relação; as fórmulas utilizadas também podem variar (ABNT, 2009).

4.5.6 Do outro lado, temos o método quantitativo, que segue uma abordagem dedutiva. Nesse método, os riscos são avaliados com base em dados numéricos, probabilidades e análises estatísticas. Ele fornece uma avaliação mais precisa da probabilidade e do impacto dos riscos.

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

4.5.7.1 Mesmo onde uma completa quantificação tenha sido conduzida, é preciso reconhecer que os níveis de risco calculado são estimativos. A colaboração entre métodos qualitativos e quantitativos na avaliação de riscos ajuda a mitigar o impacto de divergências de opiniões e vieses, resultando em decisões mais informadas e eficazes na gestão de riscos.

4.5.8 A partir dessas informações, pode-se determinar o nível de cada risco, a fim de permitir a geração da matriz de riscos, realizando-se o enquadramento do risco nas faixas da matriz e o cálculo do índice do risco para o processo analisado. A análise fornece uma entrada para a avaliação de riscos e para as decisões sobre a necessidade de os riscos serem tratados.

4.5.9 Em sua forma qualitativa mais simples, a relação entre o nível de risco e as variáveis que o compõe pode ser ilustrada por meio de uma matriz como a que segue (Gestão de Riscos - Avaliação da Maturidade):

4.5.10 Identificação e Avaliação dos Controles Internos de Gestão.

4.5.10.1 Os controles internos de gestão, conceituados pela Instrução Normativa Conjunta nº 1/2016/MPOG/CGU, de 2016, como um conjunto de regras, procedimentos, diretrizes, protocolos, rotinas de sistemas informatizados, conferências e trâmites de documentos e informações, entre outros, operacionalizados de forma integrada, destinados a enfrentar os riscos e fornecer segurança razoável de que os objetivos organizacionais serão alcançados.

4.5.10.2 As atividades de controles internos, implementadas de forma manual ou automatizada, são atividades materiais e formais, como políticas, procedimentos, técnicas e ferramentas que desempenham um papel fundamental no funcionamento eficaz e eficiente de uma organização, tais como, mitigação de riscos, melhoria da eficiência operacional, garantia de conformidade regulatória e tomada de decisão informada.

4.5.11 Tipos de Controles:

4.5.11.1 Controles preventivos: são os projetados para detectar erros, falhas, desperdícios ou irregularidades, antes da operacionalização de um processo (atividades), permitindo a adoção de medidas

tempestivas de correção.

4.5.11.2 Controles Atenuadores e Recuperação: são os projetados para detectar erros, falhas, desperdícios ou irregularidades, após a operacionalização de um processo (atividades). Eles são implementados para reduzir ou mitigar a probabilidade de ocorrência de um evento de risco ou para minimizar a consequência, caso ocorra.

4.5.11.3 Controles detectivos: são os projetados para detectar erros, falhas, desperdícios ou irregularidades, durante a operacionalização de um processo.

4.5.11.4 A avaliação desses controles, envolve a verificação da eficácia dos controles existentes e a determinação se são adequados para "suportarem" os riscos identificados. O objetivo é determinar se os controles são capazes de reduzir o risco a um nível aceitável.

4.5.12 Categorias - Desenho e Operação

4.5.12.1 Os controles de gestão são essenciais para garantir que os objetivos organizacionais sejam alcançados de maneira eficiente e eficaz. Eles são divididos em duas categorias principais: desenho (*design*) e operação (*Operating Controls*).

4.5.12.2 Na categoria desenho, pressupõe planejamento estratégico, estrutura organizacional, políticas e procedimentos operacionais, gestão de riscos, com os controles preventivos e detectivos, controle da informação, protegendo os dados e sistemas de informação contra acessos não autorizados, alterações indevidas e indisponibilidades.

4.5.12.3 Por outro lado, quanto à operação, pressupõe a execução de planos e políticas, com implementação de estratégicas em conformidade também com o planejamento estratégico e monitoramento de desempenho desses mesmos objetivos.

4.5.12.4 Desse modo, os componentes de controles internos de gestão definem o enfoque recomendável para a estrutura de controles internos e fornecem bases para sua avaliação, sendo os mesmos aplicados a todos os aspectos operacionais de cada organização.

4.5.12.5 Considerando-se todas as informações acima e as ferramentas disponibilizadas, o gestor de riscos deverá avaliar os controles existentes que mitigarão os riscos identificados.

4.5.13 Escala de probabilidade

4.5.13.1 Define como a probabilidade de um evento ocorrerá e será medida, analisando as causas ou o evento de risco considerando aspectos como, por exemplo, a frequência observada ou esperada.

4.5.13.2 A Probabilidade (P) é pontuada de 1 a 5, conforme tabela abaixo:

4.5.14 Escala de impacto

4.5.14.1 Define como o impacto será mensurado, em função da análise das consequências de um evento de risco com relação às dimensões (custo, prazo, escopo e qualidade) no caso de projetos/processos/iniciativa, e com relação à severidade que avalia o comprometimento do desempenho, confiabilidade ou qualidade do processo de trabalho ou do serviço provido tanto para o público interno ou externo. É importante lembrar que o termo impacto, deverá ser considerada como sinônimo de consequência.

4.5.14.2 O Impacto (I) é pontuado de 1 a 5, conforme demonstra a tabela abaixo:

4.5.15 Escala de Nível de risco

Define o grau de risco para avaliação da intensidade dos quais (riscos) uma instituição está

exposta.

