Boletim de Serviço Eletrônico em 23/05/2022
DOU de 23/05/2022, seção 1, página 299

INSTITUTO NACIONAL DO SEGURO SOCIAL

RESOLUÇÃO CEGOV/INSS Nº 20, DE 20 DE MAIO DE 2022

Aprova a Metodologia de Gerenciamento de Riscos do INSS.

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 Aprovar, nos termos do Anexo desta Resolução, a Metodologia de Gerenciamento de Riscos do INSS, que tem por objetivo subsidiar a tomada de decisão, baseada em técnica e ferramentas específicas, 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.

Art. 2º Esta Metodologia encontra-se em conformidade com a Política de Gestão de Riscos do INSS, instituída pelo CEGOV, por meio da Resolução nº 5/CEGOV/INSS, de 28 de maio de 2020.

Art. 3º A Metodologia de Gerenciamento de Riscos integra o Sistema de Gestão de Riscos do INSS – SGR-INSS.

Art. 4º O Anexo desta Resolução será publicado no Boletim de Serviço Eletrônico e divulgado no Portal do Instituto.

Art. 5º Esta Resolução entra em vigor em 1º de junho de 2022.

GUILHERME GASTALDELLO PINHEIRO SERRANO
Presidente

AILTON NUNES DE MATOS JUNIOR
Diretor de Benefícios e Relacionamento com o Cidadão
Substituto

JOBSON DE PAIVA SILVEIRA SALES
Diretor de Gestão de Pessoas

LARISSA ANDRADE MORA
Diretora de Orçamento, Finanças e Logística

ALEXANDRE GUIMARÃES
Diretor de Governança, Planejamento e Inovação

JOÃO RODRIGUES DA SILVA FILHO
Diretor de Tecnologia da Informação

Documento assinado eletronicamente por **JOBSON DE PAIVA SILVEIRA SALES**, **Diretor(a) de Gestão de Pessoas**, em 20/05/2022, às 17:09, 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 **JOAO RODRIGUES DA SILVA FILHO**, **Diretor(a) de Tecnologia da Informação**, em 20/05/2022, às 17:09, 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 **AILTON NUNES DE MATOS JUNIOR**, **Diretor(a) de Benefícios e Relacionamento com o Cidadão Substituto(a)**, em 20/05/2022, às 17:10, 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 **ALEXANDRE GUIMARAES**, **Diretor(a) de Governança, Planejamento e Inovação**, em 20/05/2022, às 17:10, 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 **LARISSA ANDRADE MORA**, **Diretor(a) de Orçamento, Finanças e Logística**, em 20/05/2022, às 17:17, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

ANEXO

RESOLUÇÃO CEGOV/INSS Nº 20, DE 20 DE MAIO DE 2022

METODOLOGIA DE GESTÃO DE RISCOS DO INSS

1. Introdução

1.1 O Instituto Nacional do Seguro Social - INSS é partícipe do Comitê de Gestão de Riscos, Transparência, Controle e Integridade - CRTCI do Ministério da Economia (ME), cujo principal objetivo é promover a cultura da gestão de riscos em todos os seus órgãos e entidades vinculadas, a fim de alcançar a gradual convergência de métodos, resultados e comunicação.

1.2 Os riscos acompanham todas as atividades humanas e interferem nos resultados desejados. Não é diferente com as decisões e ações para alcançar o sucesso na missão de um órgão ou entidade.

1.3 A cultura de gerir os riscos é a solução para a cultura de “apagar incêndios”. Analisar previamente e elaborar mitigações para os riscos são fundamentais para que haja economia de recursos e melhores resultados. Fazendo mais e melhor, utilizando menos tempo e orçamento.

1.4 O processo de gestão de riscos do INSS está alicerçado nos 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 Gerenciamento de Riscos;

III - Solução Tecnológica e Apoio; e

IV - Capacitação Contínua.

1.5 Logo, a sua implementação perpassa pelo gerenciamento dos riscos, que consiste em um processo 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 desta Autarquia, ocorrendo nos níveis hierárquicos da estrutura organizacional sejam estratégico, tático ou operacional e nos macroprocessos sejam eles de natureza finalística, gerencial ou de sustentação.

1.6 Enfim, mantém relação direta e intrínseca com o cumprimento da Missão Institucional que é “Garantir proteção social aos cidadãos por meio do reconhecimento de direitos”. E para o alcance da Visão: “Ser reconhecido pela excelência no relacionamento com o cidadão” e se apresenta como mais um importante instrumento para a gestão profissional nos tempos atuais.

1.7 Este documento tem por objetivo apresentar a Metodologia de Gerenciamento de Riscos do INSS, 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.

1.8 A Metodologia de Gestão de Riscos do INSS objetiva subsidiar à tomada de decisão, baseada em técnica e ferramentas específicas, 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.

1.9 Deste modo, a presente normativa oferece orientações específicas para a implementação do gerenciamento de riscos, que deverá acontecer gradualmente, de forma dinâmica e interativa, permitindo visualizar a identificação clara dos elos de conexão e interdependência entre todos os processos executados na organização, respeitando os objetivos, princípios e os pilares preceituados para a gestão de riscos do INSS.

