CAPES

Metodologia de Gestão de Riscos da CAPES

2ª Edição - Março 2026

EXPEDIENTE

COMITÊ INTERNO DE GOVERNANÇA

Presidente

Denise Pires de Carvalho

Diretor de Avaliação da Pós-Graduação (DAV)

Antonio Gomes de Souza Filho

Diretora de Formação de Professores da Educação Básica (DEB)

Marcia Serra Ferreira

Diretora de Informação Científica e Estudos Avançados (DICE)

Daniela Freddo

Diretor de Articulação e Inovação em Educação Aberta (DIEA)

Antonio Carlos Rodrigues de Amorim

Diretor de Programas e Bolsas no País (DPB)

Luiz Antonio Pessan

Diretor de Relações Internacionais (DRI)

Rui Vicente Oppermann

Diretora de Gestão (DGES)

Luciana Mendonça Gottschall

Diretor de Tecnologia da Informação (DTI)

Gustavo Jardim Portella

CONSOLIDAÇÃO DO CONTEÚDO

Chefe da Assessoria de Governança e Desenvolvimento Institucional (ASGDI)

Yuri Ghobad da Silva

Coordenador de Assuntos Estratégicos Institucionais (CAES/ASGDI)

Elivelton Oliveira Santa Cruz

Coordenação de Assuntos Estratégicos Institucionais (CAES/ASGDI)
Caroline Venâncio Aires

CONSULTORIA EM GESTÃO DE RISCOS
Auditor-Chefe
Germano de Oliveira Farias

Equipe da Auditoria Interna da CAPES
Brunna Hisla da Silva Sena
Daniela Amorim Meira
Patrícia Reis Paiva

ENDEREÇO
Fundação Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – CAPES
Setor Bancário Norte (SBN), Quadra 2, Bloco L, Lote 06, Edifício CAPES
CEP 70040-031 – Brasília/DF.

Sumário

LISTA DE FIGURAS

LISTA DE QUADROS

Apresentação

A Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES) tem, ao longo dos anos, buscado aprimorar suas práticas de governança institucional. Nesse contexto, a Gestão de Riscos se apresenta como um instrumento essencial para a melhoria contínua.

A gestão de riscos tem como objetivo garantir que as incertezas não desviem a organização de seus objetivos, levando em consideração os riscos inerentes às atividades institucionais, às novas realidades, às mudanças sociais, às dinâmicas da administração pública e aos requisitos legais e regulatórios. Ao criar e proteger valor, a gestão de riscos contribui significativamente para a melhoria dos resultados da gestão e para o cumprimento dos objetivos institucionais.

Com o intuito de assegurar que a CAPES atinja seus objetivos institucionais, foi desenvolvida a Metodologia de Gestão de Riscos da CAPES, a qual está apresentada neste guia.

O objetivo deste material é promover uma compreensão mais aprofundada sobre a gestão de riscos, facilitar a disseminação do conhecimento sobre o processo na CAPES e apresentar a metodologia institucional adotada.

A presente metodologia detalha as atividades envolvidas no processo de gestão de riscos, promovendo autonomia e eficiência na sua aplicação em processos organizacionais, podendo ser utilizada em diversos níveis institucionais.

Esta é a segunda versão da metodologia de gestão de riscos da CAPES, aprimorada a partir de um ensaio de gestão de riscos realizado pela Assessoria de Governança e Desenvolvimento Institucional (ASGDI). O Ensaio consistiu na aplicação prática da metodologia em um processo da cadeia de valor da CAPES executado pela ASGDI e foi realizado pela própria Assessoria com o apoio da Auditoria Interna da CAPES (AUD) e da Controladoria-geral da União (CGU), nos papeis de consultoria e assessoria, respectivamente.

O aprimoramento da metodologia resultou em alterações de procedimentos, dinâmicas e análises nas etapas da metodologia. Essas alterações tiveram o intuito de contribuir para o refinamento da aplicabilidade da gestão de riscos na CAPES e para esclarecer os conceitos utilizados.

1. Introdução

No setor público, a gestão de riscos tem como objetivo fornecer à administração instrumentos para enfrentar as incertezas e suas implicações. Ela abrange tanto riscos quanto oportunidades, sempre com foco no interesse público. Essa prática favorece o uso eficiente, eficaz e efetivo dos recursos, promove a transparência e fortalece a imagem institucional.

Além disso, a gestão de riscos também busca ampliar a capacidade organizacional de enfrentar eventos inesperados e proporcionar uma tomada de decisão mais racional por parte dos gestores. Portanto, está diretamente ligada ao princípio constitucional da eficiência (TCU, 2020).

Com a publicação da Instrução Normativa Conjunta CGU/MP nº 01/2016, que dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo federal, e do Decreto nº 9.203/2017, que estabelece a política de governança da administração pública federal direta, autárquica e fundacional, a CAPES deu início ao processo de institucionalização da gestão de riscos com a publicação da Portaria CAPES nº 37, de 20 de fevereiro de 2018. Essa portaria instituiu a Política de Gestão de Riscos da CAPES e levou à criação do Comitê de Governança, Riscos e Controles, embora a metodologia não tenha sido efetivamente implementada à época.

O aprimoramento contínuo dos normativos federais evidenciou a necessidade de uma política de gestão de riscos mais atualizada e adequada ao contexto da CAPES. Assim, foi publicada a Portaria CAPES nº 301, de 22 de dezembro de 2022, a qual estabeleceu a Política de Gestão de Riscos e Controles Internos da entidade.

Essa nova política buscou alinhar-se à governança institucional e ao planejamento estratégico da CAPES e atribuiu competências conforme definido na Portaria CAPES nº 126, de 30 de junho de 2022, que instituiu a estrutura de governança da CAPES. Também foram adotadas em seu texto diversas medidas para sistematizar práticas relacionadas à gestão de riscos e controles internos, conforme as orientações dos normativos dos órgãos de controle.

Dentre as medidas, foi estabelecida a metodologia de gestão de riscos como forma de operacionalizar essa gestão. Sendo assim, novos esforços foram adotados para garantir uma implementação eficaz. O desenvolvimento dessa Metodologia foi fundamentado em *frameworks* internacionais, com destaque para a ISO 31000:2018, e em documentos de órgãos de referência no assunto, como o Tribunal de Contas da União (TCU) e a Controladoria-Geral da União (CGU).

Além disso, foram realizadas atividades de *benchmarking* em metodologias desenvolvidas por outros órgãos públicos. Essa prática é indicada no Roteiro de Avaliação de Maturidade da Gestão de Riscos do TCU (2018), que aponta que a adoção de padrões e boas práticas convencionadas em modelos de referência de gestão de riscos é uma forma eficaz de estabelecer uma abordagem sistemática, oportuna e estruturada para gestão de riscos, pois evita que sejam acumulados instrumentos e procedimentos burocráticos e desarticulados.

1.1. Principais Conceitos

Alta Administração: presidente da CAPES e seus diretores.

Apetite ao risco: nível de risco que a instituição está disposta a aceitar;

Causa: condição que possibilita a ocorrência de um risco, podendo ter origem tanto no ambiente interno quanto externo;

Consequência: efeito resultante de um risco que impacta direta ou indiretamente os objetivos do objeto em análise.

Controles internos: conjunto de regras, procedimentos e rotinas para enfrentar riscos e garantir a segurança na consecução dos objetivos.

Gestão de riscos: processo contínuo, estabelecido, direcionado e monitorado pela Alta Administração, que abrange as atividades de identificar, avaliar e gerenciar potenciais eventos que possam impactar a organização. Seu objetivo é proporcionar uma segurança adequada em relação à realização dos objetivos estabelecidos;

Gestor de riscos: é responsável por assegurar, por meio da aplicação de controles internos de gestão, o gerenciamento de riscos específicos, garantindo que estes se mantenham dentro do nível desejado e do apetite de risco da organização.

Governança: conjunto de mecanismos de liderança, estratégia e controle implementados para avaliar, direcionar e monitorar a gestão, com o objetivo de conduzir políticas públicas e prestar serviços de interesse da sociedade;

Impacto: mensuração qualitativa ou quantitativa do resultado ou efeito de um risco.

Macroprocesso: conjunto de processos interrelacionados e ordenados para o cumprimento de objetivos e metas da organização.

Matriz de risco: matriz gráfica que apresenta o conjunto de combinações de probabilidade e impacto e respectivas classificações.

Modelo das três linhas: estrutura que organiza as responsabilidades em três linhas: 1ª linha: identifica, avalia e mitiga riscos; 2ª linha: fornece metodologias, supervisiona e reporta; e 3ª linha: avalia de forma independente a governança e gestão de riscos.

Nível de Risco: magnitude do risco, resultante da combinação de probabilidade e impacto.

Objetivos estratégicos: fins a serem perseguidos pela organização para cumprir sua missão institucional e alcançar sua visão de futuro.

