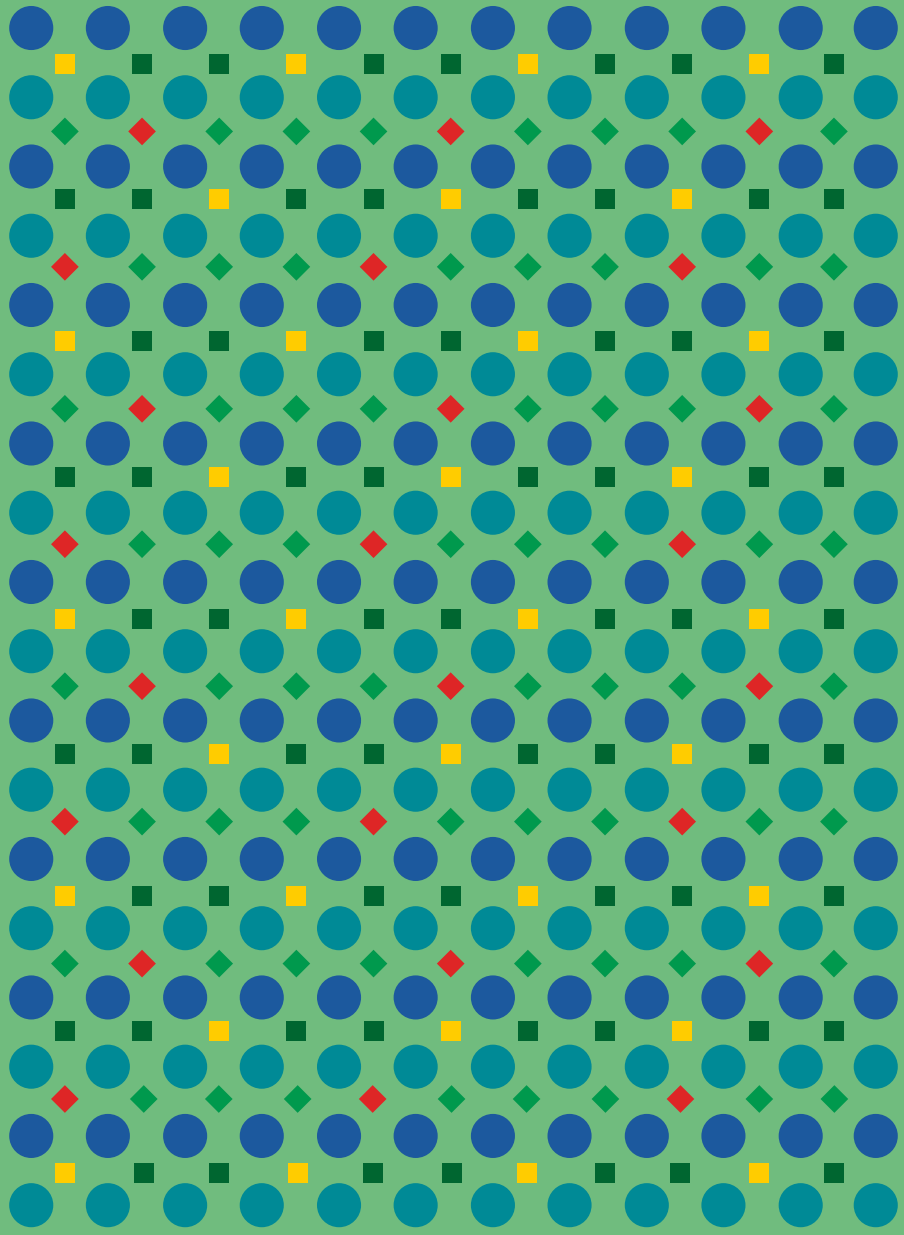
Metodologia de Gestão de Riscos da CAPES



CAPES

MINISTÉRIO DA EDUCAÇÃO

GOVERNO FEDERAL
BRASIL
UNIÃO E RECONSTRUÇÃO

Expediente

COMITÊ INTERNO DE GOVERNANÇA

Presidente
Denise Pires de Carvalho

Diretor de Programas e Bolsas no País (DPB)
Luiz Antonio Pessan

Diretor de Avaliação (DAV)
Antonio Gomes de Souza Filho

Diretor de Relações Internacionais (DRI)
Rui Vicente Oppermann

Diretor de Educação a Distância (DED)
Antonio Carlos Rodrigues de Amorim

Diretora de Formação de Professores da Educação Básica (DEB)
Marcia Serra Ferreira