Escala de Nível de Risco	
Níveis	Pontuação
RC - RISCO CRÍTICO	13 a 25
RA - RISCO ALTO	7 a 12
RM - RISCO MODERADO	4 a 6
RP - RISCO PEQUENO	1 a 3

4.5.16 Impacto – Fatores para análise

Amplia a compreensão das consequências relacionadas aos efeitos do evento de risco, fornecendo diretrizes adicionais para avaliar o impacto. Isso deverá ser feito, levando em consideração os critérios definidos pela gestão, juntamente com os pesos associados a esses critérios, conforme indicado na métrica apresentada:

Impacto - Fatores para Análise							
	Estratégico-Operacional					Econômico-Financeiro	Peso
	Esforço de Gestão	Regulação	Reputação	Negócios/ Serviços à Sociedade	Intervenção Hierárquica	Orçamentário	
Orientações para atribuição de pesos	Evento com potencial para levar o negócio ou serviço ao colapso	Determina interrupção das atividades	Com destaque na mídia nacional e internacional, podendo atingir os objetivos estratégicos e a missão	Prejudica o alcance da missão do INSS	Exigiria a intervenção do CEGOV	> = 25%	5-Catastrófico
	Evento crítico, mas que com a devida gestão pode ser suportado	Determina ações de caráter pecuniários (multas)	Com algum destaque na mídia nacional, provocando exposição significativa	Prejudica o alcance da missão da Unidade	Exigiria a intervenção do Presidente	> = 10% < 25%	4-Grande
	Evento significativo que pode ser gerenciado em circunstâncias normais	Determina ações de caráter corretivo	Pode chegar à mídia provocando a exposição por um curto período de tempo	Prejudica o alcance dos objetivos estratégicos	Exigiria a intervenção do Diretor	> = 3% < 10%	3-Moderado
	Evento cujas consequências podem ser absorvidas, mas carecem de esforço da gestão para minimizar o impacto	Determina ações de caráter orientativo	Tende a limitar-se às partes envolvidas	Prejudica o alcance das metas do processo	Exigiria a intervenção do Coordenador	> = 1% < 3%	2-Pequeno
	Evento cujo impacto pode ser absorvido por meio de atividades normais	Pouco ou nenhum impacto	Impacto apenas interno / sem impacto	Pouco ou nenhum impacto nas metas	Seria alcançada no funcionamento normal da atividade	< 1%	1-Insignificante

4.5.17 Escala de probabilidade - Frequência observada/esperada

Com vista a proporcionar uma visão abrangente sobre o evento de risco, esta escala define a probabilidade em termos percentuais, representando a chance de um evento de risco ocorrer, variando de muito baixa a muito alta, quando combinada com a escala de impacto.

Probabilidade					
Aspectos Avaliativos	Evento pode ocorrer apenas em circunstâncias excepcionais	Evento pode ocorrer em algum momento	Evento deve ocorrer em algum momento	Evento provavelmente ocorra na maioria das circunstâncias	Evento esperado que ocorra na maioria das circunstâncias
Frequência Observada/Esperada	Muito baixa (< 10%)	Baixa (>=10% <= 30%)	Média (>=30% <= 50%)	Alta (>=50% <= 90%)	Muito alta (>90%)
Peso	1	2	3	4	5

4.5.18 Descrição do Nível de Risco

DESCRIÇÃO DO NÍVEL DE RISCO

A descrição do nível de risco é fundamental para categorizar a gravidade dos riscos identificados. Os níveis tumam ser definidos da seguinte forma:

Risco Crítico	Nível de risco muito alem do apetite a risco. Indica que nenhuma opção de resposta foi identificada para reduzir a probabilidade e o impacto a nível aceitável
Risco Alto	Nível de risco além do apetite a riscos. Indica que o risco residual será reduzido a um nível compatível com a tolerância a riscos
Risco Moderado	Nível de risco dentro do apetite a risco. Indica que o risco residual requer atividades de monitoramento específicas, visando a manutenção de resposta e controles para manter o risco neste nível ou reduzi-lo sem custos adicionais.
Risco Pequeno	Nível de risco dentro do apetite a risco. Indica que o risco inerente já está dentro da tolerância a risco

A seguir podemos ver a Matriz de Risco composta por todos os elementos apresentados, ou seja, as escalas de probabilidade e impacto com os correspondentes níveis de risco.

4.5.19 Avaliação

4.5.19.1 Nessa fase é feita a comparação dos níveis estimados de risco, que foram encontrados durante a etapa de análise, com os critérios de risco definidos quando o contexto foi estabelecido, a fim de determinar a significância do nível e do tipo de risco.

4.5.19.2 Chega-se à compreensão do risco, obtida durante a análise de riscos, para tomar decisões sobre as ações futuras. A finalidade da avaliação de riscos é auxiliar na tomada de decisões com base nos resultados da análise, sobre quais riscos necessitam de tratamento e a prioridade para a implementação do tratamento. Envolve comparar o nível de risco com os critérios de risco estabelecidos quando o contexto foi considerado, para determinar se o risco e ou sua magnitude é aceitável ou tolerável ou se algum tratamento é exigido (ABNT, 2009).

4.5.20 Apetite a Risco do INSS - Declaração

4.5.20.1 O apetite a riscos reflete o nível de risco, grau máximo de exposição, e tipos de riscos (financeiros, operacionais, estratégicos, integridade, imagem/reputação entre outros) que a instituição está disposta aceitar em suas atividades, projetos, iniciativas, e tem como propósito final, alcançar os objetivos estratégicos da Instituição.