Objetos de gestão de riscos: qualquer instrumento que os gestores de riscos queiram implementar a gestão de riscos como processo de trabalho, projeto, programa, edital etc.

Política de Gestão de Riscos e Controles Internos: declaração de intenções e diretrizes gerais de uma organização relacionadas à gestão de riscos e controles internos;

Probabilidade: expressão da chance de um risco ocorrer.

Processo organizacional: conjunto de atividades correlacionadas desenvolvidas com o objetivo de gerar resultados claramente definidos para a organização.

Resposta ao risco: ação que deve ser tomada após o cálculo do nível de risco, a qual deve incluir as opções: mitigar, compartilhar, evitar ou aceitar.

Risco: possibilidade de ocorrência de um evento que possa impactar o alcance dos objetivos, sendo seu nível mensurado em termos de probabilidade e impacto;

Risco inerente: risco intrínseco ao objeto sem considerar quaisquer medidas de controle que possam reduzir a probabilidade de sua ocorrência ou seu impacto.

Risco residual: risco que permanece mesmo após a implementação de medidas de controle destinadas ao tratamento do risco.

Tipologia de Riscos: tipo ou grupo ao qual um risco está associado, podendo envolver uma ou múltiplas categorias simultaneamente.

Unidade organizacional: unidade administrativa na qual está inserido o objeto da gestão de riscos.

2. Política de Gestão de Riscos da CAPES

A CAPES estabeleceu a Política de Gestão de Riscos e Controles Internos, regulamentada pela Portaria CAPES nº 301/2022, como um mecanismo para aprimorar os processos de liderança, estratégia e controle da instituição. Por meio dessa política, a CAPES visa aprimorar o desempenho organizacional, garantindo ganhos em termos de entrega de resultados e no alcance dos objetivos institucionais.

Além de apoiar os gestores nas tomadas de decisões de forma mais racional e fundamentada, a política amplia a capacidade da CAPES de lidar com eventos inesperados. Outro propósito é estimular a transparência e promover o uso eficiente, eficaz e efetivo dos recursos, contribuindo para o fortalecimento da imagem da instituição perante a sociedade.

2.1. Princípios, diretrizes e objetivos

A Política de Gestão de Riscos e Controles Internos da CAPES estabelece que, em sua implementação, serão observados os princípios dispostos na Instrução Normativa Conjunta CGU/MP nº 1/2016, bem como os demais princípios emanados pelos órgãos de controle.

Os princípios estabelecidos na política da CAPES são:

Quadro 1 - Princípios vinculados à Gestão de Riscos

PRINCÍPIOS VINCULADOS À GESTÃO DE RISCOS
Gestão de Riscos realizada de forma sistemática, estruturada e oportuna, subordinada ao interesse público;
Estabelecimento de níveis de exposição a riscos adequados;
Estabelecimento de procedimentos de controle interno proporcionais ao risco, observada a relação custo-benefício, e destinados;
Utilização do mapeamento de riscos para apoio à tomada de decisão e à elaboração do planejamento estratégico;
Utilização da gestão de riscos para apoio à melhoria contínua dos processos organizacionais.

Fonte: art. 2º, inciso I da Portaria CAPES nº 301/2022.

Quadro 2 - Princípios vinculados aos Controles Internos

PRINCÍPIOS VINCULADOS AOS CONTROLES INTERNOS
Aderência à Integridade e a valores éticos;
Competência da Alta Administração em exercer a supervisão do desenvolvimento e do desempenho dos controles internos da gestão;
Coerência e harmonização da estrutura de competências e responsabilidades dos diversos níveis de gestão da entidade;
Compromisso da Alta Administração em atrair, desenvolver e reter pessoas com competências técnicas, em alinhamento com os objetivos da organização;
Clara definição dos responsáveis pelos diversos controles internos da gestão no âmbito da organização;
Mapeamento das vulnerabilidades que impactam os objetivos, de forma que sejam adequadamente identificados os riscos a serem geridos;
Identificação e avaliação das mudanças internas e externas à entidade que possam afetar significativamente os controles internos da gestão;
Desenvolvimento e implementação de atividades de controle que contribuam para a obtenção de níveis aceitáveis de riscos;
Adequado suporte de tecnologia da informação para apoiar a implementação dos controles internos da gestão;
Definição de políticas e normas que suportem as atividades de controles internos da gestão;
Utilização de informações relevantes e de qualidade para apoiar o funcionamento dos controles internos da gestão;
Definição de políticas e normas que suportem as atividades de controles internos da gestão;
Utilização de informações relevantes e de qualidade para apoiar o funcionamento dos controles internos da gestão;
Disseminação de informações necessárias ao fortalecimento da cultura e da valorização dos controles internos da gestão;
Realização de avaliações periódicas para verificar a eficácia do funcionamento dos controles internos da gestão;
Comunicação do resultado da avaliação dos controles internos da gestão aos responsáveis pela adoção de ações corretivas, incluindo a Alta Administração.

Fonte: art. 2º, inciso II da Portaria CAPES nº 301/2022.

A Política de Gestão de Riscos e Controles Internos da CAPES também estabeleceu que a implementação da gestão de riscos deve observar as seguintes diretrizes:

Quadro 3 - Diretrizes vinculados à Gestão de Riscos

DIRETRIZES VINCULADOS À GESTÃO DE RISCOS
Gestão de riscos integrada ao Planejamento Estratégico Institucional, aos processos e às políticas da organização;
Identificação, avaliação, tratamento e monitoramento periódico dos riscos;
Mensuração do desempenho da gestão de riscos;
Integração das instâncias responsáveis pela gestão de riscos;
Utilização de metodologia e ferramentas para o apoio à gestão de riscos; e
Desenvolvimento contínuo dos agentes públicos responsáveis pela gestão de riscos.

Fonte: art. 3º da Portaria CAPES nº 301/2022.

Quanto aos objetivos a serem observados na implementação da Política de Gestão de Riscos, deverão ser considerados os dispostos na Instrução Normativa Conjunta CGU/MP nº 1, de 2016, os quais estão divididos em objetivos vinculados à Gestão de Riscos e objetivos vinculados aos Controles internos, conforme a seguir:

Quadro 4 - Objetivos vinculados à Gestão de Riscos

OBJETIVOS VINCULADOS À GESTÃO DE RISCOS
Assegurar que os responsáveis pela tomada de decisão, em todos os níveis, tenham acesso tempestivo a informações suficientes quanto aos riscos aos quais está exposta a organização, inclusive para determinar questões relativas à delegação, se for o caso;
Aumentar a probabilidade de alcance dos objetivos da organização, reduzindo os riscos a níveis aceitáveis;e
Agregar valor à organização por meio da melhoria dos processos de tomada de decisão e do tratamento adequado dos riscos e dos impactos negativos decorrentes de sua materialização.

Fonte: art. 4º, inciso I, da Portaria CAPES nº 301/2022.

Quadro 5 - Objetivos vinculados aos Controles Internos

OBJETIVOS VINCULADOS AOS CONTROLES INTERNOS
Dar suporte à missão, à continuidade e à sustentabilidade institucional, pela garantia razoável de atingimento dos objetivos estratégicos da CAPES;
Proporcionar a eficiência, a eficácia e a efetividade operacional, mediante execução ordenada, ética e econômica das operações;
Assegurar que as informações produzidas sejam íntegras e confiáveis à tomada de decisões, ao cumprimento de obrigações de transparência e à prestação de contas;
Assegurar a conformidade com as leis e regulamentos aplicáveis, incluindo normas, políticas, programas, planos e procedimentos de governo e da própria organização; e
Salvaguardar e proteger bens, ativos e recursos públicos contra desperdício, perda, mau uso, dano, utilização não autorizada ou apropriação indevida.

Fonte: art. 4º, inciso II, da Portaria CAPES nº 301/2022.

2.2. Estrutura de Gestão de Riscos da CAPES

A governança orienta a direção da organização, suas relações externas e internas, bem como as regras, processos e práticas necessárias para alcançar seus propósitos. As estruturas de gestão traduzem essa direção em estratégias e objetivos necessários para atingir níveis desejados de desempenho sustentável e viabilidade a longo prazo. Nesse contexto, determinar a responsabilização pela gestão de riscos e os papéis de supervisão dentro da organização é parte integrante da governança (ABNT, 2018).

A estrutura de gestão de riscos tem como objetivo apoiar a organização na incorporação da gestão de riscos em suas atividades essenciais. Sua eficácia está diretamente relacionada à sua integração com a governança e as atividades da organização. Dessa forma, a gestão de riscos desempenha um papel fundamental na governança institucional, pois visa assegurar o cumprimento do plano estratégico e dos planos operacionais da instituição, além de integrar o processo decisório e as definições das estratégias.