2. Conceitos da Gestão de Riscos

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

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

II - **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;

III - **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;

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

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

VI - **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;

VII - **medida de controle**: medida aplicada pela organização para tratar os riscos, aumentando a probabilidade de que os objetivos e as metas organizacionais estabelecidos sejam alcançados, bem como medidas de resposta aos riscos que mitiguem, transfiram ou evitem esses riscos;

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

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

X - **primeira linha:** Gestão operacional, controles internos da gestão executados por todos os agentes públicos responsáveis pela condução de atividades e tarefas, no âmbito dos macroprocessos gerenciais, finalísticos e de apoio dos órgãos e entidades. É composta pelos servidores e pelos responsáveis pelo gerenciamento de riscos dos processos organizacionais;

XI - **segunda 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, CEGOV e Comitês Temáticos;

XII - **terceira 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;

XIII - **processo de gestão 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;

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

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

XVI - **risco inerente**: o risco a que uma organização está exposta sem considerar quaisquer ações gerenciais que possam reduzir a probabilidade de sua ocorrência ou seu impacto (art. 2º, XIV - Guia de Gerenciamento de Riscos do Ministério da Economia);

XVII - **risco residual**: risco a que uma organização está exposta após a implementação de ações gerenciais para o tratamento do risco. (Art. 2º, XV - Guia de Gerenciamento de Riscos do Ministério da Economia);

XVIII - **riscos operacionais**: eventos que podem comprometer as atividades do órgão ou entidade, normalmente associados a falhas, deficiência ou inadequação de processos internos, pessoas, infraestrutura e sistemas;

XIX - **riscos de imagem/reputação do órgão**: eventos que podem comprometer a confiança da sociedade (ou de parceiros, de clientes ou de fornecedores) em relação à capacidade do órgão ou da entidade em cumprir sua missão institucional;

XX - r**iscos legais**: eventos derivados de alterações legislativas ou normativas que podem comprometer as atividades do órgão ou entidade;

XXI - **riscos financeiros/orçamentários**: eventos que podem comprometer a capacidade do órgão ou entidade de contar com os recursos orçamentários e financeiros necessários à realização de suas atividades, ou eventos que possam comprometer a própria execução orçamentária, como atrasos no cronograma de licitações;

XXII - **riscos à integridade**: riscos que configurem ações ou omissões que possam favorecer a ocorrência de fraudes ou atos de corrupção;

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

XXIV - **análise quantitativas**: investigar o impacto e efeitos do risco com precisão numérica; e

XXV - **análise semi-quantitativa**: associação das duas práticas (métrica e subjetiva) tornando-se um multicritério de apoio à decisão.

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.

3.2 Estruturada em pilares fundamentais para sua implementação, composta pela Política de Gestão de Riscos, Metodologia de Gerenciamento de Riscos, objeto deste Caderno, Solução Tecnológica e Apoio e Capacitação Contínua.

Figura 01: Pilares da Gestão de Riscos do INSS.

3.3 Preconiza o auxílio à tomada de decisão com vistas a prover razoável segurança no cumprimento da missão institucional pela concretização dos objetivos estratégicos, permeando os processos de trabalho, sejam eles finalísticos, gerenciais ou de sustentação.

3.4 Tem por finalidade estabelecer e difundir princípios, diretrizes, objetivos, competências e responsabilidades necessárias aos processos de governança e gestão das políticas, programas, processos e projetos da Autarquia, implantada por meio de ciclos de revisão e melhoria contínua, estando sua operacionalidade descrita nesta metodologia.

3.5 Obedece a uma arquitetura (princípios, estrutura e processos), sob a disciplina de processo, que incorpora toda a organização em todos os níveis, ou seja, aplicando-se, irrestritamente, a todos os macroprocessos da Cadeia de Valor do INSS. Recomenda-se que a avaliação dos riscos aconteça na instância **Processo de Trabalho** que pode ser visualizado na figura a seguir:

Figura 02: Estrutura do processo da Gestão de Riscos - Hierarquia de Processos.

3.6 O processo de gestão de riscos do INSS é composto por três instâncias, a saber:

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, atuando como **segunda linha e primeira linha, respectivamente**;

II - **instância avaliadora**: composta pela DIGOV atuando como **segunda linha** e Auditoria Interna atuando como **terceira linha**. Recomenda-se a leitura da Declaração de Posicionamento do IIA constante das Referências Conceituais deste documento; e

III - **instância executora**: composta pelas Diretorias, Superintendências Regionais, Gestores de Riscos, Coordenadores Setoriais de Gestão de Riscos, executando todos os passos previstos para a realização do gerenciamento de riscos, atuando como primeira linha.