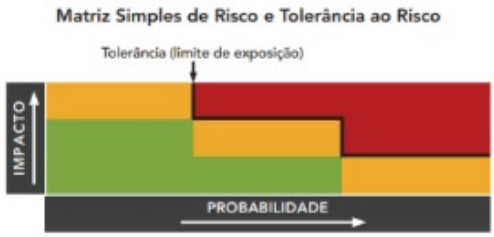


Figura 5: Matriz de avaliação dos riscos (UK Orange Book 2004 – traduzido e adaptado)

4.5.20.2 Esta declaração não apenas orienta as decisões em relação aos riscos, mas também facilita a comunicação interna e externa sobre a abordagem do INSS ao risco. É indispensável revisar e atualizar, periodicamente, o apetite a risco da instituição para assegurar que esta diretriz continue alinhada com os objetivos e a realidade operacional dos processos organizacionais.

4.5.20.3 O nível de Apetite a Riscos definido neste documento, considerando os objetivos estratégicos e o conceito preceituado nesta metodologia, é compatível com a natureza e a complexidade das nossas atividades e considerou os seguintes aspectos ao limitar seu apetite a risco em Moderado:

I - as categorias de riscos e os respectivos níveis que a instituição está disposta a assumir;

II - a capacidade e maturidade da instituição de gerenciar riscos de forma efetiva e prudente;

III - os objetivos estratégicos da instituição;

IV - o ambiente regulatório em que a instituição atua;

V - cultura organizacional; e

VI - comunicação e transparência.

4.5.20.4 Por conseguinte, foram estabelecidos os parâmetros, associados aos níveis de riscos, para a priorização e tratamento constantes na tabela abaixo:

TABELA APETITE A RISCOS – TRATAMENTO POR NÍVEL DE RISCO

Nível de Risco	**Critério para priorização e tratamento de risco**	**Comunicação**	**Tratamento do risco (Recomendação**	**Tempo para iniciar a ação de controles**	**Instância/Autoridade responsável pela postergação da Implementação Controle**

Crítico (13 a 25)	Nível de risco residual muito além do Apetite a Riscos; tem elevada probabilidade de impactar a capacidade de atingir a missão/objetivos estratégicos. Os controles podem ser inadequadamente projetados ou ineficazes. Risco inaceitável. Tem alta probabilidade de ocorrência e poderá resultar em impacto extremamente severo, caso ocorram.	Autoridade Máxima da Área responsável pelo objeto de gestão, DIGOV/CEGOV;	Evitar ou Mitigar; exigem a implementação imediata de estratégias de proteção e prevenção – ação imediata;	1 a 3 meses	Dirigente máximo do órgão ou unidade descentralizada.
Alto (7 a 12)	Nível de risco residual além do apetite a riscos, com probabilidade de impactar a capacidade de atingir a missão/objetivos estratégicos. Os controles podem ser inadequadamente projetados ou ineficazes. Risco inaceitável. Seu grau de probabilidade pode variar de muito baixo, mas com alto impacto, ou alta probabilidade de ocorrer, mas com baixo impacto.	Autoridade Máxima da Área responsável pelo objeto de gestão e DIGOV; Riscos de Integridade e Estratégico ao DIGOV/CEGOV	Mitigar Compartilhar ou Transferir; as ações podem ser implementadas com mais planejamento e tempo – ação de curto e médio prazo;	3 a 6 meses	Dirigente da unidade administrativa abaixo da autoridade máxima do órgão ou unidade descentralizada

Moderado (4 a 6)	Nível de risco residual dentro do apetite a riscos, podendo atrasar ou interromper a realização da missão/objetivos estratégicos. Os controles podem ser adequadamente projetados e geralmente são efetivos. Representam os riscos com consequências gerenciáveis à Autarquia.	Autoridade Máxima da Área responsável pelo objeto de gestão e DIGOV; Riscos de Integridade e Estratégico ao CEGOV	Aceitar o risco, estes riscos somente devem ser tratados caso os benefícios gerados pela sua mitigação sejam superiores aos custos de implementação de controles – risco tolerável.	Gestão de rotina dos controles existentes e do alcance dos objetivos; acompanhar as mudanças de contexto.	N/A
Pequeno (1 a 3)	Nível de risco residual dentro do Apetite a Riscos, não impedirá substancialmente a capacidade de alcançar a missão/objetivos estratégicos. Os controles podem ser prudentemente projetados e eficazes. Possuem baixa probabilidade e pequeno impacto, representando pequenos problemas e prejuízos.	Autoridade Máxima da Área responsável pelo objeto de gestão e DIGOV; Riscos de Integridade e Estratégico ao CEGOV	Aceitar o risco, estes riscos somente devem ser tratados caso os benefícios gerados pela sua mitigação sejam superiores aos custos de implementação de controles – risco tolerável.	Gestão de rotina dos controles existentes e do alcance dos objetivos; acompanhar as mudanças de contexto.	N/A.

* Todos os riscos de Integridade e Estratégicos, independentemente do nível, deverão ser comunicados, de forma imediata, à DIGOV que comunicará ao CEGOV.

4.5.20.5 Assim sendo, todos os riscos cujos níveis estejam dentro da (s) faixa (s) de apetite a risco:

I - podem ser aceitos, sem que seja implementada medida de tratamento, mas com a necessidade de acompanhamento; e

II - deverão ser tratados e monitorados, de forma que seja reduzido a um nível compatível com a tolerância a riscos.