2.2.1. Desenvolvimento da estrutura de gestão de riscos

O desenvolvimento da estrutura de gestão de riscos contempla os componentes de liderança e comprometimento, concepção, integração, implementação, avaliação e melhoria da

gestão de riscos, conforme estabelece a ISO 31.000:2018. Nesse sentido, a estrutura da CAPES pode ser compreendida da seguinte forma:

- **Liderança e comprometimento**: a alta administração, representada pela presidência da CAPES, foi designada como a principal responsável pelo estabelecimento da estratégia da organização e pela estrutura de gestão de riscos da CAPES. Isso inclui o estabelecimento, manutenção, monitoramento e aprimoramento dos controles internos da gestão. Além disso, o Comitê Interno de Governança da CAPES (CIG) desempenha um papel crucial nesse processo, sendo responsável pela aprovação da política e da metodologia de gestão de riscos e controles internos da CAPES.
- **Concepção da estrutura**: A estrutura, definida pela Política de Gestão de Riscos e Controles Internos da CAPES, foi elaborada levando em conta os fatores de contexto internos e externos. Essa estrutura se concretiza por meio do estabelecimento de responsabilidades e da atribuição de papéis.
- **Implementação, avaliação e melhoria**: a implementação, realizada por meio da aplicação da metodologia de gestão de riscos, fundamenta-se no estabelecimento de um plano de gestão de riscos institucional. Esse plano pode ser revisado e aprimorado continuamente.

Segundo o art. 6º da Portaria CAPES nº 301/2022, comporão a estrutura de Gestão de Riscos e Controles Internos da entidade:

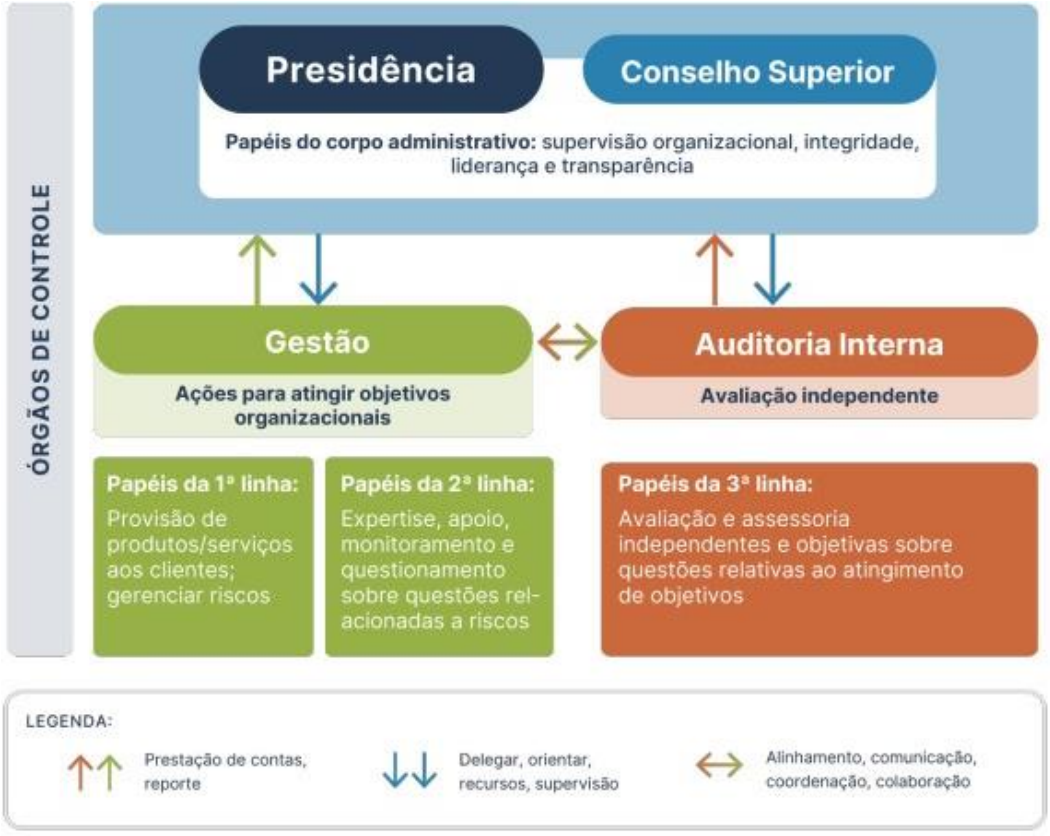
> I - Alta Administração;
> II - Comitê Interno de Governança;
> III - Comitê Gerencial de Governança;
> IV - Coordenação-Geral de Governança e Planejamento;
> V - Unidade de Gestão da Integridade;
> VI - Gestores de riscos; e
> VII - Auditoria Interna.

2.3. Competências e responsabilidades

As competências e responsabilidades no gerenciamento de riscos foram estabelecidas com base no Modelo das Três Linhas, proposto pelo *Institute of Internal Auditors* (IIA). Essa abordagem visa auxiliar as organizações a identificarem estruturas e processos mais adequados para o atingimento dos objetivos institucionais, possibilitando uma maior compreensão dos papéis e responsabilidades de cada grupo. Assim, cada um pode desempenhar suas funções específicas na gestão de riscos de forma coordenada.

A figura 1 apresenta uma adaptação do Modelo das Três Linhas do IIA ao contexto da CAPES, na qual o órgão de governança do modelo original foi substituído pela Presidência e pelo Conselho Superior.

Figura 1 - Estrutura de competências e responsabilidades baseada no Modelo de Três Linhas do IIA



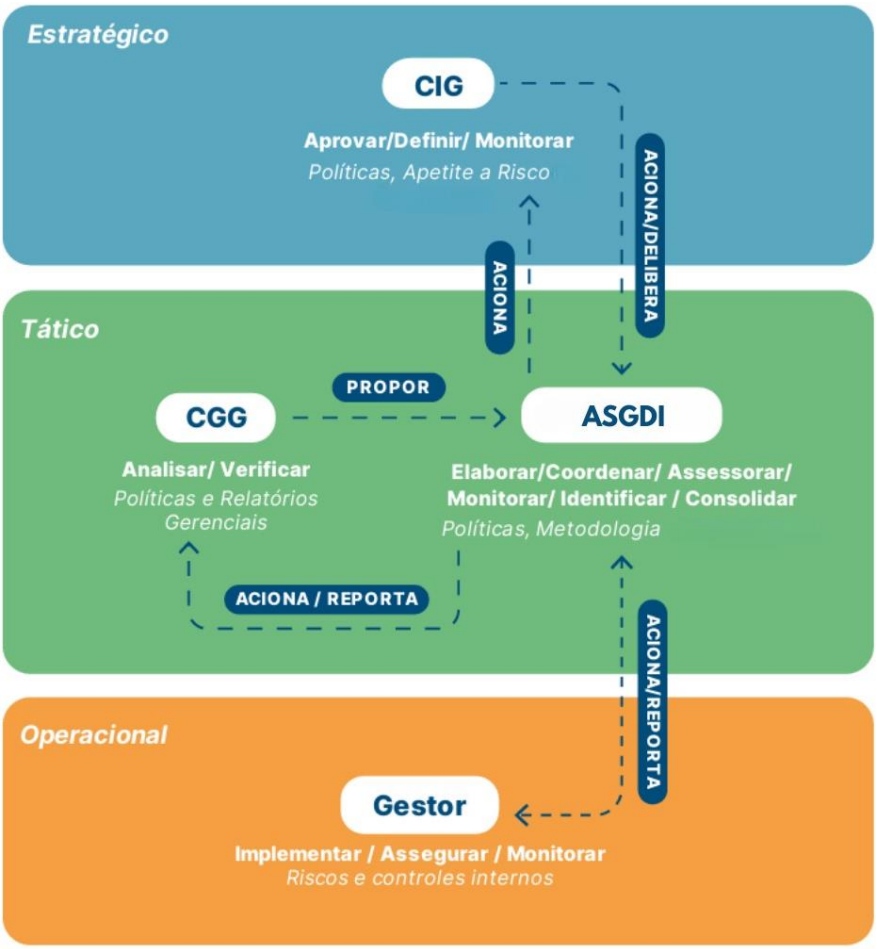
Fonte: Elaboração Própria

2.3.1. Fluxo de comunicação e operacionalização

A Política de Gestão de Riscos e Controles Internos da CAPES detalha as competências e responsabilidades envolvidas no processo de gestão de riscos, estruturando a coordenação e os papéis dos agentes e instâncias com base no modelo mencionado. O objetivo é prevenir falhas, eliminar duplicidades e aprimorar a comunicação, por meio do esclarecimento das atribuições relacionadas ao gerenciamento de riscos.

Considerando esse contexto, o fluxo de comunicação e a operacionalização da gestão de riscos da CAPES podem ser assim representados:

Figura 2 - Fluxo de Comunicação e Operacionalização entre as instâncias da CAPES



Fonte: Elaboração Própria

O nível operacional, representado pelo gestor de riscos, poderá acionar o nível tático, representado pela Assessoria de Governança e Desenvolvimento Institucional (ASGDI). Isso pode ocorrer tanto para obter orientações sobre o monitoramento dos riscos relacionados à sua unidade quanto para reportar novos riscos associados ao processo. O nível operacional também é responsável por responder ao nível tático sobre o monitoramento das ações definidas no plano de ação e das ações de gestão de riscos de forma abrangente.

