Ministério da Educação
Secretaria de Educação Profissional e Tecnológica
Instituto Federal de Educação, Ciência e Tecnologia de Mato Grosso do Sul

MANUAL

DE

GESTÃO DE RISCOS

DO IFMS

INSTITUTO FEDERAL
Mato Grosso do Sul

JANEIRO/ 2025

Missão

Promover a educação de excelência por meio do ensino, pesquisa e extensão nas diversas áreas do conhecimento técnico e tecnológico, formando profissional humanista e inovador, com vistas a induzir o desenvolvimento econômico e social local, regional e nacional.

Visão

Ser reconhecido como uma instituição de ensino de excelência, sendo referência em educação, ciência e tecnologia no Estado de Mato Grosso do Sul.

Valores

Inovação;
Ética;
Compromisso com o desenvolvimento local e regional;
Transparência;
Compromisso Social.

INSTITUTO FEDERAL
Mato Grosso do Sul

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE MATO GROSSO DO SUL - IFMS	
Endereço:	R. Jorn. Belizário Lima, 236, Vila Glória - Campo Grande - MS CEP: 79004-270
CNPJ:	10.673.078/0001-20

identificação	
	MANUAL DE GESTÃO DE RISCOS DO IFMS
Proponente:	Comitê de Governança, Gestão de Riscos e Controle Interno do IFMS
Elaborado por:	Diretoria de Gestão Sistêmica, Governança, Riscos, Transparência e Inovação e Inovação Pública (Digov)

SUMÁRIO

1 INTRODUÇÃO

Eventos incertos que podem impactar o alcance dos objetivos estratégicos são uma realidade inerente a qualquer instituição, seja ela pública ou privada. Esses eventos, independentemente da natureza — econômica, social, legal, tecnológica ou operacional —, demandam uma gestão de riscos eficiente. Essa prática é essencial para garantir que a organização alcance seus objetivos de forma segura e eficaz, mesmo em cenários adversos. Além disso, a gestão de riscos contribui para uma tomada de decisões mais assertiva e para a redução de retrabalhos.

No Brasil, o marco regulatório para a gestão de riscos é a Instrução Normativa Conjunta nº 1, de 10 de maio de 2016, emitida pelo Ministério do Planejamento, Orçamento e Gestão e pela Controladoria-Geral da União — MP/CGU. Essa Instrução aborda os controles internos, a gestão de riscos e a governança no âmbito do Poder Executivo federal. Além disso, o Decreto nº 9.203, de 22 de novembro de 2017, que dispõe sobre a política de governança da administração pública federal, reforça a relevância da prática de gestão de riscos.

Em conformidade com esses normativos, o IFMS criou o Comitê de Governança, Gestão de Riscos e Controle Interno em 2017 e estabeleceu a Política de Gestão de Riscos no mesmo ano. No início de 2024, a instituição revisou o Regimento Geral e instituiu a Diretoria de Gestão Sistêmica, Governança, Riscos, Transparência e Inovação Pública — Digov, fortalecendo ainda mais a estrutura de gestão de riscos.

Com a criação da Digov, a Política de Gestão de Riscos do IFMS foi revisada e atualizada com o objetivo de estabelecer diretrizes para uma abordagem integrada e promover a disseminação de uma cultura organizacional voltada à gestão de riscos em todas as instâncias institucionais. Como complemento a essa ação, este Manual foi elaborado para apresentar, aos(às) servidores(as), as normas e os conceitos básicos relacionados ao tema, a estrutura da gestão de riscos, a metodologia do processo de gerenciamento de riscos e a ferramenta tecnológica que deve ser utilizada nesse contexto.

Embora o foco principal deste Manual sejam os processos de trabalho, a gestão de riscos aqui descrita pode ser adaptada a políticas institucionais, procedimentos operacionais padrão, serviços e projetos. Desse modo, espera-se que este documento seja um referencial para consultas rápidas e se torne uma ferramenta prática e de fácil entendimento, com foco no apoio a servidores(as) quanto ao aprimoramento contínuo da gestão de riscos na instituição.

2 NORMATIVOS RELACIONADOS

A gestão de riscos na administração pública federal é guiada por um conjunto de normas e regulamentações, às quais se somam os documentos elaborados pelo IFMS, conforme disposto a seguir:

i. Legislação Federal:

a) Instrução Normativa Conjunta MP/CGU nº 1, de 2016 - dispõe sobre controles internos, gestão de riscos e governança no âmbito do poder executivo federal; e

b) Decreto nº 9.203, de 2017 - dispõe sobre a política de governança da administração pública federal direta, autárquica e fundacional.

ii. Documentos Institucionais:

a) Portaria IFMS nº 771, de 11 de maio de 2018 - institui o Programa de Integridade do IFMS;

b) Resolução COSUP/IFMS nº 1, de 21 de janeiro de 2025 - atualiza a Política de Gestão de Riscos do IFMS; e

c) Portaria/Reitoria IFMS nº 1.311, de 7 de novembro de 2023 - institui o Comitê de Governança, Gestão de Riscos e Controle Interno do IFMS.

iii. Normas Técnicas:

a) ABNT NBR ISO 31000:2018 - fornece diretrizes para gerenciar riscos enfrentados pelas organizações;

b) ABNT NBR ISO/IEC 31010:2021 - fornece orientação para a seleção e aplicação de várias técnicas que podem ser usadas para ajudar a melhorar o modo como a incerteza é considerada e a entender o risco; e

c) ABNT NBR ISO 31073:2022 - define termos genéricos relacionados à gestão de riscos enfrentados pelas organizações.