Diretora de Gestão (DGES)
Luciana Mendonça Gottschall

Diretor de Tecnologia da Informação (DTI)
Gustavo Jardim Portella

CONSOLIDAÇÃO DO CONTEÚDO

Coordenador-Geral de Governança e Planejamento (CGGOV)
Yuri Ghobad da Silva

Coordenador de Assuntos Estratégicos Institucionais (CAES/CGGOV)
Elivelton Oliveira Santa Cruz

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

CONSULTORIA EM GESTÃO DE RISCOS

EQUIPE DA AUDITORIA INTERNA DA CAPES:

Germano de Oliveira Farias
Brunna Hisla da Silva Sena
Daniela Amorim Meira
Patrícia Reis Paiva

PROJETO GRÁFICO E DIAGRAMAÇÃO

Coordenação-Geral de Comunicação Social (CGCOM)
Julia Lozzi Teixeira

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

LISTA DE TABELAS

Apresentação

A Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES) tem, ao longo dos anos, buscado aprimorar suas práticas de governança institucional. A Gestão de Riscos tem sido um instrumento crucial para essa melhoria contínua.

A Gestão de Riscos contribui significativamente para a melhoria dos resultados da gestão e para o cumprimento dos objetivos institucionais, pois visa criar e proteger valor. Com a publicação da Portaria nº 301, em 22 de dezembro de 2022, que estabelece uma nova política de gestão de riscos e controles internos na CAPES, foram adotados novos esforços para garantir uma implementação eficaz.

Dessa forma, este manual foi elaborado com o objetivo de proporcionar uma compreensão mais aprofundada sobre a gestão de riscos, facilitar a disseminação do conhecimento sobre o processo de gestão de riscos na CAPES e apresentar a metodologia de gestão de riscos institucional. Seu propósito é capacitar os gestores de riscos, promovendo autonomia e eficiência no controle de processos, programas e ações.

1. Introdução

A gestão de riscos está diretamente ligada ao princípio constitucional da eficiência, sendo relevante quando resulta em melhorias na entrega de resultados e no cumprimento dos objetivos institucionais. Ela se torna uma valiosa aliada para o gestor, permitindo uma tomada de decisão mais racional e aumentando a capacidade da organização de enfrentar eventos inesperados que possam impactar negativamente seus objetivos. Dessa forma, favorece o uso eficiente, eficaz e efetivo dos recursos, promove a transparência e fortalece a imagem da instituição (TCU, 2020).

A gestão de riscos envolve a identificação, avaliação e priorização de potenciais riscos em macroprocessos, processos ou programas, seguida pela aplicação coordenada e econômica de recursos para minimizar, monitorar e controlar a probabilidade e o impacto de eventos negativos, ou maximizar as oportunidades. O objetivo é assegurar que as incertezas não desviem os esforços da organização de seus objetivos (TCU, 2017a).

No setor público, a gestão de riscos busca equipar a administração com instrumentos para enfrentar a incerteza e suas ramificações, abrangendo tanto riscos quanto oportunidades, sempre focada no interesse público. Essa abordagem fortalece a capacidade de gestão de agregar valor e fornecer serviços com maior eficiência, eficácia e economia, mantendo em mente princípios como equidade e justiça.

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 iniciou a institucionalização da gestão de riscos com a publicação da Portaria CAPES nº 37, de 20 de fevereiro de 2018. Esta portaria instituiu a Política de Gestão de Riscos da CAPES e levou à criação do Comitê de Governança, Riscos e Controles, mas não foi efetivamente implementada na época.

O aprimoramento contínuo dos normativos federais indicou a necessidade de uma política de gestão de riscos mais adequada ao contexto da CAPES. Assim, em 2022, foi publicada a Portaria nº 301, de 22 de dezembro de 2022, que estabelece uma nova política de gestão de riscos e controles internos na entidade. Esta portaria incorpora os controles internos de acordo com as orientações dos órgãos de controle e implementa uma metodologia de gestão de riscos institucional.