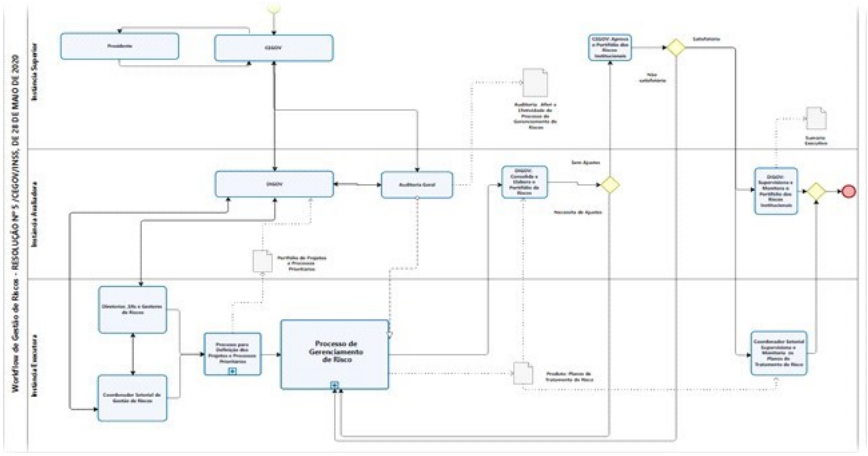

Figura 03 - **Workflow** da Gestão de Riscos do INSS – Anexo I

3.7 Todo ato de agir, omitir ou de exação traz consigo algum risco. Logo, são quase inesgotáveis as oportunidades de análise de risco sobre esses atos. Alguns desses ocorrem de forma isolada e a grande maioria possui baixo impacto para a organização como um todo. Em geral, até em função de sua baixa complexidade, esses atos menos importantes são tratados nas relações internas da organização, que geralmente concentrará sua atenção para aqueles atos que poderão lhe provocar maiores danos (riscos negativos) ou que poderão lhe abrir boas oportunidades (riscos positivos). Por fim, importante registrar que esses atos precisam estar necessariamente alinhados e em equilíbrio com o planejamento estratégico da organização e à sua cadeia de valor. (Fonte: Guia de Riscos do Ministério da Economia – revisado 2021, adaptado, grifo nosso).

3.8 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 processos de trabalho deverão ser considerados os princípios da Gestão de Risco do INSS, sendo fundamental para garantir a integração e o alinhamento das ações e projetos conduzidos.

3.9 Os **riscos estratégicos** serão monitorados pela DIGOV, a partir da priorização dos processos e ações estratégicas definidas pela área responsável pelo Planejamento Estratégico da Instituição, para que, sob a ótica do contexto de riscos, eventos de riscos que poderão impactar no seu sucesso sejam identificados, avaliados e monitorados, especificadamente. Perceber a integração dos riscos aos processos organizacionais é reconhecê-los, especificá-los e alinhá-los ao cumprimento da missão, alcance da visão, incluindo as competências legais instituídas para o INSS, conforme recomendado pelo COSO 2017 e Manual TCU 2018.

3.10 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, tais como, esta metodologia, solução tecnológica e apoio (planilha documentadora, sistemas de acompanhamento e gerenciamento de riscos) e capacitações.

3.11 Assim, para proporcionar a efetividade desse processo, faz-se necessário reunir e utilizar desses recursos, preceituados nesta metodologia, instrumentalizando os servidores na sua **práxis**, pois estes são os detentores do conhecimento dos processos operacionais.

3.12 Destaca-se como um importante vetor para a Gestão de Riscos, a existência de um processo eficaz de comunicação e informação dos riscos e seus resultados – **Plano de comunicação e consulta**.

3.13 Este Plano deverá ser formal, com utilização de relatórios gerenciais, mensagens de reporte e outros recursos de comunicação, que permitam a atuação mais próxima do fato gerador do risco e da tomada de decisão, em todas as instâncias das unidades da Autarquia.

3.14 Ressalta-se que as informações geradas no processo de gerenciamento de riscos deverão ser confiáveis, íntegras e tempestivas e, dependendo do contexto, restritas. Esse nível de restrição deve ser observado pelos servidores do INSS e demais partes. Para o meio externo, quando necessário, as comunicações sobre a Gestão de Riscos da Autarquia serão feitas pelos canais oficiais do INSS.

3.15 Por fim, 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 contínuo 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.

3.16 As atribuições de cada um destes componentes encontram-se descritas na Política de Gestão de Riscos do INSS disciplinada pela Resolução nº 5/CEGOV/INSS, de 2020, e podem ser visualizadas mais facilmente na Matriz RACI (Anexo VI), na qual é possível identificar, as instâncias e responsáveis, com os seguintes papéis:

I - Responsável;

II - Aprovador;

III - Consultado; e

IV - Informado.

3.17. Atuação dos Gestores de Riscos:

I - auxiliar a DIGOV na definição dos indicadores de gestão de riscos, visando à identificação de riscos não mapeados e a exclusão daqueles que, eventualmente, tenham perdido a importância;

II - apresentar à DIGOV os resultados do monitoramento sobre a efetividade do tratamento do risco;

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

IV - 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; e

V - identificar a natureza e a extensão do **risco residual** após o tratamento do risco.

3.18. Atuação dos Coordenadores Setoriais de Gestão de Riscos:

I - elaborar e encaminhar à DIGOV o Plano de Tratamento dos Riscos, em conformidade com as diretrizes estabelecidas pelo CEGOV e orientações da DIGOV;

II - propor ações a serem incluídas no Plano de Integridade do INSS para assegurar a existência de condições mínimas para o exercício da boa governança;

III - implementar as ações previstas no Plano de Integridade do INSS;

IV - 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;

V - aprovar a periodicidade máxima do ciclo do processo de gerenciamento de riscos para os processos organizacionais sob sua responsabilidade;

VI - consolidar os resultados das diversas áreas em relatórios gerenciais e encaminhá-los a DIGOV;

VII - reportar à DIGOV, com a máxima urgência, o surgimento de Riscos-Chave e/ou o incremento de um risco já mapeado;

VIII - assessorar na elaboração do Plano de contingência relacionados a riscos dos processos organizacionais da unidade de sua área de atuação; (se essa atuação permanecer é interessante definir o que é o plano de contingência)

IX - comunicar à DIGOV as mudanças ou fragilidades relacionadas aos riscos-chaves; e

X - assessorar na elaboração dos processos de gerenciamento de riscos da unidade de sua área de atuação.