A lista apresentada, embora não seja exaustiva, fornece uma base para a implementação da gestão de riscos na instituição. Todavia, são normativos sujeitos a alterações, o que torna fundamental o acompanhamento contínuo de publicações a eles relacionadas, bem como a revisão periódica de documentos institucionais.

3 CONCEITOS

De forma concisa, os conceitos básicos relacionados à gestão de riscos, com base na norma ABNT NBR ISO 31073:2022 e na Instrução Normativa Conjunta MP/CGU nº 1, de 2016, são:

i. Aceitação do risco: é uma decisão consciente de assumir um risco específico, podendo ocorrer sem o tratamento do risco ou durante o processo de tratamento de riscos;

ii. Ação de evitar o risco: decisão informada de não se envolver ou retirar-se de uma atividade, a fim de não ser exposto a um risco específico;

iii. Apetite ao risco: nível de risco que uma organização está disposta a aceitar;

iv. Avaliação de riscos: processo de comparar os resultados da análise de riscos com os critérios de risco para determinar se o risco é aceitável ou tolerável;

v. Consequência: resultado de um evento que afeta os objetivos;

vi. Contexto externo: ambiente externo no qual a organização busca atingir seus objetivos;

vii. Contexto interno: ambiente interno no qual a organização busca atingir seus objetivos;

viii. Controle de risco: medida que mantém ou modifica o risco;

ix. Controles internos da gestão: conjunto integrado de regras, procedimentos, diretrizes, protocolos, rotinas de sistemas informatizados, conferências e trâmites de documentos e informações. Esses elementos, coordenados pela direção e por servidores(as), garantem a redução de riscos e o cumprimento da missão da entidade;

x. Compartilhamento de riscos: forma de tratamento de riscos que envolve a distribuição acordada de riscos com outras partes;

xi. Evento de risco: ocorrência que pode ter um impacto positivo ou negativo em um objetivo;

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

xiii. Gestão de riscos: atividades coordenadas para dirigir e controlar uma organização no que se refere a riscos;

xiv. Gestores(as) de riscos: responsáveis por coordenar as atividades de gestão de riscos em uma organização;

xv. Identificação de riscos: processo de busca, reconhecimento e descrição de riscos;

xvi. Medidas de contingência ou prevenção: ações para minimizar as consequências ou evitar a ocorrência de um evento de risco;

xvii. Mensuração de risco: estimativa da importância de um risco e cálculo da probabilidade e do impacto de sua ocorrência;

xviii. Monitoramento de riscos: verificação, supervisão, observação crítica ou identificação da situação, executadas de forma contínua, a fim de identificar mudanças no nível de desempenho requerido ou esperado;

xix. Nível de risco: magnitude de um risco ou combinação de riscos, expressa em termos da combinação das consequências e de suas probabilidades;

xx. Oportunidade: combinação de circunstâncias as quais se espera que sejam favoráveis aos objetivos;

xxi. Política de Gestão de Riscos: declaração das intenções e diretrizes de uma organização relacionadas à gestão de riscos;

xxii. Probabilidade: medida da chance de ocorrência expressa como um número entre 0 e 1, onde 0 é a impossibilidade e 1 é certeza absoluta;

xxiii. Processo de gestão de riscos: processo global de identificação de riscos, análise de riscos e avaliação de riscos;

xxiv. Parte interessada: *stakeholder* - pessoa ou organização que pode afetar, ser afetada, ou perceber-se afetada por uma decisão ou atividade;

xxv. Proprietário de riscos: pessoa ou entidade com a responsabilização e a autoridade para gerenciar riscos;

xxvi. Reporte de riscos: forma de comunicação destinada a informar partes interessadas específicas, internas ou externas, fornecendo informações relativas ao estado atual do risco e à sua gestão;

xxvii. Responsáveis por unidades: responsáveis por coletar informações e implementar a gestão de riscos em suas áreas;

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

xxix. Risco inerente: risco ao qual uma organização está exposta sem considerar quaisquer ações gerenciais que possam reduzir a probabilidade de sua ocorrência ou seu impacto;

xxx. Risco residual: risco ao qual uma organização está exposta após a implementação de ações gerenciais para o tratamento do risco;

xxxi. Tolerância ao risco: refere-se à disposição da organização ou das partes interessadas em suportar o risco residual para alcançar seus objetivos. A tolerância ao risco pode ser influenciada por requisitos legais ou regulatórios; e