A nova política visa alinhar-se com a governança institucional e o planejamento estratégico da CAPES, atribuindo competências conforme definido na Portaria nº 126, de 30 de junho de 2022, que instituiu a estrutura de governança da CAPES. A gestão de riscos na CAPES busca garantir que as incertezas não desviem a organização de seus objetivos, considerando os riscos inerentes às atividades institucionais, novas realidades, mudanças sociais, dinâmicas da administração pública e requisitos legais e regulatórios.

Uma gestão de riscos eficaz gera benefícios diretos para os cidadãos e outras partes interessadas da organização. Ela proporciona suporte adequado às decisões sobre a alocação e uso dos recursos públicos, aumentando a eficácia no atingimento de objetivos e protegendo o valor público ao otimizar o desempenho e os resultados entregues.

Portanto, é essencial que a organização gerencie, identifique, analise e avalie riscos para alcançar seus objetivos e propósitos.

É com o propósito de que a CAPES atinja seus objetivos organizacionais que a metodologia de gestão de riscos foi desenvolvida e está proposta neste documento.

1.1. Fundamentos da Gestão de Riscos da CAPES

No âmbito do executivo federal, o marco regulatório orientativo em gestão de riscos é a Instrução Normativa Conjunta MP/CGU nº 01/2016, que dispõe sobre controles internos, gestão de risco e governança no âmbito do Poder Executivo Federal. Além da IN, o Decreto nº 9.203/2017, que dispõe sobre a política de governança da administração pública federal direta, autárquica e fundacional, agregou especialmente quanto às atribuições da alta administração.

No âmbito institucional, com a instituição da Portaria CAPES nº 301/2022, que estabelece Política de Gestão de Riscos e Controles Internos da entidade, foram estabelecidas diretrizes a serem observadas na sua implementação, dentre elas a necessidade da utilização de metodologia e ferramentas para apoio à gestão de riscos.

O desenvolvimento da metodologia de gestão de riscos da CAPES foi pautado em frameworks internacionais, especialmente a ABNT NBR 31000:2018; em referências nacionais, como o Manual de Gestão de Riscos do TCU e em metodologias desenvolvidas por outros órgãos públicos, como a CGU, MEC e MCTI. Essa prática é indicada no Roteiro de Avaliação de Maturidade da Gestão de Riscos do TCU, publicado em 2018, que considera que a adoção de padrões e boas práticas convencionados em modelos de referência de gestão de risco, é uma maneira eficaz de se estabelecer uma abordagem sistemática, oportuna e estruturada para gestão de riscos, evitando que sejam acumulados instrumentos e procedimentos burocráticos e descoordenados.

A ISO 31000 é um framework desenvolvido pela International Organization for Standardization – Technical Committee on Risk Management (ISO/TC), com o objetivo de estabelecer um padrão internacional para a gestão de riscos corporativos. No Brasil, a Associação Brasileira de Normas Técnicas (ABNT) realizou a tradução, com a primeira versão publicada em 2009 e atualizada em 2018. O escopo da norma é fornecer diretrizes para a gestão de riscos enfrentados pelas organizações, permitindo que essas diretrizes sejam personalizadas para se adequar a qualquer organização, contexto, atividade e nível de tomada de decisão.