3.19 Atuação dos servidores e colaboradores em geral

I - conhecer os riscos do seu processo de trabalho;

II - monitorar a evolução dos níveis de riscos e da efetividade das medidas de controles internos implementadas nos objetos de gestão em que estiverem envolvidos e reportar, imediatamente, ao responsável pelo gerenciamento de riscos as mudanças ou fragilidades identificadas;

III - realizar a execução dos processos de gerenciamento de riscos no âmbito de sua atuação, visando identificar os riscos do seu processo de trabalho; e

IV - 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 Gerenciamento de Riscos

4.1 A Metodologia de Gerenciamento 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.

4.2 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 Casa, pressupõe um modelo de aplicação integrada e descentralizada.

4.3 Ainda, deverá contemplar critérios predefinidos de avaliação continuada, de forma a permitir a comparabilidade entre os riscos, estando a 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;

VI - monitoramento e melhoria contínua.

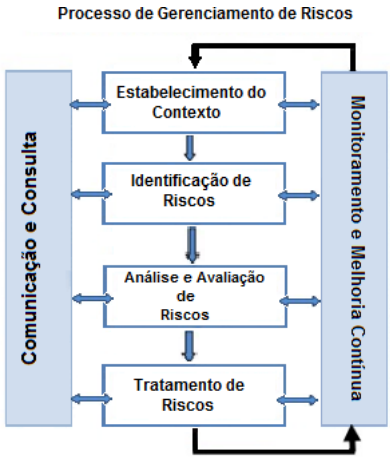

Figura 04 – Fonte: Norma ABNT NBR ISO 31000:2009 – Adaptado.

4.4 Para fins de descrição do processo de gestão de riscos neste documento, os termos gestão de riscos e gerenciamento de riscos serão utilizados da seguinte forma:

I - **gestão de riscos** refere-se à arquitetura que engloba os princípios, a estrutura e o processo, conforme apresentado no Anexo I; e

II - **gerenciamento de riscos** refere-se à aplicação dessa arquitetura para riscos específicos, como apresentado no Anexo II.

4.5 A compreensão das atividades que envolve o gerenciamento de riscos será descrita como processo de trabalho, com as ações que devem ser realizadas pelos gestores de riscos.

4.6 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. (Manual de gestão de riscos do TCU – Brasília, maio 2018, com adaptação). Esta orientação deve ser aplicada em todas as etapas desta metodologia.

4.7 Após a escolha dos projetos, processos de trabalhos e serviços, dar-se-á início ao **processo de gerenciamento de riscos**, conforme o fluxo abaixo. Para tanto apresentamos um modelo de Planilha Documentadora **(Anexo III deste documento)** para dar suporte e registro deste processo:

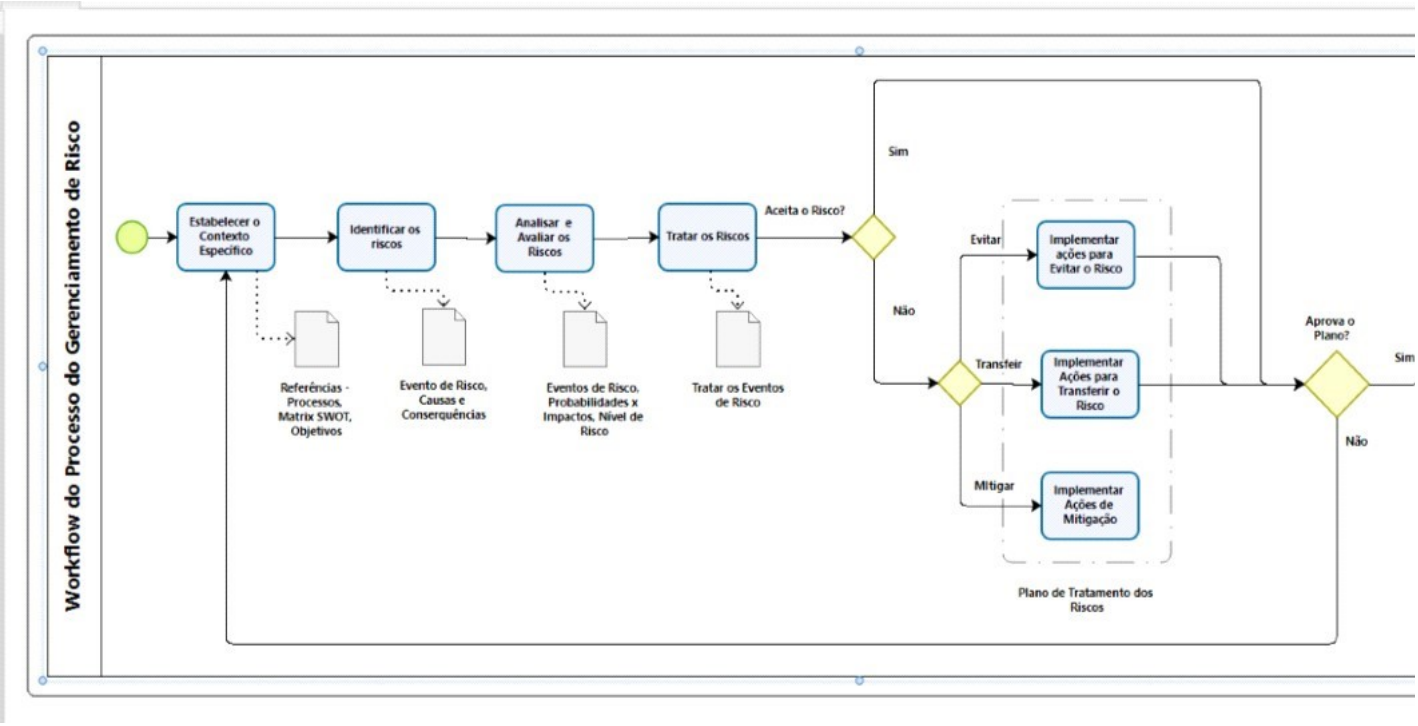

Figura 05 - **Workflow** do Processo de Gerenciamento de Riscos – Anexo II

4.8 Estabelecimento de contexto

4.8.1 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 (Resolução nº 5/CEGOV/INSS, de 2020).

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

4.8.3 Em outras palavras, o estabelecimento do contexto considera os objetivos da organização, sua cadeia de valor (processos) e registra os fatores correspondentes ao ambiente interno (forças x fraquezas) que estão sob sua governabilidade e o ambiente externo (oportunidades x ameaças) que não estão, que impactam os objetivos, resultados e partes interessadas.

4.8.4 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.

4.8.5 Deverão ser identificados:

I - órgão/Unidade do objeto;

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

III - informações sobre a fixação de objetivos: missão, visão e objetivos da instituição;

IV - informações sobre o macroprocesso, processo, processo de trabalho: registrar sua descrição, objetivos, leis, regulamentos e sistemas associados;

V - especificar quais principais fatores ou fontes de riscos, internos e externos, que poderão afetar os objetivos e ou resultados (pessoas, sistemas informatizados, estruturas organizacionais, legislação, recursos, partes interessadas, etc.);

VI - quais os objetos de gestão de risco mais importantes para a sua unidade ou trabalho; e

VII - quais os objetivos/finalidade de cada objeto.

4.8.6 Após personalização do objeto de gestão é necessária a identificação dos atributos internos e externos relacionados ao objeto em estudo. A ferramenta indicada para relacionar estes fatores é a Matriz **SWOT**.

4.8.7 A Matriz **SWOT** é uma ferramenta gerencial utilizada para 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.

4.8.8 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.

4.8.9 A estruturação da **SWOT** baseia-se em uma matriz com quatro quadrantes, dos quais, lista-se em cada quadrante os pontos identificados conforme a classificação Ambiente Interno, em Pontos Fortes e Pontos Fracos e Ambiente Externo, em Ameaças e Oportunidades.

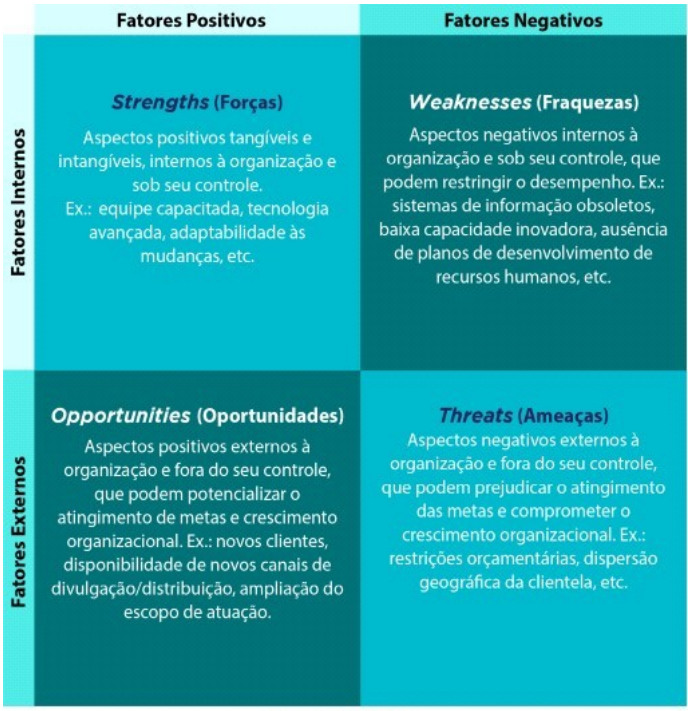

Figura: Análise SWOT

Figura 06 - Análise **SWOT**

4.8.10 Desta maneira, essa estratégia fomentará a tomada de decisão e resultará em elementos para seguir à segunda etapa, uma vez que 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 possíveis impactos à tomada de decisão.

4.9 Identificação de riscos

4.9.1 Compreende o reconhecimento e a descrição dos riscos relacionados a um objeto de gestão, envolvendo a identificação de possíveis fontes de riscos. (Fonte: Resolução nº 5/CEGOV/INSS, de 2020).