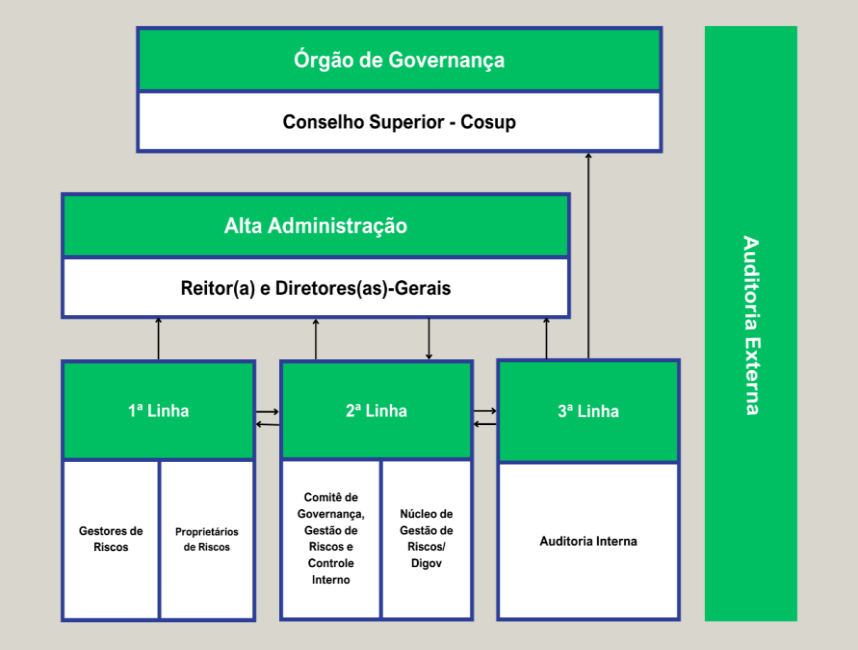
xxxii. Tratamento de riscos: processo para modificar os riscos.

Para outros conceitos ou uma compreensão mais detalhada, recomenda-se a consulta aos documentos citados no início desta seção, que oferecem maior profundidade e abrangência sobre o tema.

4 ESTRUTURA DE GESTÃO DE RISCOS

No IFMS, a estrutura de gestão de riscos segue o modelo de Três Linhas, proposto pelo *The Institute of Internal Auditors* — IIA em 2013 e revisado em 2020. A implementação desse modelo, com as devidas adaptações para se adequar às estruturas de governança do IFMS, está ilustrada na Figura 1.

Figura 1 - Modelo de Três Linhas para gestão de riscos



Legenda: ↑: Prestação de contas e reporte | ↓: Delegação, orientação, recursos e supervisão | ↔: Alinhamento, comunicação, coordenação e colaboração.
Fonte: adaptado de IAA (2020, p. 4) [1].

Em 2020, o IIA atualizou o modelo, removendo o termo “de defesa” das linhas, enfatizando uma abordagem mais proativa e não apenas reativa para garantir o alcance dos objetivos organizacionais e fortalecer a governança[2].

[1] *THE INSTITUTE OF INTERNAL AUDITORS* (IIA). **Modelo das três linhas do IIA 2020:** uma atualização das três linhas de defesa. *The Institute of Internal Auditors*/ Instituto dos Auditores Internos do Brasil, 2020. Disponível em: https://iiabrasil.org.br/korbilload/upl/editorHTML/uploadDireto/20200758glob-th-editorHTML-00000013-20082020141130.pdf. Acesso em: 12 nov. 2024.

[2] UNIVERSIDADE FEDERAL DE SANTA CATARINA (UFSC). **Manual para elaboração do plano de Gestão de Riscos**. Florianópolis: UFSC, 2020. Disponível em: https://gestaoderiscos.paginas.ufsc.br/files/2020/05/Manual-Plano-de-Gest%C3%A3o-de-Riscos-v10-NOVO-c.pdf. Acesso em: 10 nov. 2024.

O modelo das Três Linhas é uma abordagem eficaz para melhorar a comunicação no gerenciamento de riscos e controle, esclarecendo papéis e responsabilidades[3]. A primeira linha é responsável pelo gerenciamento direto dos riscos, enquanto a segunda, atuando como guardiã do processo, supervisiona e incentiva a prática correta. A terceira linha, a Auditoria Interna, avalia as duas primeiras. Cada uma dessas linhas tem papel distinto dentro da governança organizacional.

A estrutura em linhas não implica uma ordem hierárquica, uma vez que as funções podem ser desempenhadas simultaneamente. O processo de interação entre as linhas e as instâncias de governança envolve aspectos como responsabilização, reporte, supervisão, alinhamento e comunicação[4].

No IFMS, a primeira linha é formada por Gestores(as) de Riscos e Proprietários(as) de Risco, responsáveis por identificar, avaliar, tratar e monitorar os riscos em suas respectivas áreas, utilizando ferramentas e metodologias definidas pela 2ª linha. A 1ª linha também é responsável por implementar os controles internos, garantir a conformidade com as políticas e diretrizes estabelecidas e comunicar os resultados à 2ª linha. A segunda linha inclui o Comitê de Governança, Gestão de Riscos e Controle Interno, além da Digov e o Núcleo de Gestão de Riscos, responsáveis por definir as diretrizes para a gestão de riscos; aprovar a metodologia e ferramentas a serem utilizadas na gestão de riscos; analisar os relatórios de gestão de riscos e os resultados das auditorias; supervisionar o funcionamento da 1ª linha e garantir a implementação da Política de Gestão de Riscos e diretrizes; subsidiar a alta administração para tomada de decisões estratégicas relacionadas à gestão de riscos, bem como realizar acompanhamento contínuo das atividades da 1ª linha, analisando os indicadores de desempenho e os relatórios de gestão de riscos. A terceira linha é representada pela Auditoria Interna — Audit, responsável por realizar auditorias independentes e objetivas sobre a eficácia da gestão de riscos, verificar a conformidade das operações com as políticas, diretrizes e normas aplicáveis, e comunicar os resultados à alta administração e aos órgãos de governança.