4.5.20.6 Quanto maior a probabilidade e o impacto, maior será o nível do risco residual, conforme apresentado na Matriz de Classificação de Riscos.

4.5.20.7 O processo de avaliação de riscos tenta responder às seguintes questões fundamentais:

I - o que pode acontecer e suas causas?

II - quais são as consequências?

III - qual é a probabilidade da ocorrência do evento de risco?

IV - qual é o impacto do evento de risco, no caso dele se materializar?

V - quais são as ações que podem mitigar as consequências do evento de risco?

VI - o nível de risco é tolerável ou aceitável e requer tratamento adicional?

4.6 Tratamento do Risco

4.6.1 A fase de tratamento compreende o planejamento e a realização de ações para modificar o nível do risco. Fundamenta-se na emissão de planos de tratamento de riscos com a finalidade de definir e documentar como as opções de tratamento escolhidas serão implementadas.

4.6.2 O objetivo é documentar todo o processo de implementação por meio de planos de tratamento, registrando as informações de justificativa, providências, responsáveis, cronogramas, dentre outras. Reflete a decisão de implementar ações de tratamento e, portanto, envolve informações relativas a prazos, metas, custos, resultados, providências e responsabilidades.

4.6.3 Constitui-se ainda em selecionar e acordar uma ou mais opções pertinentes para modificar os riscos e seus efeitos, ou ambos, e a implementação de ações para tratá-los.

4.6.4 O tratamento dos riscos deve seguir os seguintes passos:

- identificar as **causas e consequências** dos riscos priorizados;
- levantadas as causas e consequências, registrar as **possíveis medidas de resposta ao risco**;
- avaliar a **viabilidade da implantação dessas medidas** (custo-benefício, viabilidade técnica, tempestividade, efeitos colaterais do tratamento etc.);
- **decidir quais serão implementadas**;
- elaborar **plano de implementação** das medidas para inclusão nos planos institucionais.

4.6.5 Resposta ao Risco

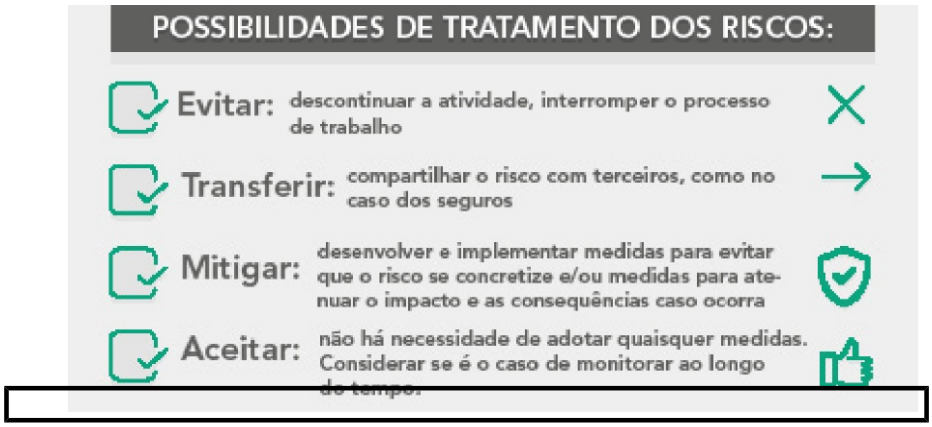
4.6.5.1 De acordo com o nível de riscos, deverá ser escolhida a forma de tratamento:

I - aceitar o risco: aceitar ou tolerar o evento de risco sem que nenhuma ação específica seja tomada, pois ou o nível do risco é considerado baixo ou a capacidade da organização para tratar o risco é limitada ou o custo é desproporcional ao benefício;

II - transferir o risco: compartilhar ou transferir uma parte do evento de risco a terceiros;

III - mitigar o risco: reduzir o impacto ou a probabilidade de ocorrência do evento de risco; e

IV - evitar o risco: ação para evitar totalmente o evento de risco.



4.6.5.2 Selecionar a opção mais adequada envolve equilibrar, de um lado, os custos e esforços de implementação e, de outro, os benefícios decorrentes.

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

Orientações que constituem em medidas de Tratamentos de Riscos:

Nível de Risco	Descrição do Nível de Risco	Parâmetro de Análise para Adoção de Resposta	Tipo de Resposta	Ação de Controle
Risco Crítico	Indica que nenhuma opção de resposta foi identificada para reduzir a probabilidade e o impacto a nível aceitável	Custo desproporcional; capacidade limitada diante do risco identificado	Evitar	Promover ações que evitem/eliminem as causas e/ou efeitos
Risco Alto	Indica que o risco residual será reduzido a um nível compatível com a tolerância a riscos	Nem todos os riscos podem ser transferidos. Ex.: Risco de Imagem, Risco de Reputação	Mitigar	Adotar medidas para reduzir a probabilidade ou impacto dos riscos, ou ambos
Risco Moderado	Indica que o risco residual será reduzido a um nível compatível com a tolerância a riscos	Reduzir probabilidade ou impacto, ou ambos	Transferir	Reduzir a probabilidade ou impacto pela transferência ou compartilhamento de uma parte do risco (seguro, transações de hedge ou terceirização da atividade
Risco Pequeno	Indica que o risco inerente já está dentro da tolerância a risco	Verificar a possibilidade de retirar controles considerados desnecessários	Aceitar	Conviver com o evento de risco mantendo práticas e procedimentos existentes

4.6.5.4 Os gestores devem registrar e acompanhar as informações das ações de tratamento. Uma vez implementada, o tratamento fornece novos controles ou modifica os existentes. Os tomadores de decisão e outras partes interessadas devem estar cientes da natureza e da extensão do risco residual após o tratamento do risco.