A ASGDI, no nível tático, pode acionar o nível operacional durante o monitoramento das ações de riscos, além de ser responsável pelo reporte ao Comitê Gerencial de Governança (CGG) sobre o progresso das ações definidas no plano de ação.

No nível estratégico, o Comitê Interno de Governança (CIG) pode ser acionado pelo nível tático para definir, aprovar e monitorar as ações da política de gestão de riscos e controles internos.

2.3.2. Resumo das competências e responsabilidades

As competências e responsabilidades estabelecidas na política de gestão de riscos, que se referem à metodologia e à própria gestão dos riscos, podem ser assim resumidas:

ELABORAÇÃO E APROVAÇÃO DA METODOLOGIA:
ASGDI: Elabora e propõe a metodologia;
CGG: Analisa e opina sobre propostas e relatórios gerenciais sobre a metodologia.
CIG: Aprova a metodologia.

IMPLEMENTAÇÃO DA METODOLOGIA:
ASGDI: Coordena a implementação;
CIG: Definem os termos para a implementação.
CGG: Propõem os termos para a implementação.

GESTÃO DE RISCOS:
ASGDI: Monitora a gestão de riscos (adequação, efetividade e eficácia).

APETITE A RISCOS:
CIG: Define o apetite a riscos.

GESTÃO DE RISCOS DE PROCESSOS OU PROJETOS ORGANIZACIONAIS:

Para processos ou projetos sob sua responsabilidade
Gestor de Riscos: Identifica, analisa e avalia os riscos; propõe respostas e medidas de controle; assegura que o risco seja gerenciado; monitora a evolução dos níveis de risco e a efetividade das medidas e controles implementados; informa a ASGDI sobre mudanças significativas no curso do monitoramento dos riscos; responde às requisições da ASGDI ou instância superior para elaboração de relatórios gerenciais.

Para processo ou projetos em que estiverem envolvidos
Todos os colaboradores: monitoram a evolução dos níveis de risco e a efetividade das medidas de controles implementadas, reportando imediatamente ao gestor de riscos mudanças ou fragilidades identificadas nos processos ou projetos organizacionais.

2.3.3. Integração ao Planejamento Estratégico

No âmbito da CAPES, a Política de Gestão de Riscos e Controles Internos estabelece como diretriz a integração entre a gestão de riscos e o Planejamento Estratégico Institucional. Essa integração implica que os processos e ações devem estar diretamente alinhados aos objetivos estratégicos da instituição, além de serem integrados aos níveis tático e operacional, à gestão e à cultura organizacional, bem como às funções e atividades relevantes da entidade.

Nesse contexto, a gestão de riscos será implementada na atual cadeia de valor desenvolvida pela instituição, conforme os macroprocessos estabelecidos. Sua incorporação ocorrerá de forma gradual em todas as diretorias da CAPES, considerando a priorização da demanda em outros objetos da gestão de riscos.

3. Metodologia de Gestão de Riscos da CAPES

Com o objetivo de estabelecer as etapas para a operacionalização dos riscos, a metodologia é implementada por meio de um processo estruturado de gestão de riscos. Esse processo requer a aplicação sistemática de políticas, procedimentos e práticas, envolvendo um conjunto de atividades coordenadas destinadas a lidar com eventos que podem afetar os objetivos organizacionais. As etapas clássicas desse processo incluem identificar, analisar, avaliar, priorizar e responder aos riscos, mediante a implementação de controles ou outras respostas, além de monitorar e comunicar o desempenho da gestão de riscos. (ABNT, 2018; BRASIL, 2018).

A Metodologia de Gestão de Riscos da CAPES constitui a operacionalização de procedimentos para a implementação da gestão de riscos na instituição. Contudo, é fundamental observar as legislações pertinentes que abordam temas específicos, como aquelas relacionadas a licitações, prestação de contas de convênios e contratos.

Quanto aos objetos possíveis de aplicação da presente metodologia, estes podem ser variados, incluindo programas, projetos, processos, editais, entre outros.

Durante sua aplicação, é essencial registrar, organizar, documentar e referenciar os dados e informações utilizados, de modo a evidenciar o embasamento dos resultados, subsidiar a aprovação pelas instâncias competentes e construir um histórico dos fatos que serão importantes para futuras ações dos gestores.

3.1. Etapas

As etapas que envolvem a operacionalização da gestão de riscos na CAPES foram estabelecidas com base nas etapas mínimas previstas no art. 5º da Portaria CAPES nº 301/2022, que versa sobre a Política de Gestão de Riscos da CAPES e estabelece que:

> Art. 5º A operacionalização da gestão de riscos deverá ser descrita na Metodologia de Gestão de Riscos da CAPES, que deverá contemplar, no mínimo, as seguintes etapas:
>
> I - Escopo, contexto e critério;
>
> II - Identificação de risco;
>
> III - análise de riscos;
>
> IV - Avaliação de riscos;
>
> V - Tratamento de riscos;
>
> VI - Registro e relato;
>
> VII - comunicação e consulta;
>
> VIII - monitoramento e análise crítica.

Assim, considerando o contexto da entidade e visando proporcionar uma maior compreensão da metodologia por parte dos usuários, foram estabelecidas as seguintes etapas para a operacionalização da gestão de riscos, conforme ilustrado na figura 3 a seguir:

Figura 3 - Operacionalização da Gestão de Riscos

Fonte: Elaboração Própria

Conforme apresentado na figura, o processo de gestão de riscos é estruturado a partir de um Plano de Gestão de Riscos, que consiste em seis etapas. Após a conclusão dessas etapas, o plano de ação é implementado. É importante destacar que a comunicação e o monitoramento devem ocorrer durante todo o processo.

Além disso, após a consultoria com a CGU, houve uma alteração na etapa 3, o que resultou em uma diferenciação em relação à política de gestão de riscos. No entanto, a política de gestão de riscos será atualizada.

Nos tópicos a seguir, cada elemento do processo de gestão de riscos será detalhado individualmente.

3.1.1. Plano de Gestão de Riscos

Plano de Gestão de Riscos

Documento de planejamento em que são definidos os objetos prioritários a serem gerenciados, os respectivos responsáveis e o cronograma de gerenciamento.

O Plano de Gestão de Riscos é um documento de planejamento institucional que tem como objetivo estabelecer os objetos prioritários a serem gerenciados na CAPES. A elaboração desse plano é essencial para a realização de um trabalho sistematizado, uma vez que o processo de gestão de riscos pode ser aplicado em diferentes níveis e objetos.

No âmbito da CAPES, a Assessoria de Governança e Desenvolvimento Institucional (ASGDI), responsável por coordenar a implementação da metodologia de gestão de riscos, definiu, em consonância com o Plano Estratégico Institucional da CAPES 2024-2027 (PEI) os processos da cadeia de valor do próprio PEI como objetos prioritários a serem gerenciados. Essa priorização deve ser feita já que os processos organizacionais mencionados são os principais instrumentos que impactam no alcance dos objetivos estratégicos. No entanto, as áreas podem utilizar a metodologia para identificar os riscos de quaisquer objetos de seu interesse.

Os objetivos a serem alcançados e as estratégias para atingi-los estão definidos no PEI, Ele abrange a missão, a visão, os valores e os objetivos estratégicos para um ciclo de quatro anos, representados no mapa estratégico. Os objetivos estratégicos estão associados a indicadores, metas e a um portfólio de projetos. Além disso, para alcançar esses objetivos, as áreas podem desenvolver programas, projetos, processos de trabalho, editais, entre outros, que são objetos da gestão de riscos.

Figura 4 - Perspectiva da Gestão de Riscos na CAPES

Fonte: Elaboração Própria

3.1.2. Entendimento do Contexto

O entendimento do contexto tem como objetivo identificar e compreender os fatores dos ambientes interno e externo à organização, nos quais o objeto de gestão de riscos está inserido. Esses fatores podem influenciar o alcance dos resultados esperados pela entidade.