1.2. Principais Conceitos

- **Apetite ao risco:** nível de risco que a instituição está disposta a aceitar;
- **Auditoria Interna:** atividade independente e objetiva de avaliação e de consultoria, desenhada para adicionar valor e melhorar as operações de uma organização;
- **Causas:** São as condições que possibilitam a ocorrência de um evento, também conhecidas como fatores de risco. Podem ter origem tanto no ambiente interno quanto externo;
- **Comitê Gerencial de Governança da CAPES (CGG):** constitui instância interna e intermediária de governança, de natureza consultiva e avaliativa;
- **Comitê Interno de Governança da CAPES (CIG):** Constitui instância interna e estratégica de governança, de natureza deliberativa, consultiva e avaliativa;
- **Consequência:** É o resultado de um evento de risco que impacta os objetivos do processo. As consequências podem ser certas ou incertas, e podem ter efeitos positivos ou negativos. Essas consequências podem ser expressas de forma qualitativa ou quantitativa, e podem se intensificar por meio de efeitos em cascata e cumulativos;
- **Controles internos da gestão:** conjunto de regras, procedimentos, diretrizes, protocolos e rotinas de sistemas informatizados, além de conferências e trâmites de documentos e informações. Esses elementos são operacionalizados de forma integrada pela direção e pelo corpo de servidores das organizações, com o propósito de enfrentar riscos e garantir uma segurança adequada, assegurando que os objetivos sejam alcançados;
- **Evento de Risco:** Um evento é um incidente ou ocorrência originada de fontes internas ou externas que afeta a realização dos objetivos. Esses eventos podem ter impactos negativos, positivos ou ambos. Aqueles que geram impactos negativos são considerados riscos, referindo-se à possibilidade de um evento que possa comprometer o cumprimento dos objetivos estabelecidos;
- **Gerenciamento de riscos:** é o processo de identificar, avaliar, administrar e controlar potenciais eventos ou situações, visando proporcionar uma segurança adequada em relação ao alcance dos objetivos da organização;
- **Gestão de riscos:** é um 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 o 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 dentro do apetite de risco da organização;
- **Governança:** refere-se ao 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:** é o resultado ou efeito de um evento. Um único evento pode gerar uma série de impactos possíveis;
- **Incerteza:** é a incapacidade de prever com antecedência a real probabilidade ou o impacto de eventos futuros;
- **Mensuração de risco:** refere-se à estimativa da importância de um risco, incluindo o cálculo da probabilidade e do impacto de sua ocorrência;
- **Política de Gestão de Riscos e Controles Internos:** é uma declaração de intenções e diretrizes gerais de uma organização relacionadas à gestão de riscos;
- **Probabilidade:** refere-se à chance de um evento específico ocorrer. Ela expressa a possibilidade de que algo aconteça, podendo ser definida, medida ou determinada de forma objetiva ou subjetiva, qualitativa ou quantitativa;
- **Resposta ao risco:** é a ação da administração tomada após a avaliação do risco, que pode incluir reter, reduzir, transferir ou evitar o risco;

- **Risco inerente:** é o risco ao qual uma organização está exposta sem levar em conta quaisquer ações gerenciais que possam reduzir a probabilidade de sua ocorrência ou seu impacto;
- **Risco residual:** é o risco ao qual uma organização está exposta após a implementação de ações gerenciais destinadas ao tratamento do risco;
- **Risco:** é a possibilidade de ocorrência de um evento que possa impactar o alcance dos objetivos da organização, sendo mensurado em termos de impacto e probabilidade.

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 busca melhorar o desempenho dos processos, garantindo ganhos em termos de entrega de resultados e alcance dos objetivos institucionais. Além disso, a política auxilia os gestores na tomada de decisões de forma mais racional, aumentando a capacidade da organização de lidar com eventos inesperados. Outro objetivo é estimular a transparência e o uso eficiente, eficaz e efetivo dos recursos, fortalecendo a imagem da instituição perante a sociedade.

2.3. Princípios, diretrizes e objetivos

A Política de Gestão de Riscos e Controles Internos da CAPES (Portaria CAPES nº 301/2022) estabelece que na sua implementação serão observados os princípios dispostos na Instrução Normativa Conjunta CGU/MP nº1/2016. Dentre eles:

Tabela 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 da Portaria CAPES nº 301/2022.

Tabela 2 - Prncípios 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 reponsabilidades 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;
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; e
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.

Além disso, deverão ser de observância pela CAPES os demais princípios delineados pelos órgãos de controle que visam aprimorar e aperfeiçoar a Política de Gestão de Riscos e Controles Internos da Administração Pública federal. (Parágrafo único do art.2º da Portaria CAPES 301/2022).

A política também estabeleceu que a implementação da gestão de riscos deve observar as seguintes diretrizes:

Tabela 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.

Por conseguinte, no que se refere aos objetivos para a implementação da gestão de riscos, serão observados os que estão dispostos na Instrução Normativa Conjunta CGU/MP nº 1, de 2016, sendo eles:

Tabela 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 da Portaria CAPES nº 301/2022.