4.6.5.5 É importante que se tenha consciência que sempre existirá algum nível de risco residual, não somente porque os recursos são limitados, mas também em decorrência da incerteza e das limitações inerentes a todas as atividades de uma organização.

4.6.6 Ferramenta de melhorias e respostas a riscos

4.6.6.1 Algumas ferramentas poderão ser utilizadas para ampliar a visão sobre possíveis causas de um problema ou riscos. Para fins dessa metodologia, sugerimos a utilização da técnica de 5W2H.

4.6.6.2 A proposta de melhorias ou respostas, a partir da 5W2H, direciona as perguntas às causas

fundamentais dos eventos de riscos, no sentido de se encontrar maneiras de reduzir ou mitigar suas causas e impactos, a saber:

What/O quê? – Deve-se analisar o que é feito e o que é consumido nas atividades afetadas pelas causas fundamentais do risco. O que pode ser alterado em relação aos objetos dessas atividades no sentido de mitigar a causa do problema?

Who/Quem? – Deve-se analisar quem são os responsáveis pelo planejamento, execução e avaliação das atividades cuja causa em questão afeta.

When/Quando? – Deve-se analisar o momento em que as atividades são executadas frente às necessidades da sociedade. O que pode ser alterado em relação ao momento de realização das tarefas no sentido de mitigar a causa?

*Why/*Por quê? – Por que o processo segue essa rotina? Por que a solução proposta deve ser implementada?

Where/Onde? – Qual o local em que as atividades são executadas? O que pode ser alterado em relação ao local de realização das tarefas no sentido de mitigar a causa?

How/Como? – Como a atividade é planejada, executada e avaliada? O que pode ser alterado em relação à maneira em que as tarefas são realizadas no sentido de mitigar a causa? Por outro lado, como será implementada a solução proposta?

How Much/Quanto? – Qual o custo das atividades? Que alterações podem ser propostas relacionadas ao custo, no sentido de mitigar as causas? Por outro lado, quanto vai custar a implementação/alteração proposta para as atividades?

5W					2H		
WHAT (O QUE)	WHY (POR QUE)	WHERE (ONDE)	WHO (QUEM)	WHEN (QUANDO)	HOW (COMO)	HOW MUCH (QUANTO CUSTA)	STATUS
O QUE SERÁ FEITO? QUAL É O SEU OBJETIVO? COMO DESCREVER O MELHOR QUE PODE OBTER NESTA SITUAÇÃO?	POR QUE SERÁ FEITO? QUAL É A RAZÃO QUE MOTIVA ESSA AÇÃO? O QUE VAI CONSEGUIR DE RETORNO? FAZ PARTE DE SUA MISSÃO? VALE A PENA?	ONDE SERÁ FEITO?	POR QUEM SERÁ FEITO? QUEM ESTÁ ENVOLVIDO OU É RESPONSÁVEL EM CADA AÇÃO? QUEM DEVE SER AVISADO?	QUANDO SERÁ FEITO? QUAIS SÃO AS PRIMEIRAS AÇÕES NECESSÁRIAS? ESSAS AÇÕES SÃO PROATIVAS OU DEPENDEM DE OUTRAS FORA DO SEU CONTROLE?	COMO SERÁ FEITO? COMO INICIAR, MENSURAR E ATIVAR AS AÇÕES NECESSÁRIAS? QUAIS SÃO AS SOLUÇÕES DE CONTINGÊNGIA, NO CASO DE ENCONTRAR OBSTÁCULOS? O QUE SINALIZARÁ QUE É O MOMENTO DE AGIR ASSIM?	QUANTO CUSTARÁ FAZER? QUANTO CUSTARÁ EM TEMPO, ESFORÇO, DINHEIRO, CONHECIMENTO, PREPARAÇÃO PSICOLÓGICA E NEGOCIAÇÃO OU MOTIVAÇÃO PESSOAL E DE GRUPO?	

4.6.6.3 Diante do exposto, percebe-se que os aspectos fundamentais para administrar um plano de ação estão contemplados por meio do 5W2H, onde os elementos formadores desse acróstico são indispensáveis para coordenar uma ou mais ações. Por isso, sua adoção, por gestores de riscos.

4.6.6.4 Nesta etapa convém o estabelecimento dos indicadores Chave de Risco com vistas ao acompanhamento da dinâmica do evento de riscos.

4.6.7 Indicadores para a Gestão de Riscos

4.6.7.1 Os objetivos estratégicos de uma instituição estão intrinsecamente relacionados ao estabelecimento de indicadores de desempenho, sobre os quais são definidas as metas a serem alcançadas.

4.6.7.2 Indicadores de desempenho na gestão de riscos são métricas cruciais para avaliar a eficácia das estratégias de mitigação e controle de riscos dentro de uma organização. Conforme previsto na Política de Gestão de Riscos do INSS, compete a DIGOV propor ao CEGOV os indicadores de desempenho para a gestão de riscos.