Nessa etapa, podem ser levantadas diversas informações relacionadas ao objeto. No Quadro 6, há exemplos dessas informações:

Quadro 6 - Entendimento do Contexto

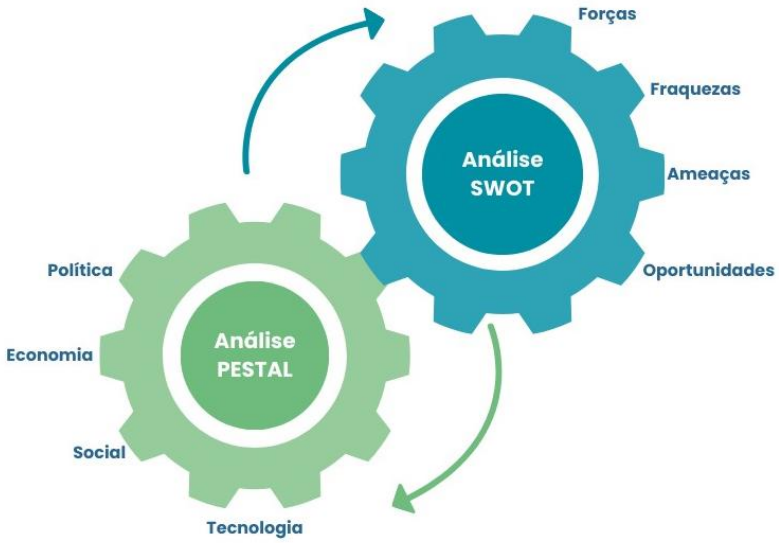
Possui fluxo estabelecido?
Possui previsão orçamentária?
Quais são os objetivos do objeto?
Quais os normativos pertinentes ao objeto? (internos e externos)
Quais as infraestruturas utilizadas pelo objeto?
As infraestruturas são suficientes e estão adequados para a operacionalização do objeto?
Quais os recursos humanos utilizados para atender o objeto? (quantitativo)
Os recursos humanos são suficientes e estão adequados para a operacionalização do objeto?
Quais os principais problemas do passado relacionados ao objeto? (Problemas passados, ajustados/melhorados no presente). *Os problemas atuais estão descritos na análise SWOT*

Fonte: Elaboração Própria

Além do levantamento dessas informações, uma das principais ferramentas que pode auxiliar no entendimento do contexto é a Análise SWOT. Essa ferramenta proporciona o levantamento dos fatores internos e externos à instituição que influenciam o cumprimento de seus objetivos, indicando, assim, possíveis riscos.

Outras ferramentas podem ser utilizadas para melhor compreensão do contexto em que o objeto está inserido, como a matriz RACI, a matriz de responsabilidades e a Análise PESTAL. A figura 5 representa uma utilização da Análise SWOT em conjunto com a Análise PESTAL.

Figura 5 - Ferramentas para o entendimento do contexto da Gestão de Riscos na CAPES



Fonte: Elaboração Própria

3.1.3. Identificação dos Riscos

ETAPA 2 – Identificação dos Riscos

Etapa em que os riscos são identificados, são levantadas as possíveis causas e consequências, e são classificadas em categorias.

O propósito da identificação de riscos é encontrar, reconhecer e descrever riscos que possam ajudar ou impedir que uma organização alcance seus objetivos. Informações pertinentes, apropriadas e atualizadas são importantes na identificação de riscos. (ABNT, 2018).

Importante!

Uma boa gestão de riscos exige um esforço holístico, interdisciplinar e de permanente verificação do ambiente ao qual a organização está inserida, proporcionando uma identificação abrangente e que permita detectar e transformar condições de risco.

A identificação deve incluir todos os riscos, estando suas fontes sob o controle da organização ou não, mesmo que as fontes ou causas dos riscos possam não ser evidentes.

Para identificar os riscos, é necessário considerar o entendimento do contexto, realizado na etapa anterior. Com base nesse entendimento, no conhecimento da equipe sobre o objeto em

análise e na opinião de especialistas, podem ser aplicadas diversas técnicas para identificar os possíveis riscos relacionados ao objeto.

A identificação dos riscos consiste em reconhecer e descrever de forma estruturada, os riscos, suas causas e consequências, bem como a tipologia a que pertencem. Por fim, deve-se realizar a vinculação do risco aos objetivos do objeto analisado, assegurando a coerência com o contexto organizacional e o alinhamento com o planejamento estratégico. Cada um desses itens pode ser resumido conforme abaixo:

CAUSAS:
São as condições que possibilitam a ocorrência de um evento de risco. Podem ter origem tanto no ambiente interno quanto externo. Uma causa é composta por: **fonte + vulnerabilidade.**

RISCO:
Trata-se da possibilidade de ocorrência de um evento que possa comprometer negativamente o alcance dos objetivos relacionados ao objeto em análise.

CONSEQUÊNCIAS:
São os efeitos resultantes de um evento de risco que impactam diretamente ou indiretamente os objetivos do objeto em análise.

Uma sintaxe muito utilizada para designar os riscos e que pode auxiliar na sua identificação é:

Devido a [causa] +	Poderá ocorrer [risco]	+ que poderá levar a [consequência]

Exemplo: Devido à falta de manutenção no sistema de informática poderá ocorrer uma falha no sistema de pagamento, o que poderá ocasionar atraso no pagamento das bolsas.

A referida sintaxe está representada graficamente abaixo:

Para facilitar a identificação das causas, é fundamental mapear as possíveis fontes de risco e suas respectivas vulnerabilidades. Esse levantamento contribui para uma análise mais precisa dos fatores que podem originar os riscos, conforme ilustrado nos exemplos a seguir:

Quadro 7 - Fontes e Vulnerabilidades

Fontes de Risco	Vulnerabilidades
Pessoas	Quantidade inadequada; escassez de pessoal; ausência de treinamento; falta de preparo; perfil inapropriado, com más intenções.
Processo	Mal elaborados (por exemplo: fluxo, desenho); sem manuais ou instruções formalizadas (procedimentos, documentos padronizados); Falta de divisão clara de responsabilidades.
Sistemas	Sistemas desatualizados; ausência de manuais de operação; não se integram com outros sistemas e não contam com controles de acesso lógico ou backups.
Infraestrutura Física	Localização inadequada; instalações ou disposição imprópria e a falta de controles de acesso físico.
Estrutura Organizacional	Falta de transparência em relação às funções e responsabilidades; falha nos fluxos de informação e comunicação; excesso de centralização de responsabilidades; delegações exageradas.
Tecnologia	Métodos ultrapassados/produtos obsoletos; ausência de investimento em TI; falta de proteção de patentes para a tecnologia; processo produtivo sem salvaguardas contra a espionagem.
Eventos Externos	Alteração súbita contra o clima; eventos incontroláveis.

Após a identificação dos riscos, com suas respectivas causas e consequências, é possível classificá-los em categorias específicas, o que contribui para uma compreensão mais clara e uma organização mais eficiente dos riscos identificados. A seguir, apresenta-se o quadro com a tipologia de riscos, que auxilia na categorização e no direcionamento das estratégias de tratamento adequadas.

Quadro 8 - Tipologia de Riscos

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, assim como de catástrofes naturais ou de ações de terceiros;
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;
Riscos legais/ de conformidade	Eventos derivados de alterações legislativas ou normativas que podem comprometer as atividades do órgão ou entidade, bem como a eventos relacionados à corrupção, fraudes, irregularidades ou desvios éticos e de conduta que podem comprometer os valores, as ações e o alcance dos objetivos da CAPES;
Riscos financeiros/ orçamentários	Riscos que podem comprometer a capacidade da CAPES de executar suas ações, eventos ou atividades, como, por exemplo, restrições orçamentárias que impossibilitem o fomento e a qualificação da formação de pessoal de nível superior.
Risco à integridade	Vulnerabilidade que pode favorecer ou facilitar a ocorrência de práticas de corrupção, fraudes, irregularidades ou desvios éticos e de conduta, os quais podem comprometer os objetivos da instituição.
Risco de Negócios	Riscos relativos às atividades e aos negócios da CAPES, como acordos, termos de cooperação, contratos, parcerias, relação entre sistemas de diversos órgãos da Administração.
Riscos Políticos	Riscos decorrentes das mudanças de políticas públicas, de governo e gestão, da ausência de critérios para priorização de demandas educacionais pelo governo e de debates políticos sobre as atividades e funcionamentos da CAPES.

Eventualmente, um risco pode ser classificado em mais de uma tipologia simultaneamente.

3.1.4. Identificação e Avaliação dos Controles

Os controles são procedimentos que buscam modificar o nível de um risco. Os controles incluem, mas não estão limitados, a qualquer processo, política, dispositivo, prática ou outras condições e/ou ações que mantêm e/ou modificam o risco (ABNT, 2018).

A etapa de identificação e avaliação dos controles tem como objetivo identificar os controles implementados para mitigar os riscos identificados na etapa anterior e realizar a avaliação da sua efetividade.

O primeiro passo dessa etapa consiste na **identificação dos controles** atualmente em vigor para cada risco. Na sequência, os controles devem ser **classificados em três categorias:** preventivos, corretivos e detectivos.

Essa classificação depende da atuação dos controles em relação aos elementos do risco: nas causas (controles preventivos), nas consequências (controles corretivos), ou ao próprio risco (controles detectivos), conforme apresentado no quadro a seguir:

Quadro 9 - Tipos de Controle

Controles Preventivos	Controles Corretivos	Controles Detectivos
Atuam nas causas do risco, com o objetivo de diminuir a probabilidade de ocorrência, ou seja, prevenir. *Exemplos: Redesenho de tarefas ou processos*	**Atuam nas consequências do risco, caso o risco se materialize. Objetivam diminuir o impacto.** *Exemplos: Desenvolvimento de planos de contingência*	**Atuam na detecção da materialização de um evento de risco. Não podem mitigar um risco.** *Exemplos: Monitoramento*

É importante destacar que um único risco pode estar associado a diferentes tipos de controle, permitindo a existência simultânea de controles preventivos, detectivos e corretivos para um mesmo evento.