4.9.2 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.

4.9.3 A finalidade é mapear onde, o porquê e como os eventos de risco, causas e consequências, sejam elas, positivas ou negativas, poderão impedir, inibir ou atrasar a consecução dos objetivos dos processos, ou quais situações que poderiam existir, afetar o alcance dos objetivos do sistema ou da organização. É feito o levantamento das possíveis causas associadas aos eventos de risco.

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

4.9.5 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.

4.9.6 Poderão ser adotadas técnicas e ferramentas como Matriz **SWOT, brainstorming, brainwriting**, entrevistas, visitas técnicas, pesquisas, etc., com o intuito de extrair detalhada base de apontamentos sobre o objeto de gestão de risco.

4.9.7 Independentemente de suas fontes estarem ou não sob seu 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.

4.9.8 Causas fundamentais e problemas dos riscos 4

Fonte de risco	**Fragilidades relacionadas**
Pessoas	Pouco capacitada, desmotivada, estressada, desonesta
Processo	Mal desenhado, redundante, incompleto
Sistemas	Obsoleto, inseguro, sem documentação, não amigável, complexo
Legislação	Inadequada, ineficiente, obsoleta
Evento externo	Desastre ambiental, crise econômica, influência política

Tabela I

4.9.9 Algumas perguntas-chaves poderão ajudar nesta fase 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.

4.9.10 A sintaxe abaixo auxiliará na descrição dos eventos de riscos identificados:

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

Fonte: TCU, 2017

4.10 Análise e Avaliação de riscos

4.10.1 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. (Fonte: Resolução nº 5/CEGOV/INSS, de 2020).

4.10.2 Análise

4.10.2.1 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).

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

4.10.2.3 Dependendo das circunstâncias, a análise de riscos pode ser qualitativa, semi-quantitativa ou quantitativa, ou, ainda, uma combinação destas, e ser mais ou menos detalhada (ABNT, 2009). Porém, essa relação simples pode não refletir relações não lineares, sendo necessário, assim, incluir um fator de ponderação para uma das duas variáveis (probabilidade ou impacto, de modo a atingir a escala relativa necessária entre eles) e ou um operador exponencial para uma ou para ambas as variáveis (DE CICCO, 2009, adaptado).

4.10.2.4 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.

4.10.2.5 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)

4.10.2.6 Escala de probabilidade

4.10.2.6.1 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.

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

Probabilidade	**Possibilidade de ocorrência do risco**
5 – Muito Alta	Evento esperado que ocorra na maioria das circunstâncias >90%
4 – Alta	Evento provavelmente ocorra na maioria das circunstâncias >=50% <= 90%
3 – Média	Evento deve ocorrer em algum momento >=30% <= 50%
2 – Baixa	Evento pode ocorrer em algum momento >=10% <= 30%
1 – Muito Baixa	Evento pode ocorrer apenas em circunstâncias excepcionais <10%

Tabela II

4.10.2.7 Escala de impacto

4.10.2.7.1 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.

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

Impacto	**A ocorrência do risco causará**
5 – Catastrófico	Evento com potencial para levar o negócio/serviço ao colapso.
4 – Grande	Evento crítico, mas com a devida gestão pode ser suportado.
3 – Moderado	Evento significativo que pode ser gerenciado em circunstâncias normais.
2 – Pequeno	Evento cujas as consequências podem ser absorvidas, mas carece do esforço da gestão para minimizar o impacto.
1 – Insignificante	Evento cujo impacto pode ser absorvido por meio de atividades normais.

Tabela III

4.10.2.8 Escala de Nível de risco

4.10.2.8.1 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

Tabela IV – Planilha Documentadora

4.10.2.9 Descrição do Nível de Risco

Risco Crítico	Nível de risco muito além 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

Tabela V

4.10.2.10 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.

Matriz de Riscos						
IMPACTO	Catastrófico	5	5	10	15	20	25
	Grande	4	4	8	12	16	20
	Moderado	3	3	6	9	12	15
	Pequeno	2	2	4	6	8	10
	Insignificante	1	1	2	3	4	5
			1	2	3	4	5
			Muito Baixa	Baixa	Média	Alta	Muito Alta
			PROBABILIDADE				

Tabela VI – Planilha documentadora

4.10.3 Avaliação

4.10.3.1 Na fase de Avaliação de Riscos 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.

4.10.3.2 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 de riscos, 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).

4.10.3.3 São critérios de relevância considerados nesta metodologia, como fatores de análise, com vista a definir o nível de risco residual:

I - esforço da gestão;

II - regulação;

III - reputação;

IV - negócios/serviços à sociedade;

V - intervenção hierárquica; e

VI - valor orçamentário.

4.10.3.4 Uma boa prática para apoiar o processo de avaliação de riscos é estabelecer critérios para priorização e tratamento (apetite a risco, nível recomendado de atenção, tempo de resposta requerido, comunicação etc.) associados aos níveis de risco. Segue-se um exemplo simples. (TCU Gestão de Riscos - Avaliação da Maturidade).