2.3.1. INTEGRAÇÃO AO PLANEJAMENTO ESTRATÉGICO

No âmbito da CAPES, um dos princípios estabelecidos na Política de Gestão de Riscos e Controles Internos é o alinhamento estratégico e sistêmico. Para um bom gerenciamento de riscos, é essencial considerar todos os elementos relevantes dispostos no Plano Estratégico da entidade, bem como observar as diretrizes derivadas dos órgãos centrais dos sistemas federais.

De acordo com a Portaria CAPES nº 301/2022, a gestão de riscos deve estar em consonância com o Planejamento Estratégico Institucional vigente. Isso implica que os processos e ações devem estar diretamente ligados 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 instituição.

Nesse contexto, a gestão de riscos será implementada na atual cadeia de valor desenvolvida pela entidade, conforme os macroprocessos estabelecidos. Ela será gradualmente incorporada em todas as diretorias da CAPES, com a priorização dos processos e projetos organizacionais.

2.3.2. ESTRUTURA DE GESTÃO DE RISCOS DA CAPES

A gestão de riscos assume um papel fundamental na governança da entidade, com o objetivo de assegurar o cumprimento do plano estratégico e operacional da instituição, além de integrar o processo decisório e a definição da estratégia. Isso visa a estabelecer uma estrutura clara de responsabilidades e funções.

A governança orienta a direção da organização, suas relações externas e internas, e as regras, processos e práticas necessárias para alcançar seu propósito. As estruturas de gestão traduzem essa direção em estratégias e objetivos necessários para atingir níveis desejados de desempenho sustentável e viabilidade a longo prazo. Assim, 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 ajudar a organização a incorporar a gestão de riscos em suas atividades importantes. A eficácia da gestão de riscos está ligada à sua integração com a governança e as atividades da organização.

O desenvolvimento da estrutura de gestão de riscos envolve os componentes de liderança e comprometimento, concepção, integração, implementação, avaliação e melhoria da gestão de riscos, conforme estabelece a ISO 31.000:2018. Dessa forma, a estrutura da CAPES pode ser compreendida da seguinte maneira:

→ **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 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.

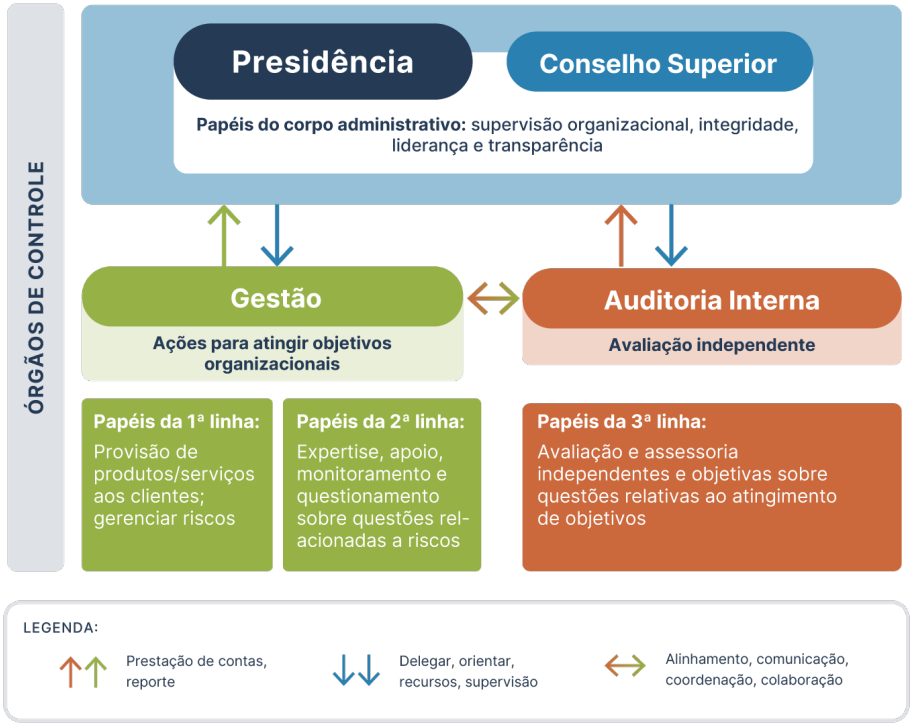
2.3.3. COMPETÊNCIAS E RESPONSABILIDADES

As competências e responsabilidades no gerenciamento de riscos foram estabelecidas com base no modelo de três linhas do *Institute of Internal Auditors (IIA)*. Essa abordagem visa garantir que cada grupo de servidores tenha funções específicas na gestão de riscos, atuando de forma coordenada.