Para avaliar a efetividade dos controles de cada risco, deve-se utilizar a escala apresentada no quadro a seguir:

Quadro 10 - Escala de Efetividade dos Controles

Nível	Descrição	Avaliação
Fraco	Controles que são desorganizados e aplicados caso a caso, dependendo do conhecimento das pessoas. Reduzem pouco o risco.	**1**
Mediano	Controles que não cobrem todos os aspectos relevantes. Há falhas no desenho ou nas ferramentas. Reduzem apenas parte do risco.	**2**
Satisfatório	Controles implementados de forma sistemática, com bom desenho e ferramentas adequadas, mas ainda podem melhorar. Reduzem o risco de forma adequada.	**3**
Forte	Controles consolidados, com fluxo bem estabelecidos, que tratam dos aspectos relevantes do risco. Mitigam o máximo possível do risco.	**4**

Fonte: Elaboração própria.

Com os controles avaliados, a critério da unidade, o fator de avaliação apresentado na escala pode ser utilizado por meio da média aritmética dos controles para definir a avaliação do bloco. Alternativamente, os gestores podem optar por realizar uma análise qualitativa dos controles existentes, sem a necessidade de calcular a média aritmética para determinar a efetividade desses controles.

3.1.5. Cálculo dos níveis de risco

ETAPA 4 – Cálculo dos Níveis de Risco

Etapa em que é realizado o cálculo dos níveis de risco residual e inerente.

Os níveis de risco são calculados para subsidiar as decisões de resposta aos riscos.

Nesta etapa, deverão ser calculados o Nível de Risco Residual e o Nível de Risco Inerente, cujos cálculos envolvem a avaliação da probabilidade e do impacto. Esses níveis se diferenciam basicamente por considerar ou não a implementação dos controles mitigadores, conforme a definição apresentada no quadro a seguir:

Quadro 11 - Níveis de Risco

Risco Residual	Risco Inerente
O nível de risco que permanece após a implementação dos controles mitigadores.	O nível de risco presente em um processo ou atividade antes de serem aplicados quaisquer controles.

Para estimar a probabilidade de ocorrência de um risco, tanto para fins de cálculo de nível de risco residual quanto do nível de risco inerente, utiliza-se a escala de probabilidade apresentada no Quadro 12 a seguir:

Quadro 12 - Escala de Probabilidade

Níveis	Probabilidade	Descrição
1	Muito baixa	Improvável. O evento poderá ocorrer apenas em situações excepcionais. Há registros de ocorrência, porém são raros os casos práticos observados.
2	Baixa	Pouco provável. O evento poderá ocorrer de forma eventual ou inesperada, com baixa frequência.
3	Média	Possível. O evento pode ocorrer em algum momento, com base em um histórico moderado de ocorrências.
4	Alta	Provável. O evento tende a ocorrer na maioria das circunstâncias, de acordo com padrões observados em situações anteriores.
5	Muito alta	Praticamente certa. O evento é recorrente, com registros consistentes de ocorrência em situações semelhantes, o que demonstra claramente sua alta frequência.

Fonte: Elaboração própria.

Para estimar o impacto de um risco caso ele ocorra, tanto para o cálculo do nível de risco residual quanto do risco inerente, utiliza-se a escala de impacto apresentada no Quadro 13 a seguir:

Quadro 13 - Escala de Impacto

Níveis	Impacto	Descrição
1	Muito baixo	Impacto mínimo. Não altera o alcance dos objetivos do objeto ou a alteração é insignificante.
2	Baixo	Impacto pequeno. Compromete muito pouco o alcance dos objetivos do objeto, sendo de fácil reparação/recuperação.
3	Médio	Impacto moderado. Compromete razoavelmente o alcance dos objetivos do objeto, porém é possível a reparação/recuperação.
4	Alto	Impacto significativo. Compromete a maior parte do alcance dos objetivos do objeto, sendo de difícil reparação/recuperação.
5	Muito alto	Impacto catastrófico. Compromete totalmente ou quase totalmente o alcance dos objetivos do objeto, sem a possibilidade de reparação/recuperação.

Fonte: Elaboração própria.

3.1.5.1. Cálculo do Nível de Risco Residual

O nível de risco residual será obtido pela multiplicação da probabilidade residual pelo impacto residual do risco. Nesse contexto, a função de risco é definida como:

Figura 6 - Função do Risco Residual

Fonte: Elaboração própria.

Para estimar a probabilidade residual, é necessário utilizar a escala de probabilidade (Quadro 11) e considerar, na análise, a sua mitigação com base no conjunto de controles preventivos elencados na etapa anterior.

Da mesma forma, para estimar o impacto residual, é necessário utilizar a escala de impacto (Quadro 12), considerando a mitigação do impacto com base no conjunto de controles corretivos (também elencados na etapa anterior).

Dica
Uma dica importante nesta etapa é realizar a comparação tanto entre as probabilidades residuais dos diferentes eventos identificados quanto entre os impactos residuais. Essa comparação permite dimensionar a diferença relativa entre os eventos de risco, contribuindo para a definição de prioridades no tratamento dos riscos mais relevantes.

3.1.5.2.Cálculo do Nível de Risco Inerente

O nível de risco inerente é obtido pela multiplicação da probabilidade inerente pelo impacto inerente do risco. Nesse contexto, a função de risco é definida como:

Figura 7 - Função do Risco Inerente

Fonte: Elaboração Própria

Para estimar a probabilidade inerente e o impacto inerente, é necessário utilizar as mesmas escalas de probabilidade (Quadro 12) e de impacto (Quadro 13) já apresentadas. No entanto, tanto para probabilidade quanto para o impacto, deve-se desconsiderar a existência de controles implementados relacionados ao risco.

A mesma orientação descrita anteriormente, de comparar a probabilidade e o impacto de um risco em relação a outro, aplica-se também à probabilidade inerente e ao impacto inerente.

3.1.5.3. Classificação dos Níveis de Risco

A matriz de riscos, também conhecida como mapa de calor, é uma ferramenta que classifica qualitativamente os níveis de probabilidade e impacto dos riscos. Esta matriz está dividida em quatro áreas, que representam os níveis de risco: baixo, médio, alto e crítico. conforme ilustrado a seguir:

Quadro 14 - Matriz de Riscos/Matriz de Calor

MATRIZ DE RISCOS/MATRIZ DE CALOR						
IMPACTO	Muito Alto 5	5	10	15	20	25
	Alto 4	4	8	12	16	20
	Médio 3	3	6	9	12	15
	Baixo 2	2	4	6	8	10
	Muito Baixo 1	1	2	3	4	5
		Muito Baixa 1	Baixa 2	Média 3	Alta 4	Muito Alta 5
	PROBABILIDADE					

Fonte: elaboração própria.

A classificação das faixas pode ser visualizada no quadro abaixo:

Quadro 15 - Classificação do Nível de Risco

Classificação	Faixa
Risco Baixo	1 a 3,99
Risco Médio	4 a 6,99
Risco Alto	7 a 12,99
Risco Crítico	13 a 25

Fonte: Elaboração própria.

Nos riscos gerenciados pela Diretoria de Tecnologia da Informação (DTI), pode-se considerar o impacto como a dimensão mais relevante da Matriz.

3.1.5.4. Apetite a Riscos

O apetite ao risco é definido pela Portaria CAPES nº 301/2022 como o "nível de risco que a instituição está disposta a aceitar", devendo esse apetite ser estabelecido pelo Comitê Interno de Governança, conforme o art. 8º, inciso II da mesma portaria.

Considerando o nível de risco institucional, os riscos que excederem essa faixa deverão ser tratados e monitorados, sendo permitidas justificativas caso não sejam abordados ou priorizados.

Dessa forma, o estabelecimento do apetite de riscos é fundamental para que a instituição declare até qual nível de exposição ao risco está disposta a aceitar e até o quanto está disposta a assumir em prol do alcance dos seus objetivos.