Nível de risco	Critério para priorização e tratamento de riscos
RC Risco Crítico	Nível de risco muito além do apetite a risco. Qualquer risco nesse nível deve ser comunicado à governança e alta administração e ter uma resposta imediata. Postergação de medidas só com autorização do dirigente máximo.
RA Risco Alto	Nível de risco além do apetite a risco. Qualquer risco nesse nível dever ser comunicado a alta administração e ter uma ação tomada em período determinado. Postergação de medidas só com autorização do dirigente de área.
RM Risco Moderado	Nível de risco dentro do apetite a risco. Geralmente nenhuma medida especial é necessária, porém requer atividades de monitoramento específicas e atenção da gerência na manutenção de respostas e controles para manter o risco nesse nível, ou reduzi-lo sem custos adicionais.
RP Risco Pequeno	Nível de risco dentro do apetite a risco, mas é possível que existam oportunidades de maior retorno que podem ser exploradas assumindo-se mais riscos, avaliando a relação custos x benefícios, como diminuir o nível de controles.

Tabela VII - Diretrizes para priorização e tratamento de riscos (adaptado de BRASIL, 2013a).

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

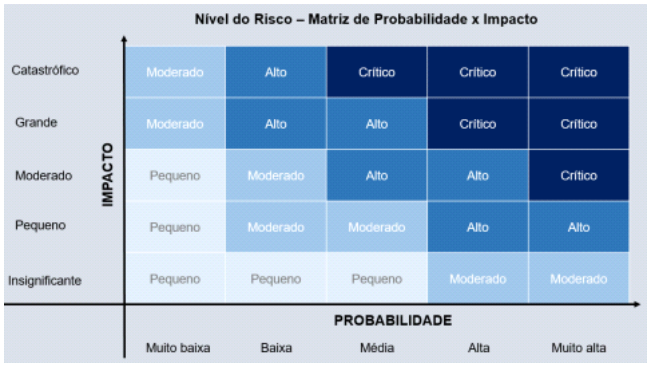

Tabela VIII

4.10.3.6 Ainda, 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?

4.11 Tratamento do risco

4.11.1 Compreende o planejamento e a realização de ações para modificar o nível do risco. (Fonte: Resolução nº 5/CEGOV/INSS, de 2020).

4.11.2 Consiste na emissão de planos de tratamento de riscos com a finalidade de definir e documentar como as opções de tratamento escolhidas serão implementadas. O objetivo é documentar todo o processo de implementação através 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.

4.11.3 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. Esta etapa é acompanhada por um processo cíclico de reavaliação do novo nível de risco, tendo em vista a determinação de sua tolerabilidade em relação aos critérios previamente definidos, a fim de decidir se o tratamento adicional é requerido, e inclui a:

I - avaliação do tratamento já realizado;

II - avaliação dos níveis de risco residual frente ao apetite e às tolerâncias a risco definidos;

III - definição e a implementação de tratamento adicional nos casos em que o risco residual extrapolar o apetite e as tolerâncias; e

IV - avaliação da eficácia desse tratamento. (Fonte: ABNT, 2009)

4.11.4 De acordo com o nível de riscos, deverá ser escolhida a forma de tratamento. Selecionar a opção mais adequada envolve equilibrar, de um lado, os custos e esforços de implementação e, de outro, os benefícios decorrentes, dentre as seguintes opções:

I - **mitigar o risco**: reduzir o impacto ou a probabilidade de ocorrência do evento de risco;

II - **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;

III - **transferir o risco**: compartilhar ou transferir uma parte do evento de risco a terceiros; e

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

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. Exemplo: 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

Tabela IX – Planilha Documentadora

4.11.5 Os gestores devem registrar e recuperar 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.

4.11.6 Ferramentas de melhorias e respostas a riscos

4.11.6.1 Técnicas dos “5 por quês?”

Figura 08 - Revista AdNormas

4.11.6.2 Inúmeras ferramentas como Análise de Desperdícios, Análise de Desvios Positivos, Diagrama de Ishikawa ou Espinha de Peixe, são simples e eficientes para ampliar a visão sobre possíveis causas de um problema ou riscos. Porém, sugerimos a 5W2H ou 4Q1POC, esta última, origina-se de sete perguntas em inglês: **What?, Who? When? Why?, Where? How? e How much?** que foram traduzidas para o português, 4Q1POC: O quê? Quem? Quando? Quanto? Por quê? Onde? e Como?

4.11.6.3 A proposta de melhorias ou respostas, a partir dessa técnica, direciona as perguntas às causas fundamentais dos eventos de riscos, no sentido de se encontrar maneiras de revertê-los ou mitigar seus efeitos, a saber:

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

II - **Who**/Quem? – Deve-se analisar quem são os clientes e fornecedores do processo, bem como quem são os responsáveis pelo planejamento, execução e avaliação das atividades cuja causa em questão afeta. O que pode ser alterado em relação aos atores dessas atividades no sentido de mitigar a causa?

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

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

V - **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?

VI - **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?

VII - **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?

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

4.11.6.5 Nesta etapa convém o estabelecido nos indicadores Chave de Risco com vistas ao acompanhamento da dinâmica do evento de riscos.

4.12 Comunicação e Consulta

4.12.1 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. (Fonte: Resolução nº 5/CEGOV/INSS, de 2020).

4.12.2 É importante que a comunicação ocorra de forma **vertical** e **horizontal**:

4.12.3 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.

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

4.12.5 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. (Fonte: Manual de Gestão de Risco, TCU - adaptado)

4.12.6 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.