4.6.7.3 Conceitualmente, indicadores são medidas de ordem quantitativa ou qualitativa, dotada de significado particular e utilizada para organizar e captar as informações relevantes dos elementos que compõem o objeto da observação. É um recurso metodológico que informa empiricamente sobre a evolução do aspecto observado (Guia de Gestão de Riscos do Ministério da Economia, 2021). Na gestão de riscos podem ser adotados indicadores tradicionais, destinados a mensurar o desempenho pregresso em relação à gestão de riscos, como por exemplo:

I - frequência de materialização do risco;

II - tempo de tratamento;

III - severidade dos impactos; e

IV - percentual dos processos de trabalho do INSS, já com gestão de riscos.

4.6.7.4 É importante destacar que os exemplos citados nessa metodologia se configuram com um rol exemplificativo de indiciadores, não taxativo.

4.6.7.5 Antes de começar o processo de construção de indicadores, a equipe deve pesquisar a existência de indicadores aceitos entre profissionais e especialistas. Deve também pesquisar os indicadores possíveis de serem calculados, levando em consideração a disponibilidade de dados, nos sistemas, relatórios e outras fontes de informações.

4.6.7.6 Conforme o gerenciamento de riscos avance sobre os processos de trabalho, é possível delimitar indicadores-chaves de risco (ICR), os quais se prestam a orientar, principalmente, a antecipação em face de riscos operacionais que estão na iminência de se materializar, com ênfase no futuro.

4.6.7.7 Os ICR’s são usados para monitorar as variações no desempenho em relação à meta para o cumprimento de objetivos estratégicos e operacionais relevantes para o INSS, além de alertarem os gestores sobre a necessidade de tomar ações corretivas de forma diligente. A ABNT (2009) recomenda que as organizações monitorem e analisem crítica e periodicamente os indicadores de riscos, de forma a garantir sua adequação.

4.7 Comunicação e Consulta

4.7.1 Refere-se à identificação das partes interessadas em objetos de gestão de riscos e obtenção, fornecimento ou compartilhamento de informações relativas à gestão de riscos sobre tais objetos, observada a classificação da informação quanto ao sigilo. É importante que a comunicação ocorra de forma vertical e horizontal.

4.7.2 A comunicação vertical ocorre no sentido da base para a cúpula ou vice-versa, proporcionando que a cúpula da organização seja informada das atividades associadas aos controles dos riscos-chave e dando-lhe a oportunidade de avocar casos concretos não relacionados a esses riscos, atribuídos a instâncias inferiores.

4.7.3 É de suma importância que todos os servidores e colaboradores conheçam os riscos do processo de trabalho na sua respectiva área de atuação.

4.7.4 Por sua vez, a comunicação horizontal é importante para que os riscos de um processo que envolva diferentes unidades, às vezes, sejam conhecidos igualmente por todos os que trabalham nesse processo (Manual de Gestão de Risco, TCU - adaptado).

4.7.5 Ainda, deverá possuir qualidade contextual e de representação com base nos critérios a seguir:

I - relevância: a informação deve ser útil para o objetivo do trabalho;

II - integralidade: as informações importantes e suficientes para a compreensão devem estar presentes;

III - adequação: volume de informação adequado e suficiente;

IV - concisão: informação deve ser apresentada de forma compacta;

V - consistência: as informações apresentadas devem ser compatíveis;

VI - clareza: informação deve ser facilmente compreensível; e

VII - padronização: informação deve ser apresentada no padrão aceitável.

4.7.6 A comunicação perpassará todas as instâncias envolvidas, de forma a inter-relacionar a coleta e disseminação de informações e iniciativas entre as partes interessadas, proporcionando a interação e compreensão suficiente dos dados necessários a cada decisão.

4.7.7 Este processo de interação deverá garantir que as informações sejam confiáveis, íntegras e tempestivas assegurando a eficiência da gestão, considerando os itens abaixo que serão implementados pela DIGOV:

I - plano de comunicação e consulta;

II - registro das ocorrências dos riscos; e

III - relatórios gerenciais de riscos.

4.7.8 Considerando os critérios acima, a DIGOV implementou os seguintes relatórios gerenciais:

I - Relatório de Comunicação de Riscos – RCR, ferramenta de comunicação dos riscos mapeados no Processo de Gerenciamento de Riscos, a cargo do CSGR, visando comunicar à autoridade máxima da área responsável pelo objeto de gestão e a Diretoria de Governança, Integridade e Inovação - DIGOV, o resultado do mapeamento dos riscos do objeto de gestão; e

II - Relatório de Risco Residual – RRR, a cargo do Gestor de Risco, consolida e documenta os riscos que permanecerão após a implementação das estratégias de tratamento e fornecerá informações para a tomada de decisões, melhorias contínuas e aprimoramento das práticas de gerenciamento de riscos.

4.8 Monitoramento

4.8.1 Compreende o acompanhamento e a verificação contínua do desempenho ou da situação de elementos da gestão de riscos.

4.8.2 A fase de monitoramento inclui tanto o acompanhamento da execução dos planos de ação das melhorias priorizadas, quanto à evolução dos indicadores do processo, elaborados ou revisados, após a identificação de problemas/riscos, monitorados a partir de então. Além de ser o momento de identificar novos riscos, analisar a eficiência dos processos instaurados e implementar as ações corretivas necessárias após a análise.

4.8.3 Trata-se do acompanhamento e da análise crítica da evolução do gerenciamento dos riscos, dos planos de tratamento de riscos, dos processos de gerenciamento de riscos e das operações realizadas no sistema e notificação dos responsáveis. O objetivo é proporcionar uma vigilância contínua sobre todo o processo de gerenciamento de riscos, etapa essencial e uma das mais importantes do ponto de vista da organização, onde os dados a serem monitorados passam a refinar o processo de avaliação de riscos, de modo que possa ser atualizado quando necessário. Importante ressaltar que nessa etapa, as responsabilidades relativas ao monitoramento e à análise crítica sejam claramente definidas (ABNT, 2009).