O objetivo é evitar falhas, eliminar duplicidade s e aprimorar a comunicação, por meio do esclarecimento de atribuições relacionadas ao gerenciamento de riscos. Dessa forma, a Política de Gestão de Riscos detalha as competências envolvidas no processo, estruturando a coordenação e os papéis dos agentes e instâncias de acordo com o Modelo de Três Linhas.

Essa estruturação de competências e responsabilidades, baseada no Modelo de Três Linhas, visa promover uma gestão de riscos mais eficaz e integrada.

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



Fonte: Elaboração Própria

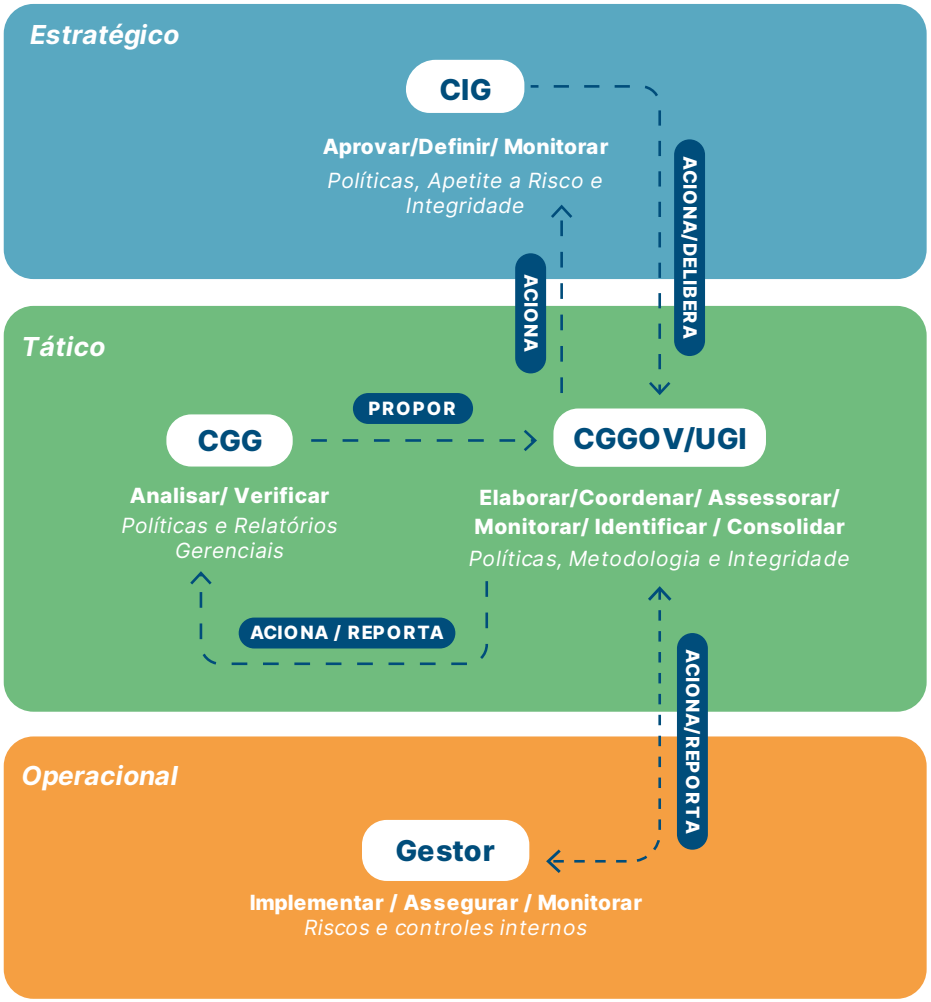
A **1ª linha** é composta pelos gestores de risco nas unidades. Esses agentes são responsáveis por identificar, avaliar, controlar e mitigar os riscos de suas respectivas unidades. Eles desenvolvem e implementam políticas e procedimentos internos para garantir que as atividades sejam realizadas conforme as metas e objetivos da organização. Além disso, são responsáveis por implementar ações corretivas e reportar os resultados às demais linhas, conforme a periodicidade determinada na política de gestão de riscos.