3.1.6. Resposta aos Riscos

Nesta etapa, serão definidas as respostas a serem dadas aos riscos, com base no nível de risco residual obtido. Existem quatro opções de respostas aos riscos: Mitigar, Compartilhar, Evitar e Aceitar, conforme detalhado no quadro a seguir:

Quadro 16 - Opções de respostas aos riscos

Opções de Respostas	Descrição
Mitigar	Mitigar o risco significa implementar controles com o objetivo de reduzir a probabilidade e/ou o impacto dos riscos, atuando nas suas causas e/ou consequências. Essa opção normalmente é selecionada quando o risco está classificado acima do apetite ao risco, buscando trazê-lo para dentro desse limite, mas pode ser selecionada para riscos dentro do apetite, desde que haja justificativa. É importante avaliar se o custo-benefício da implementação do controle é adequado.
Compartilhar	Compartilhar o risco é uma forma de mitigar o risco pode ser realizado por meio de terceirização ou contratação de seguros, visando reduzir tanto o impacto quanto a probabilidade do risco. Essa opção normalmente é selecionada quando o risco é classificado fora do apetite ao risco, buscando trazê-lo para dentro desse limite.
Evitar	Evitar o risco significa não iniciar ou descontinuar a atividade que gera o risco, especialmente quando o custo-benefício da implementação dos controles é elevado e não é possível compartilhar o risco.
Aceitar	Aceitar o risco significa que não são necessárias medidas adicionais para alterar os níveis de risco, pois estes já estão dentro do apetite a riscos. No entanto, devem ser monitorados.

Fonte: elaboração própria.

A faixa de classificação do nível de risco residual deve ser considerada na definição da resposta. O quadro a seguir apresenta as ações e as possíveis respostas para cada faixa de classificação:

Quadro 17 - Ações recomendadas para cada classificação do risco

Classificação do Nível de risco	Ações	Respostas
Risco baixo	Dentro do apetite a risco. Não é necessário implementar novo controle. Podem ser implementados novos controles, desde que justificados. Podem existir oportunidades de diminuir os controles. É necessário monitorar a efetividade dos controles existentes.	Aceitar Mitigar
Risco médio	Dentro do apetite a risco. Não é necessário implementar novo controle. Podem ser implementados novos controles, desde que justificados. É necessário monitorar a efetividade dos controles existentes.	Aceitar Mitigar
Risco alto	Acima do apetite a risco. É necessário adotar alguma medida de controle em um período determinado.	Mitigar Compartilhar
Risco crítico	Muito acima do apetite a risco. É necessário adotar uma medida de controle imediata.	Mitigar Evitar

Fonte: Elaboração Própria

3.1.7. Elaboração do Plano de Ação

A elaboração do plano de ação consiste em especificar, em um documento próprio, as ações para os riscos cujas respostas definidas na etapa anterior foram mitigar, compartilhar ou evitar.

Conforme a figura abaixo, o plano de ação deve conter os seguintes itens:

Quadro 18 - Itens do Plano de Ação

Risco								
Nivel de Risco Residual								
Resposta ao Risco								
Controles Existentes								
O que?	**Por que?**	**Como?**	**Onde?**	**Quem?**	**Quanto?**	**Quando?**	**Status**	**Gestor de Riscos**
Novo controle (Preventivo, corretivo, detectivo)	Justificativa para o novo controle (se necessário)	Descrição de como serão implementados os novos controles	Unidade (Diretoria, Coordenação)	Responsável pela implementação (cargo)	Quanto vai custar?	Previsão de início e fim da implementação	Status da implementação	Gestor responsável por tratar os riscos

Fonte: Elaboração própria.

Nesta etapa, deve-se buscar estabelecer ações de controle preventivo e corretivo, conforme a classificação apresentada na etapa de controle.

Os novos controles propostos devem considerar a relação custo-benefício e a viabilidade das ações. É essencial que haja um alinhamento entre os responsáveis pela implementação da ação quanto à exequibilidade e ao prazo de execução.

Os planos de ação devem ser discutidos com as partes interessadas, que precisam estar cientes dos riscos remanescentes. Além disso, o gestor responsável por gerenciar os riscos deve ser designado, considerando o cargo responsável pelo objeto de gestão de riscos na unidade.

Por fim, os planos de ação relacionados aos riscos críticos ou aos objetos de interesse do Comitê Interno de Governança (CIG) devem ser aprovados pelo próprio comitê.

3.1.8. Implementação do Plano de Ação

A responsabilidade principal pela implementação do plano de ação cabe ao cargo responsável pela unidade que gerencia o processo organizacional. Contudo, a execução do plano de ação demanda a colaboração de outras unidades envolvidas no processo ou cujas ações estejam dentro de sua competência.

A implementação deverá ocorrer conforme as previsões de início e fim estabelecidas no plano de ação, cabendo à ASGDI monitorar se os prazos estão sendo cumpridos. A unidade responsável poderá cancelar ações propostas, apresentando justificativas para tal decisão.

As ações previstas no plano de ação, quando concluídas, devem resultar em novos controles ou no aprimoramento de controles já estabelecidos. Esses controles, sejam novos ou aprimorados, serão utilizados como fontes para a atualização dos níveis de riscos residual a que se referem.

3.2. Comunicação

Comunicação

Atividade que ocorre ao longo de todo o processo de gestão de riscos e busca promover entre as partes interessadas, a conscientização, compartilhamento de informações e entendimento do risco.

A comunicação deve ser um processo contínuo e interativo de compartilhamento de informações entre todas as partes interessadas durante todo o processo de gerenciamento de riscos.

De acordo com a Instrução Normativa MPOG/CGU nº 01/2016, a organização deve comunicar as informações necessárias para alcançar seus objetivos a todas as partes interessadas, independentemente do nível hierárquico.

Internamente, o objetivo da CAPES é promover a disseminação de informações claras e precisas, fomentando a conscientização, o entendimento dos riscos e as decisões tomadas. Isso envolve um trabalho coordenado de troca de informações. Para tanto, será elaborado um Plano de Comunicação com duas direções: vertical e horizontal.

Quadro 19 - Plano de Comunicação

Comunicação Vertical	Comunicação Horizontal
A comunicação vertical pode ocorrer tanto no sentido da base para a alta administração quanto no sentido inverso, de forma a proporcionar o entendimento de todas as unidades organizacionais no que se refere às informações acerca dos riscos. Dessa maneira, os servidores e colaboradores terão ciência dos principais riscos que afetam a organização.	A comunicação horizontal é de suma importância para que os riscos associados a um determinado objeto sejam conhecidos pelas diferentes unidades envolvidas. Essa abordagem permite que informações relevantes sobre potenciais riscos sejam compartilhadas de maneira eficaz entre as diversas áreas da organização. Dessa forma, todos os setores podem estar cientes dos possíveis desafios e trabalhar de maneira coordenada para mitigá-los.

Fonte: Elaboração própria.

Externamente, o processo possibilita a recepção de informações relevantes e o atendimento aos requisitos e expectativas das partes interessadas, influenciando diretamente a imagem da instituição. Dessa forma, a instituição consegue comunicar-se de maneira eficaz com seu público externo, fortalecendo sua reputação e credibilidade.

3.3. Monitoramento

Monitoramento

Atividade que ocorre ao longo de todo o processo de gestão de riscos e visa um aprimoramento contínuo por meio de planejamento, análise de informações, registro dos resultados e fornecimento de retorno. Pode abranger a política, as atividades, os riscos, os planos de tratamento, os controles.

O objetivo do monitoramento é garantir e aprimorar a qualidade e a eficácia da gestão de riscos. Portanto, o monitoramento deve ser realizado de maneira planejada e periódica ao longo de todo o processo de gestão de riscos.

É essencial destacar que o monitoramento da gestão de riscos é uma parte integrante do processo de gestão e de tomada de decisão. Ele deve acompanhar o planejamento estratégico e seus desdobramentos, sem sobrecarregar excessivamente o processo.

Os objetivos e os itens de controle estão detalhados no quadro a seguir, que define a periodicidade e a responsabilidade pelo monitoramento:

Quadro 20 - Plano de Monitoramento

Objetivo do Monitoramento	Objeto do monitoramento	Quando deverá ocorrer	Quem é o responsável
Revisão	Política de Gestão de Riscos	a cada 2 anos, sendo a primeira após 1 ano do início da implementação da metodologia.	ASGDI
	Metodologia de Gestão de Riscos	a cada 2 anos, sendo a primeira após 1 ano do início da sua implementação.	ASGDI
Acompanhamento da Implementação	Plano de Gestão de Riscos	de forma contínua, ou no mínimo a cada 1 ano.	ASGDI
	Planos de Ação	de forma contínua ou no mínimo a cada 6 meses.	Gestor de Riscos, assessorado pela ASGDI
Atualização e efetividade	Os eventos de risco, causas, consequências, controles já implementados, níveis de risco e medidas de tratamento propostas no plano de ação.	de forma contínua, especialmente quando houver mudanças relevantes de contexto. Deve levar em consideração o tempo necessário para que as medidas produzam efeitos.	Gestor de Riscos, assessorado pela ASGDI
	Aprovação dos planos de ação fora do apetite a risco	de forma contínua	Comitê Interno de Governança (CIG)

Fonte: Elaboração própria.

O monitoramento inclui o planejamento, a coleta de dados, a análise de informações, o registro de resultados e o fornecimento de feedback por meio de atividades de comunicação.

O monitoramento desempenha um papel essencial na garantia da eficiência e eficácia dos controles internos de uma organização. Ao integrar essas práticas de forma sistemática e abrangente em todas as etapas do processo de gestão de riscos, a organização fortalece sua

capacidade de prevenir ações irregulares, antieconômicas e ineficazes, promovendo, assim, uma cultura de conformidade e transparência.