4.8.4 O monitoramento, no âmbito do processo de gerenciamento de riscos, deve ser realizado, principalmente, pela unidade responsável pelo processo organizacional e tem três dimensões importantes que deverão ser consideradas (Manual de Gestão de Risco, TCU - adaptado):

I - o funcionamento do Sistema de Gestão de Riscos do INSS;

II - a implementação e os resultados do tratamento de riscos propostos no Plano de Ação; e

III - a evolução do nível dos riscos, identificados e analisados, sofrerem mudanças e alterações que sejam necessários tratamento por parte do gestor, além da possibilidade de reavaliar os riscos.

4.8.5 O processo de tratamento de riscos traz em si um caráter de seriedade, rigor e profissionalismo para a resposta às ameaças, pois reduz os prejuízos organizacionais, identifica oportunidades, otimiza capital e administra múltiplos riscos.

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

I - confrontação de informações oriundas de fontes diversas;

II - identificação de comportamentos fora do padrão; e

III - variações cujos percentuais não estejam dentro dos limites estabelecidos.

4.8.7 São elementos essenciais nessa etapa os Indicadores-Chave de Riscos - ICR, na forma de medidas ou métricas em relação a um referencial definido, que sinalizam a exposição aos riscos, cabendo aos Gestores de Riscos monitorarem o nível de risco de sua área e o impacto em toda a unidade setorial.

4.8.8 Os ICR são utilizados para alertar os gestores da necessidade de tomada tempestiva de ações corretivas. O monitoramento por ICR tem a finalidade de acompanhar a eficácia dos controles e a manutenção dos riscos em níveis aceitáveis, observado o apetite de risco da instituição.

4.8.9 O ICR poderá ser estabelecido na etapa de tratamento de riscos. Registre-se que as técnicas/ferramentas indicadas para o processo de avaliação de riscos não são de uso obrigatório, podendo ser utilizadas outras técnicas/ferramentas, de acordo com o tipo de objeto de gestão, habilidade e aptidão do servidor. Recomenda-se adotar as técnicas/ferramentas constantes da Norma ABNT ISO/IEC 31010:2021.

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

4.8.11 Após a etapa de tratamento, do ciclo do processo de gerenciamento de riscos, os processos gerenciados serão revisados na periodicidade de até um ano, a fim de aprimorá-lo pelo aprendizado, corrigir eventuais falhas quanto à conformidade com as normas, controles internos deficientes, novos riscos não mapeados e riscos que perderam sua relevância de forma a aperfeiçoar a gestão.

4.8.12 O monitoramento de riscos e controles, no âmbito dos processos organizacionais do INSS, será realizado em sintonia com os princípios das “Três Linhas”, conforme descrito na tabela abaixo, em conformidade com as atribuições e responsabilidades preconizadas na Política de Gestão de Riscos do INSS:

Monitoramento e Efetividade dos Controles	
1ª linha - Gestores de risco	Garantir que os controles sejam eficazes e eficientes; implementar e acompanhar indicadores; analisar as ocorrências dos riscos; detectar mudanças que possam requerer revisão dos controles ou do Plano de Tratamento de Gerenciamento de Riscos; e identificar os riscos emergentes e comunicá-los imediatamente.
2ª linha - DIGOV	Supervisionar e gerir as operações contínuas da Autarquia, garantindo que os controles internos estejam fortalecidos contra ações irregulares, antiéticas, antieconômicas, ineficientes e ineficazes, consolidando os resultados das diversas áreas em relatórios gerenciais.

3ª linha - Auditoria	Avaliar, por meio de instrumentos e metodologia própria, a implantação, eficiência e efetividade dos controles definidos no Plano de Tratamento dos Riscos.

4.9 Melhoria contínua

4.9.1 Compreende o aperfeiçoamento ou ajuste de aspectos da gestão de riscos avaliados no monitoramento.

4.9.2 Segundo o Manual do TCU, a melhoria contínua pode ser entendida em duas dimensões:

I - a primeira está atrelada ao próprio Sistema de Gestão de Riscos do INSS, a cargo da DIGOV; e

II - a segunda, relacionada aos resultados do monitoramento sobre a efetividade do tratamento do risco, a cargo dos gestores de risco.

4.9.3 Considerando a interatividade e dinamismo do processo de gestão de riscos, ainda, a necessidade de controle e avaliação dos resultados obtidos durante esse processo, essa etapa se torna essencial para retroalimentar todo o sistema de controle, assegurando a assertividade das ações de melhorias.

4.9.4 Recursos para a realização das atividades

4.9.4.1 O Gestor de Risco é o responsável pelo processo organizacional da sua unidade, sendo a autoridade para gerenciar determinado risco da sua área de atuação e deve definir uma equipe para participar das etapas do processo de gerenciamento de riscos.

4.9.4.2 Essa equipe deve ser composta por servidores que conheçam o processo, seus objetivos, contextos, atores envolvidos, resultados e controles já existentes. A referida equipe será assessorada pelo Coordenador Setorial de Gestão de Riscos.

4.9.4.3 Os recursos operacionais e tecnológicos necessários para apoiar a condução das atividades de Gestão de Riscos do INSS foram definidos em manual operacional, publicado pela DIGOV, por meio de Portaria DIGOV/INSS Nº 26, de 4 de junho de 2024.