4.12.7 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.

4.12.8 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.

4.13 Monitoramento

4.13.1 Compreende o acompanhamento e a verificação contínua do desempenho ou da situação de elementos da gestão de riscos. (Fonte: Resolução nº 5/CEGOV/INSS, de 2020).

4.13.2 A fase de monitoramento inclui tanto o acompanhamento da execução dos planos de ação das melhorias priorizadas, quanto a 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 também implantar as ações corretivas necessárias após a análise.

4.13.3 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. (Fonte: ABNT, 2009)

4.13.4 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 (Fonte: 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.

4.13.5 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.

4.13.6 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.

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

4.13.8 Os ICR são utilizados para alertar os gestores da necessidade de tomada tempestiva de ações corretivas.

4.13.9 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.

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

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

4.13.12 O ICR poderá ser estabelecido na etapa de tratamento de riscos.

4.13.13 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.

4.14 Melhoria contínua

4.14.1 Compreende o aperfeiçoamento ou ajuste de aspectos da gestão de riscos avaliados no monitoramento. (Fonte: Resolução nº 5/CEGOV/INSS, de 2020).

4.14.2 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.

4.14.3 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.

5. Recursos para a realização das atividades

5.1 O Gestor de Risco, que é o responsável pelo processo organizacional da sua unidade, é 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.

5.2 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.

5.3 Os recursos operacionais e tecnológicos necessários para apoiar a condução das atividades de Gestão de Riscos do INSS serão definidos em manual operacional, a ser publicado pela DIGOV.

6. Considerações finais

6.1 Esta metodologia foi construída a partir das leituras acerca da gestão de riscos nos Referenciais Teóricos elencados nestes documentos, preceituados, principalmente pelo **COSO e ISO 31000**.

6.2 Apresentou-se as etapas, critérios e técnicas para a execução do Processo de Gerenciamento de Riscos, inter-relacionados e integrados com os objetivos e pressupostos elencados na Política da Instituição, em conformidade com a **Resolução nº 5/CEGOV/INSS, de 2020**.

6.3 A elaboração desse instrumental não foi uma tarefa simples, pois implicou em pesquisar, estudar, elaborar construções genéricas e específicas de cada ação, além de articular todos os elementos envolvidos (objetivos, pressupostos, objeto, método e seus desdobramentos, clientes, materiais e circunstâncias necessárias para a sua execução), a partir de uma visão concreta da realidade e comprometimento com a sua transformação. Neste sentido, a metodologia constitui, ao mesmo tempo, em um trabalho de gerenciamento eficaz, guiado pela análise ordenada de situações e problemas, vinculada à tomada de decisões para resolvê-los; e por uma prática de associação entre ideias e procedimentos que deve ser realizada de forma consciente, reflexiva e intensiva (Fonte: LÜCK, 2003 - adaptado).

7. Referências Conceituais

7.1 Decreto-Lei nº 200, de 25 de fevereiro de 1967 - Dispõe sobre a organização da Administração Federal, estabelece diretrizes para a Reforma Administrativa e dá outras providências.

7.2 Decreto nº 9.203, de 22 de novembro de 2017 - Dispõe sobre a Política de Governança da Administração Pública Federal Direta, Autárquica e Fundacional.

7.3 DE CICCO, Francesco (Rev.). Gestão de Riscos: Diretrizes para implementação da ISO 31000:2009 (Série Risk Management). Risk Tecnologia Editora, 2009.

7.4 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;

7.5 LÜCK, Heloísa. Metodologia de projetos: uma ferramenta de planejamento e gestão. 3 ed. Petrópolis, RJ: Vozes, 2003.

7.6 Portaria nº 3.213/PRES/INSS, de 10 de dezembro de 2019 – Institui o Sistema de Governança do INSS;

7.7 Resolução nº 5/CEGOV/INSS, de 28 de maio de 2020 – Institui a Política de Gestão de Riscos do INSS;

7.8 Resolução nº 8/CEGOV/INSS, de 29 de junho de 2020 - Institui o Programa de Integridade do INSS;

7.9 ABNT NBR ISO/IEC 31000:2009. Gestão de riscos - Princípios e diretrizes;

7.10 ABNT NBR ISO/IEC 31010:2012. Gestão de riscos - Técnicas para o processo de avaliação de riscos, novembro de 2012;

7.11 Guia de Gestão de Riscos do Ministério da Economia – ME. Versão 2.0 de 4 de fevereiro de 2021.

7.12 GESTÃO DE RISCOS - Avaliação da Maturidade - SEGECEX/ADGECEX/SEMEC - JANEIRO - 2018;

7.13 Manual de Gestão de Riscos do TCU - Segecres/Seplan - Brasília, Maio, 2018

7.14 Declaração de Posicionamento do IIA - https://iiabrasil.org.br/korbilload/upl/ippf/downloads/declarao-de-pos-ippf-00000001-21052018101250.pdf

8. Anexos da Metodologia de Gestão de Riscos

8.1 **Anexo I** - **Workflow** do Processo de Gestão de Riscos do INSS;

8.2 **Anexo II** - **Workflow** da Gerenciamento de Riscos do INSS;

8.3 **Anexo III** - Planilha Documentadora;

8.4 **Anexo IV** - Matriz RACI.