A Alta Administração e o Órgão de Governança, embora não estejam diretamente integrados às Três Linhas, são as principais partes interessadas e estão em posição privilegiada para assegurar que o modelo de gerenciamento de riscos e controle seja adequadamente implementado nos processos da organização.

---

[3] BRASILIANO, Antonio Celso Ribeiro. **Inteligência em riscos:** gestão integrada em riscos corporativos. 2. ed. rev. e ampl. São Paulo: Sicurezza, 2018. *E-book*. Disponível em: https://www.brasiliano.com.br/ebook-inteligencia-em-riscos. Acesso em: 17 nov. 2024.

[4] *THE INSTITUTE OF INTERNAL AUDITORS* (IIA). **Modelo das três linhas do IIA 2020:** uma atualização das três linhas de defesa. *The Institute of Internal Auditors*/ Instituto dos Auditores Internos, 2020. Disponível em: https://iiabrasil.org.br/korbilload/upl/editorHTML/uploadDireto/20200758glob-th-editorHTML-00000013-20082020141130.pdf. Acesso em: 12 nov. 2024.

A Auditoria Externa visa atender às expectativas regulatórias e apoiar a gestão na melhoria dos processos internos[5]. Nesse contexto, o Tribunal de Contas da União — TCU e a Controladoria-Geral da União — CGU desempenham papéis cruciais no fortalecimento dos controles internos e na gestão de riscos nas instituições públicas.

[5] MIRANDA, Rodrigo Fontenelle de A. **Implementando a gestão de riscos no setor público**. 2. ed. Belo Horizonte: Fórum, 2023.

5 METODOLOGIA DE GERENCIAMENTO DE RISCOS

Conforme a Instrução Normativa Conjunta MP/CGU nº 1, de 2016, o gerenciamento de riscos é um processo estruturado para identificar, avaliar, tratar e monitorar potenciais eventos ou situações que possam impactar negativamente os objetivos organizacionais. Esse processo deve ser utilizado por todas as unidades organizacionais da instituição, como forma de lidar com as incertezas e garantir o alcance dos objetivos institucionais.

Para o processo de gerenciamento de riscos no IFMS, o Comitê de Governança, Gestão de Riscos e Controle Interno decidiu adotar a norma técnica ABNT ISO 31000:2018. A norma oferece um processo consistente e uma estrutura abrangente para garantir que o risco seja gerenciado de forma eficaz, eficiente e coerente, o que justifica sua escolha, visto que havia a necessidade de adoção de um modelo abrangente e reconhecido nacionalmente, capaz de atender às demandas e aos desafios da instituição.

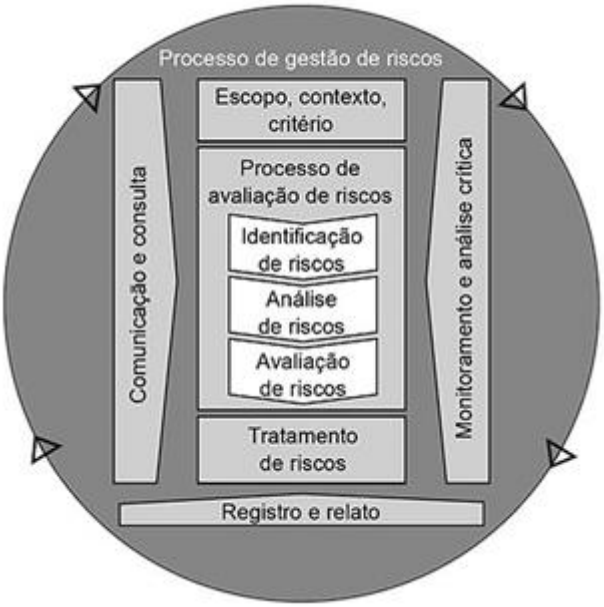
A abordagem da NBR ISO 31000:2018 é genérica e fornece princípios e diretrizes para gerenciar qualquer forma de risco de maneira sistemática, transparente e confiável, em qualquer escopo e contexto[6]. Sua metodologia é composta pelas seguintes etapas: escopo, contexto e critério; identificação, análise e avaliação de riscos (processo de avaliação de riscos); tratamento de riscos; monitoramento e análise crítica; comunicação e consulta; e registro e relato. Cada etapa visa atingir os objetivos específicos do processo de gerenciamento de riscos.

Para implementar o processo de gerenciamento de riscos, deve-se, primeiramente, definir o processo de trabalho, a meta ou o objetivo que será analisado. Os processos de trabalho a serem avaliados precisam estar devidamente mapeados, enquanto as metas ou os objetivos devem, preferencialmente, ser estabelecidos institucionalmente por meio do planejamento estratégico, tático ou operacional.

Conforme estabelecido pela NBR ISO 31000:2018, a estrutura completa do processo de gerenciamento de riscos segue representada na Figura 2.

[6] BRASILIANO, Antonio Celso Ribeiro. **Inteligência em riscos:** gestão integrada em riscos corporativos. 2. ed. rev. e ampl. São Paulo: Sicurezza, 2018. E-book. Disponível em: https://www.brasiliano.com.br/ebook-inteligencia-em-riscos. Acesso em: 17 nov. 2024.