A responsabilidade pelo monitoramento do funcionamento do futuro Sistema de Gestão de Riscos é da Assessoria de Governança e Desenvolvimento Institucional (ASGDI), dos coordenadores setoriais e da alta administração da entidade. É importante ressaltar que a gestão de riscos realizada nas unidades deve ser acompanhada pelo respectivo gestor de riscos de cada uma delas.

4. Considerações Finais

A gestão de riscos representa um avanço significativo para o fortalecimento da governança e do desempenho organizacional da instituição. Além de apoiar de forma decisiva a tomada de decisão dos gestores, constitui uma ferramenta essencial para a prevenção de falhas e um importante instrumento de governança. Ao estabelecer um processo estruturado, a CAPES reafirma seu compromisso em adotar uma abordagem proativa, alinhada aos seus objetivos estratégicos, promovendo a sistematização e a padronização da gestão de riscos na instituição. Busca-se, ainda, fomentar uma cultura organizacional pautada em boas práticas, contribuindo para decisões gerenciais mais qualificadas.

A metodologia está em conformidade com a Instrução Normativa Conjunta CGU/MP nº 01, de 10 de maio de 2016, que dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo federal, e com o Decreto nº 9.203, de 22 de novembro de 2017, que trata da política de governança da administração pública federal direta, autárquica e fundacional.

Nesta segunda versão, a metodologia de Gestão de Riscos da CAPES foi aprimorada com o apoio da Assessoria de Governança e Desenvolvimento Institucional (ASGDI), da consultoria da Unidade de Auditoria Interna (AUD) e da assessoria da Controladoria-geral da União (CGU).

Esse aprimoramento foi possível por meio da aplicação prática da metodologia em um processo da cadeia de valor realizado pela ASGDI, o que contribuiu para uma maior compreensão da sua aplicabilidade, além de proporcionar clareza conceitual, segurança e expertise às equipes participantes.

A metodologia foi desenvolvida com base nos fundamentos do *framework* ISO 31000:2018 (ABNT, 2018) e em documentos metodológicos de órgãos de referência, como TCU e CGU. Contudo, com a experiência bem-sucedida da aplicação prática, foi possível realizar alterações em uma das etapas da metodologia anteriormente proposta, além de incorporar ao documento boas práticas utilizadas pela CGU.

Com o objetivo de promover a melhoria contínua, a metodologia será constantemente aperfeiçoada. Assim, os feedbacks das unidades após sua aplicação serão essenciais para seu desenvolvimento.

A implementação dessa metodologia permitirá à CAPES identificar, avaliar e gerenciar de forma eficaz os riscos que possam comprometer o cumprimento de sua missão e o alcance

de suas metas. O estabelecimento de controles internos adequados contribuirá para a mitigação desses riscos, promovendo uma gestão mais transparente, eficiente e responsável.

Ao concluir o desenvolvimento desta metodologia, a CAPES reforça seu empenho na busca pela excelência na prestação de serviços públicos e na melhoria contínua de seus processos. Espera-se que a adoção desta metodologia de Gestão de Riscos e Controles Internos consolide a Fundação como uma referência em governança e desempenho organizacional.

Referências

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

ABNT. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO 31000: Gestão de Riscos – Princípios e diretrizes**. Rio de Janeiro: ABNT, 2018.

BRASIL. Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – CAPES**. Plano Estratégico Institucional: Anexo 2.**

BRASIL. **Instrução Normativa Conjunta CGU/MP nº 1, de 10 de maio de 2016**. Dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo federal. Diário Oficial da União de 11/05/2016 – Seção 1 – p.14.

BRASIL. **Decreto nº 9.203, de 17 de novembro de 2017.** Dispõe sobre a política de governança da administração pública federal. Diário Oficial da União, Brasília, DF, 18 out. 2017. Seção 1, p. 2.

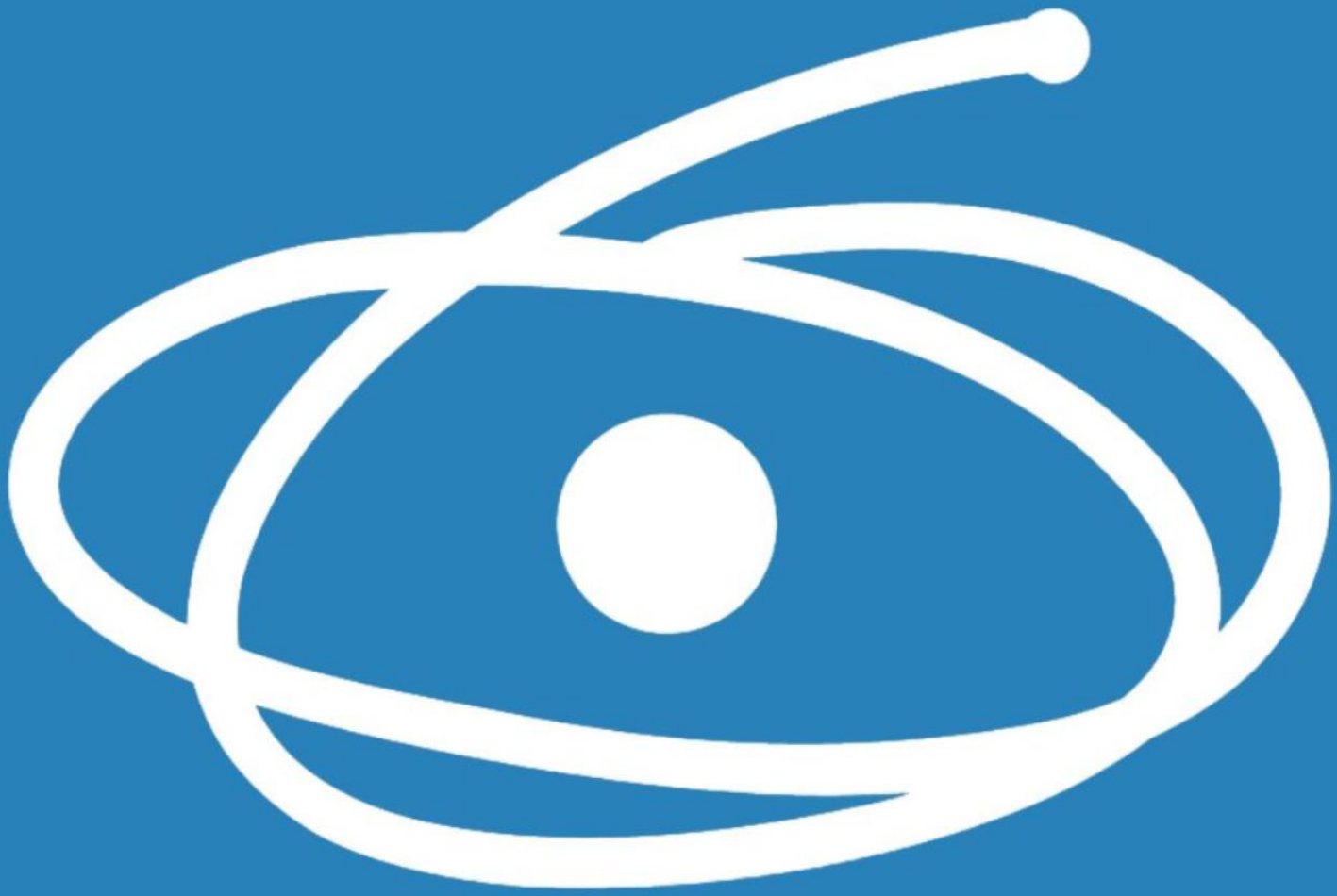
BRASIL. Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – CAPES. **Portaria GAB nº 37, de 20 de fevereiro de 2018**. Boletim de Serviço, Edição Especial nº 4, fevereiro de 2018, págs. 2-6.

BRASIL. Tribunal de Contas da União. **Roteiro de Avaliação de Maturidade da Gestão de Riscos / Tribunal de Contas da União**. – Brasília: TCU, Secretaria de Métodos e Suporte ao Controle Externo, 2018. 164 p.

BRASIL. Tribunal de Contas da União. **Manual de gestão de riscos do TCU**. Tribunal de Contas da União. Brasília: TCU, Secretaria de Planejamento, Governança e Gestão (Seplan), 2020.

BRASIL. Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - CAPES. **Portaria nº 126, de 30 de junho de 2022**. Institui a estrutura de governança da Fundação Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – CAPES. Diário Oficial da União de 05/07/2022, Seção 2, pág. 195.

BRASIL. Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – CAPES**. Portaria nº 301, de 22 de dezembro de 2022.** Dispõe sobre a Política de Gestão de Riscos e Controles Internos da Fundação Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - CAPES. Diário Oficial da União de 23/12/2022 - Seção 1 - p. 85-86.



CAPES