5. Considerações Finais

5.1 Esta Metodologia foi elaborada com o objetivo de auxiliar na sistematização e padronização do processo de gerenciamento de riscos do INSS.

5.2 O produto desse processo de trabalho oferece mais um mecanismo de auxílio à tomada de decisões pela alta administração e demais servidores, de modo que eventos com potencial impacto negativo, não prejudiquem o atingimento dos objetivos ou metas institucionais.

5.3 A elaboração deste instrumento se orientou nos referenciais teóricos reconhecidos internacionalmente, modelos de gestão COSO, COSO ERM, ISO 31000, ISO 31010, além dos normativos vigentes e aplicáveis, por meio de Decretos, Instruções Normativas, Resoluções e Manuais da CGU, TCU e outros órgãos, captando e sintetizando as melhores práticas, de forma a propiciar a condução no gerenciamento de riscos. Igualmente relevantes as Resoluções do CEGOV quanto ao Sistema de Gerenciamento de Risco e sua Política, implementadas neste Instituto.

6. Referências

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 31000:2009. Gestão de riscos – Princípios e diretrizes. Rio de Janeiro, 2009.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 31010:2021. Gestão de riscos - Técnicas de avaliação de riscos. Rio de Janeiro, 2021.

BRASIL. Agência Nacional de Transportes Aquaviários. Metodologia de Gestão de Riscos e Integridade da ANTAQ. 5. ed. Brasília, DF, outubro de 2023.

BRASIL. Controladoria-Geral da União. Portaria CGU nº 1.089, de 28 de dezembro de 2018. Diário Oficial da União, Brasília, DF, 31 de dezembro de 2018.

BRASIL. Instituto Nacional do Seguro Social. Resolução nº 5/CEGOV/INSS, de 28 de maio de 2020. Institui a Política de Gestão de Riscos do INSS. Diário Oficial da União: seção 1, Brasília, DF, 29 maio 2020.

BRASIL. Instituto Nacional do Seguro Social. Resolução nº 8/CEGOV/INSS, de 29 de junho de 2020. Institui o Programa de Integridade do INSS. Diário Oficial da União: seção 1, Brasília, DF, 30 jun. 2020.

BRASIL. Instituto Nacional do Seguro Social - INSS. Portaria Conjunta DIGOV/DTI/INSS nº 1, de 28 de março de 2023. Institui o Sistema de Gerenciamento de Riscos – SISGR/INSS, como ferramenta oficial para identificação, análise, avaliação, comunicação e acompanhamento dos riscos mapeados no âmbito do INSS. Diário Oficial da União, Brasília, DF, 29 mar. 2023. Seção 1, p. 10.

BRASIL. Instituto Nacional do Seguro Social. Portaria DIGOV/INSS nº 20, de 19 de dezembro de 2023. Aprova o Guia de Referência em Gerenciamento de Processos para o INSS. Boletim de Serviço Eletrônico, Brasília, 22 dez. 2023

BRASIL. Instituto Nacional do Seguro Social - INSS. Portaria DIGOV/INSS nº 24, de 11 de março de 2024. Aprova o Guia do Sistema de Gerenciamento de Riscos – SISGR/INSS. Diário Oficial da União, Brasília, DF, 12 mar. 2024. Seção 1, p. 5.

BRASIL. Instituto Nacional do Seguro Social. Portaria DIGOV/INSS Nº 26, de 04 de junho de 2024. Aprova o Manual de Gerenciamento de Riscos do INSS. Diário Oficial da União, Brasília, DF, 05 jun. 2024. Seção 1, p. 1.

BRASIL. Instrução Normativa Conjunta MP/CGU nº 1, de 10 de maio de 2016. Dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo Federal.

BRASIL. Lei nº 12.813, de 16 de maio de 2013. Dispõe sobre o conflito de interesses no exercício de cargo ou emprego do Poder Executivo federal, e dá outras providências. Diário Oficial da União, Brasília, DF, 17 maio 2013.

BRASIL. Ministério da Economia. Guia de Gestão de Riscos. Versão 2.0, de 4 de fevereiro de 2021.

BRASIL. Tribunal de Contas da União. Manual de Gestão de Riscos do TCU. Segecres/Seplan. Brasília, maio 2018.

BRASIL. Tribunal de Contas da União. Acórdão nº 572/2022 - TCU Plenário. Brasília, DF, 2022.

COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION (COSO). Enterprise Risk Management - Integrated Framework. 2nd ed. COSO, 2017.

COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION (COSO). Risk Assessment in Practice. COSO, 2004.

GIESTOSA, Juliana Cottard et al. Metodologias de gestão de riscos em entes públicos brasileiros: uma análise bibliográfica. Revista de Gestão e Secretariado, v. 14, n. 4, p. 5889-5910, 2023.

INSTITUTE OF INTERNAL AUDITORS BRASIL. Declaração de Posicionamento do IIA. Disponível em: https://iiabrasil.org.br/korbilload/upl/ippf/downloads/declarao-de-pos-ippf-00000001-21052018101250.pdf. Acesso em: 16 jul. 2024.

PORTER, Michael E.; ADVANTAGE, *Competitive. Creating and sustaining superior performance*. Competitive advantage, v. 167, p. 167-206, 1985.

PROJECT MANAGEMENT INSTITUTE (PMI). *A Guide to the Project Management Body of Knowledge* (PMBOK® Guide). 5. ed. Capítulo 11 - Gerenciamento do Risco do Projeto. Newtown Square: PMI, 2013.