Figura 2 - Processo de gerenciamento de riscos



Fonte: Norma ABNT NBR ISO 31000:2018 (2018, p. 9).

Com base na NBR ISO 31000:2018, o entendimento do contexto envolve a captura dos objetivos relacionados ao processo de trabalho, bem como a análise dos ambientes interno e externo nos quais a instituição busca atingir seus objetivos. Isso permite uma compreensão clara do contexto e uma visão abrangente dos fatores que podem influenciar a capacidade da instituição de alcançar os resultados planejados[7].

Para a análise do contexto, entre outros modelos de ferramentas disponíveis, destaca-se a matriz SWOT. A análise SWOT - sigla para os termos da língua inglesa *Strengths* (Forças), *Weaknesses* (Fraquezas), *Opportunities* (Oportunidades) e *Threats* (Ameaças) - é uma ferramenta de planejamento de entidades, projetos, processos e ações. Essa ferramenta é aplicável a diferentes tipos de análises de cenários, sendo um sistema simples destinado a posicionar ou verificar a posição estratégica do objeto em análise, no ambiente em questão[8]. A Figura 3 detalha de maneira sintética as características analisadas nessa técnica.

[7] BRASIL, Controladoria-Geral da União (CGU). **Curso de Introdução à Gestão de Riscos:** módulo 7: monitoramento e comunicação. [*S. l.*: *s. n.*], 2024.

[8] DISTRITO FEDERAL. Controladoria-Geral do Distrito Federal. **Projeto Gestão de Riscos:** estabelecimento de escopo, contexto e critério. Brasília: Controladoria-Geral do Distrito Federal, 2021. Disponível em: https://www.gestaoderiscos.cg.df.gov.br/wp-content/uploads/2022/01/Modelo-de-artefato-Estabelecimento-de-Escopo-Contexto-e-Crit%C3%A9rio-para-Gest%C3%A3o-de-Riscos.pdf. Acesso em: 18 nov. 2024.

Figura 3 – Modelo da ferramenta análise SWOT

Fonte: elaboração própria, 2024.

Conforme mencionado, antes de partir para a identificação de riscos, deve-se ter em mente o objetivo ou a meta que se deseja alcançar com o processo, projeto ou qualquer que seja o foco do gerenciamento de riscos. Segundo a ISO 31000:2018, a identificação de riscos tem como objetivo "encontrar, reconhecer e descrever riscos que possam ajudar ou impedir que uma organização alcance seus objetivos."[9].

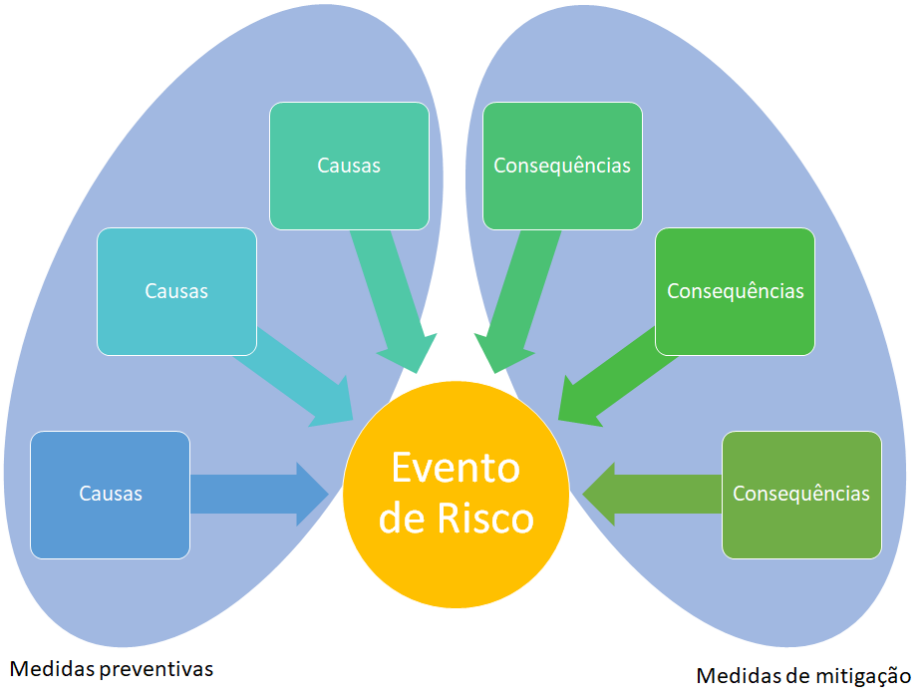
A organização pode utilizar diversas técnicas para identificar os riscos que podem afetar um ou mais objetivos. Entre essas técnicas, estão o diagrama de *Ishikawa*, também conhecido como diagrama de espinha de peixe, e o método de análise *Bow Tie*, além de outras técnicas previstas na norma ISO 31010:2021. As Figuras 4 e 5 ilustram a aplicação do diagrama de espinha de peixe e do método *Bow Tie*.

[9] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR 31000:** gestão de riscos: diretrizes. 2. ed. São Paulo: ABNT, 2018, p. 12.

Figura 4 - Exemplo do diagrama de espinha de peixe

Fonte: Enap (2024, n. p) [10].

Figura 5 - Exemplo da ferramenta *Bow Tie*



Fonte: elaboração própria, 2024.

[10] ESCOLA NACIONAL DE ADMINISTRAÇÃO PÚBLICA - ENAP. **Gestão de riscos nas contratações públicas**. [*S. l.: s. n.*], 2024.

Para a descrição de um risco, o Tribunal de Contas da União — TCU sugere a aplicação de uma sintaxe, ou seja, uma estrutura específica para organizar as informações de forma lógica e coesa. Essa estrutura deve incluir os seguintes aspectos: Devido à <CAUSA/FONTE>, poderá acontecer <DESCRIÇÃO DO EVENTO DE RISCO>, o que poderá levar à <DESCRIÇÃO DO IMPACTO/CONSEQUÊNCIA, EFEITO>, impactando na <DIMENSÃO DE OBJETIVO IMPACTADO>.[11]

Um exemplo prático dessa sintaxe pode ser obtido na seguinte situação: devido a não entrega de cotações de preços por parte de fornecedores(as), poderá acontecer a não participação da empresa em licitações, o que poderá levar à interrupção de atividades, impactando no custo e nas despesas fixas[12].

Após a identificação dos riscos, das causas e das consequências, é necessário identificar os controles presentes no processo que mitigam os riscos identificados. Esses controles podem ser classificados em preventivos; de atenuação e recuperação; e detectivos. Os controles preventivos atuam nas possíveis causas do risco para prevenir sua ocorrência, como, por exemplo, requisitos ou *checklists* definidos. Já os controles de atenuação e recuperação são executados após a ocorrência do risco, com o objetivo de diminuir o impacto de suas consequências, como planos de contingência e procedimentos apuratórios. Os controles detectivos, por sua vez, têm a função de identificar a materialização do risco ou sua iminência, como indicadores e sensores.
Para a classificação do tipo de risco, são utilizadas as tipologias descritas no Quadro 1.

Quadro 1 - Tipologias de risco

Tipo de risco	Descrição
Riscos Estratégicos	Referem-se aos riscos associados às decisões de alto nível que afetam a instituição.
Riscos Operacionais	Referem-se aos riscos ligados às operações do dia a dia da instituição.
Riscos Financeiros/Orçamentários	Referem-se aos riscos que envolvem a gestão inadequada de fundos e recursos, podendo resultar em déficits orçamentários.
Riscos de Imagem/Reputação	Referem-se aos riscos relacionados à percepção pública do IFMS, que podem surgir de escândalos ou má gestão.
Riscos de Integridade	Referem-se aos riscos que envolvem questões éticas e de conduta, como fraude ou corrupção.
Riscos Legais/De Conformidade	Referem-se aos riscos de não cumprimento de leis e regulamentos.

Fonte: elaboração própria, 2024.

11 BRASIL, Controladoria-Geral da União (CGU). **Curso de Introdução à Gestão de Riscos:** módulo 7 - Monitoramento e comunicação. [*S. l.: s. n.*], 2024.

12 BRASIL, Controladoria-Geral da União (CGU). **Curso de Introdução à Gestão de Riscos:** módulo 7 - Monitoramento e comunicação. [*S. l.: s. n.*], 2024.

As tipologias apresentadas no Quadro 1 não são exaustivas, tendo em vista a constante evolução e a possibilidade de surgimento de outros tipos de riscos, como, por exemplo, aqueles relacionados à tecnologia da informação.

Após a identificação dos eventos que possam comprometer os objetivos do processo de trabalho, inicia-se a fase de análise e avaliação de riscos. Nessa etapa, são determinados os níveis dos riscos identificados, considerando duas dimensões principais: a probabilidade e o impacto. A organização realiza a avaliação dos eventos, levando em consideração tanto os riscos inerentes quanto os riscos residuais.

Nessa etapa, deve-se também considerar o limite de exposição a riscos da instituição, comparando os parâmetros estabelecidos ao nível de riscos. Isso é essencial para determinar se o risco é aceitável ou não. Para essa avaliação, é necessário consultar a declaração de apetite a riscos da instituição.

Para cada risco identificado, são atribuídos pesos de probabilidade e impacto, resultando no valor do risco. Com esse valor, utiliza-se a matriz de riscos (Figura 6) para classificar qualitativamente o valor do risco, conforme os níveis de risco estabelecidos (Quadro 2). Esses níveis determinam quando os riscos são considerados extremos, altos, médios ou baixos.

Figura 6 - Matriz de riscos

Matriz de Riscos						
Probabilidade	Muito Alta	5	5-Moderado	10-Alto	15-Crítico	20-Crítico	25-Crítico
	Alta	4	4-Moderado	8-Alto	12-Alto	16-Crítico	20-Crítico
	Moderada	3	3-Pequeno	6-Moderado	9-Alto	12-Alto	15-Crítico
	Baixa	2	2-Pequeno	4-Moderado	6-Moderado	8-Alto	10-Alto
	Muito Baixa	1	1-Pequeno	2-Pequeno	3-Pequeno	4-Moderado	5-Moderado
			1	2	3	4	5
			Insignificante	Pequeno	Moderado	Grande	Catastrófico
			Impacto				

Fonte: adaptado da Matriz de Riscos da CGU (Brasil, 2021, p. 27-28). [13]

[13] BRASIL. Controladoria-Geral da União. Gabinete do Ministro. Núcleo de Gestão de Riscos e Integridade (NGRI). **Metodologia de Gestão de Riscos da CGU [versão 2.0]**. Distrito Federal (DF): CGU, 2021. Disponível em: https://www.gov.br/servidor/pt-br/acesso-a-informacao/gestao-de-pessoas/desempenho-e-desenvolvimento-de-pessoas/pndp-1/MGI_CartilhaGestaoRiscosPDP20240326.pdf/view. Acesso em: 12 nov. 2024.

Quadro 2 - Grau dos riscos

NÍVEL	VALOR	SÍMBOLO
CRÍTICO	MAIOR OU IGUAL A 15	
ALTO	MAIOR OU IGUAL A 8 E MENOR QUE 12	
MODERADO	MAIOR OU IGUAL A 4 E MENOR QUE 6	
PEQUENO	MENOR QUE 4	

Fonte: elaboração própria, 2024.

Uma vez mensurado o risco, é necessário identificar e avaliar os controles que respondam aos eventos de riscos identificados. Atividades de controle são as políticas e os procedimentos estabelecidos e executados para reduzir os riscos que a unidade tenha optado por responder.

As ações para responder aos eventos de risco devem estar alinhadas com o apetite ao risco estabelecido pelo Comitê de Governança, Gestão de Riscos e Controle Interno do IFMS. Isso significa que as respostas devem respeitar o nível de risco que o IFMS está disposto a aceitar.

Na prática, o tratamento de cada risco é definido pelos(as) Proprietários(as) dos Riscos, após análise das informações com os(as) Gestores(as) de Riscos, para determinação da resposta mais adequada, podendo envolver mitigar, aceitar, transferir ou evitar os riscos. Essa definição deve observar o apetite a riscos institucional previamente estabelecido por meio da Declaração de Apetite ao Risco.

Além disso, a escolha da resposta deve ser fundamentada em uma análise detalhada de custo-benefício, prazos, responsáveis e na possibilidade de surgimento de outros eventos de risco, considerando que o tratamento de riscos é um processo iterativo.

Para os riscos que necessitam de tratamento, recomenda-se a elaboração do Plano de Tratamento, com propostas de controles. O Plano de Tratamento é um conjunto de ações necessárias para adequar os níveis de riscos, por meio da adoção de novos controles ou da otimização dos controles atuais do processo, de modo que devem ser considerados aspectos como relação custo-benefício, prazos, responsáveis, alcance, eficiência, complexidade, prioridade, entre outros.

Entre as ferramentas disponíveis para a elaboração do Plano de Tratamento, sugere-se a utilização da metodologia 5W2H, devendo ser levado em consideração o nível de risco e as diretrizes para resposta.

Após a definição dos tratamentos, deve-se realizar o monitoramento contínuo. As ações de monitoramento dos riscos são preenchidas pelos(as) Proprietários(as) de Risco após análise das informações com os(as) Gestores(as) de Riscos, no mínimo semestralmente[14].

A fase do monitoramento inclui a revisão e análise periódica do gerenciamento de riscos para promover aprimoramentos constantes. Durante essa fase, são efetuadas verificações, supervisões, observações críticas e identificação contínua da situação dos riscos para avaliar a eficácia dos controles internos e alcançar os objetivos estabelecidos. No IFMS, o monitoramento do gerenciamento de riscos deve ser registrado no sistema ForRisco.

A etapa da comunicação é caracterizada pela troca de informações entre as instâncias de gestão de riscos, o que viabiliza a melhoria contínua e a evolução da maturidade do órgão. Seu objetivo é garantir uma compreensão clara e objetiva, necessária para a tomada de decisões envolvendo riscos. Ao mesmo tempo, a consulta visa obter *feedback* e informações que auxiliem nesse processo decisório.

O fluxo de comunicação e consulta deve garantir a divulgação no momento e tempo apropriados, assegurando que os objetivos sejam claros para que as pessoas envolvidas compreendam os riscos e executem as ações necessárias para mitigá-los.

Sobre a etapa de registro e relato, é conveniente que o processo de gerenciamento de riscos e seus resultados sejam documentados e relatados por meio de mecanismos apropriados, pois que objetivam: comunicar atividades e resultados do gerenciamento de riscos em toda a organização; fornecer informações para a tomada de decisão; melhorar as atividades de gestão; e auxiliar a interação com as partes integradas, incluindo aquelas com responsabilidade e com responsabilização por atividades da eficácia de riscos e controles internos[15].

[14] UNIVERSIDADE FEDERAL DO AMAZONAS (UFAM). **Manual de Gestão de Riscos da UFAM**. Manaus: UFAM, 2023. Disponível em: https://edoc.ufam.edu.br/bitstream/123456789/7116/1/Manual_de_Gestao_de_Riscos_da_Ufam_1%C2%AA_Edicao.pdf.pdf. Acesso em: 12 ago. 2024.

[15] BRASILIANO, Antonio Celso Ribeiro. **Inteligência em riscos: gestão integrada em riscos corporativos**. 2. ed. rev. e ampl. São Paulo: Sicurezza, 2018. *E-book*. Disponível em: https://www.brasiliano.com.br/ebook-inteligencia-em-riscos. Acesso em: 17 nov. 2024.

6 FERRAMENTA DE GERENCIAMENTO DE RISCOS

Com o objetivo de sistematizar e padronizar os procedimentos de gerenciamento de riscos, o IFMS realizou processo de seleção e análise para escolher a ferramenta mais adequada às necessidades institucionais.

Inicialmente, realizou-se levantamento de *softwares* disponíveis no mercado, priorizando soluções gratuitas e alinhadas às necessidades da instituição. Entre as opções encontradas, destacam-se os sistemas Ágatha e o ForRisco. Em seguida, foi realizada uma análise comparativa desses sistemas para identificar as principais diferenças entre eles, com base nos critérios apresentados no Quadro 3.

Quadro 3 - Comparativo entre os sistemas Ágatha e ForRisco

Características	**Sistema Ágatha**	**Sistema ForRisco**
Custo	Gratuito	Gratuito
Manutenção	Responsabilidade da instituição usuária	Manutenção em nuvem pela Rede Nacional de Ensino e Pesquisa (RNP)
Atualizações	Não há previsão	Contínuas e baseadas em *feedback* dos usuários
Integração com outros sistemas	Não identificada	Integração com o ForPDI
Suporte técnico	Oferecido pela instituição usuária	Oferecido pela RNP
Funcionalidades	Amplas funcionalidades	Amplas funcionalidades

Fonte: elaboração própria, 2024.

Além dos sistemas Ágatha e ForRisco, também foi considerada uma planilha documentadora. No entanto, essa ferramenta manual de gerenciamento de riscos não foi incluída no Quadro 3 devido às limitações em comparação aos sistemas informatizados.

Após a análise das opções referidas, o Comitê de Governança, Gestão de Riscos e Controle Interno optou, por unanimidade, pelo sistema ForRisco. A decisão considerou a atualização contínua, a integração com o ForPDI, o suporte técnico especializado e a ampla adoção na Rede Federal de Educação, além da manutenção e atualização pelo Ministério da Educação — MEC, em parceria com a Rede Nacional de Ensino e Pesquisa, entre outras funcionalidades que garantem o alinhamento com as melhores práticas de gestão de riscos.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR 31000:** gestão de riscos: diretrizes. 2. ed. São Paulo: ABNT, 2018.

BRASIL. Controladoria-Geral da União. Gabinete do Ministro. Núcleo de Gestão de Riscos e Integridade (NGRI). **Metodologia de Gestão de Riscos da CGU [versão 2.0]**. Distrito Federal (DF): CGU, 2021. Disponível em: https://www.gov.br/servidor/pt-br/acesso-a-informacao/gestao-de-pessoas/desempenho-e-desenvolvimento-de-pessoas/pndp-1/MGI_CartilhaGestaoRiscosPDP20240326.pdf/view. Acesso em: 12 nov. 2024.

BRASIL. Controladoria-Geral da União (CGU). **Curso de Introdução à Gestão de Riscos:** módulo 7: monitoramento e comunicação. [*S. l.*: *s. n.*], 2024.

BRASILIANO, Antonio Celso Ribeiro. **Inteligência em riscos:** gestão integrada em riscos corporativos. 2. ed. rev. e ampl. São Paulo: Sicurezza, 2018. E-book. Disponível em: https://www.brasiliano.com.br/ebook-inteligencia-em-riscos. Acesso em: 17 nov. 2024.

DISTRITO FEDERAL. Controladoria-Geral do Distrito Federal. **Projeto Gestão de Riscos:** estabelecimento de escopo, contexto e critério. Brasília: Controladoria-Geral do Distrito Federal, 2021. Disponível em: https://www.gestaoderiscos.cg.df.gov.br/wp-content/uploads/2022/01/Modelo-de-artefato-Estabelecimento-de-Escopo-Contexto-e-Crit%C3%A9rio-para-Gest%C3%A3o-de-Riscos.pdf. Acesso em: 18 nov. 2024.

ESCOLA NACIONAL DE ADMINISTRAÇÃO PÚBLICA - ENAP. **Gestão de riscos nas contratações públicas**. [*S. l.: s. n.*], 2024.

MIRANDA, Rodrigo Fontenelle de A. **Implementando a gestão de riscos no setor público**. 2. ed. Belo Horizonte: Fórum, 2023.

THE INSTITUTE OF INTERNAL AUDITORS (IIA). **Modelo das três linhas do IIA 2020:** uma atualização das três linhas de defesa. *The Institute of Internal Auditors*, 2020. Disponível em: https://iiabrasil.org.br/korbilload/upl/editorHTML/uploadDireto/20200758glob-th-editorHTML-00000013-20082020141130.pdf. Acesso em: 12 nov. 2024.

UNIVERSIDADE FEDERAL DE SANTA CATARINA (UFSC). **Manual para elaboração do plano de Gestão de Riscos**. Florianópolis: UFSC, 2020. Disponível em: https://gestaoderiscos.paginas.ufsc.br/files/2020/05/Manual-Plano-de-Gest%C3%A3o-de-Riscos-v10-NOVO-c.pdf. Acesso em: 10 nov. 2024.

UNIVERSIDADE FEDERAL DO AMAZONAS (UFAM). **Manual de Gestão de Riscos da UFAM**. Manaus: UFAM, 2023. Disponível em:

https://edoc.ufam.edu.br/bitstream/123456789/7116/1/Manual_de_Gestao_de_Riscos_da_Ufam_1%C2%AA_Edicao.pdf.pdf. Acesso em: 12 ago. 2024.