A **2ª linha** opera ao nível da gestão e é composta pela Coordenação Geral de Governança e Planejamento e pela Unidade de Gestão da Integridade. Essas instâncias apoiam o desenvolvimento dos controles internos de gestão e realizam atividades de supervisão e monitoramento das atividades da primeira linha. Isso inclui gerenciamento e monitoramento de riscos, conformidade, verificação de qualidade, controle financeiro, orientação e treinamento.

A **3ª linha** é composta pela auditoria interna, que fornece serviços de avaliação e consultoria fundamentados nos princípios de autonomia técnica e objetividade. O objetivo é contribuir para o aprimoramento da política e do plano de gestão de riscos e controles da CAPES. Os destinatários dos serviços da Auditoria Interna são a primeira e a segunda linha.

De acordo com o art. 7º da Portaria CAPES nº 301/2022, no que se refere às responsabilidades, a Presidência da Fundação é a principal responsável pelo estabelecimento da estratégia da organização e pela estrutura de gerenciamento de riscos, incluindo a manutenção, o monitoramento e o aprimoramento dos controles internos de gestão.

Figura 2 - Fluxo de Comunicação entre as instâncias da CAPES



Fonte: Elaboração Própria

Conforme ilustrado na imagem ao lado, o nível operacional, representado pelo gestor de risco na diretoria, poderá acionar o nível tático, representado pela Coordenação-Geral de Governança e Planejamento (CGGOV). 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 ampla.

A CGGOV, 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 modelo de gestão de riscos.

No nível estratégico, o Comitê Interno de Governança pode ser acionado pelo nível tático para definir, aprovar e monitorar as ações da política de gestão de integridade, riscos e controles de gestão. O CIG tem a função de aprovar a política e a metodologia de gestão de riscos e controles internos da entidade, bem como suas revisões. Segundo o art.9º da portaria, ele define os níveis de apetite ao risco aceitos pela Fundação e monitora os riscos estratégicos e de integridade, além das respectivas medidas de mitigação.

As diretorias da CAPES têm a competência de designar os gestores de riscos dos processos e projetos organizacionais sob sua responsabilidade, consoante o art. 9º da portaria. O Comitê Gerencial de Governança é responsável por analisar e opinar sobre as propostas e relatórios gerenciais elaborados pela CGGOV, relacionados à Política e à Metodologia de Gestão de Riscos e Controles Internos e suas revisões. O comitê também verifica, segundo o art.10 da Portaria, o alinhamento da Política de Gestão de Riscos e Controles Internos aos padrões de ética e conduta, em conformidade com o Programa de Integridade da Fundação e ao Planejamento Estratégico Institucional.

Segundo a Portaria, à **Coordenação-Geral de Governança e Planejamento** compete:

- Elaborar e propor a Política e a Metodologia de Gestão de Riscos e Controles Internos da CAPES e suas revisões;
- Coordenar a implementação da Política e Metodologia de Gestão de Riscos e Controles Internos, nos termos definidos pelos comitês de Governança da CAPES
- Coordenar a implementação da Política e Metodologia de Gestão de Riscos e Controles Internos, nos termos definidos pelos comitês de Governança da CAPES;
- Assessorar os gestores de riscos na identificação, avaliação, seleção de respostas e monitoramento dos riscos e controles internos;
- Monitorar a gestão de riscos e controles internos da CAPES, verificando continuamente sua adequação, efetividade e eficácia; Identificar, analisar e avaliar os riscos estratégicos; e
- Consolidar os resultados das diversas áreas em relatórios gerenciais e encaminhá-los ao Comitê Gerencial de Governança ou qualquer outra instância superior que os solicitar.

À Unidade de Gestão da Integridade compete:

- Identificar, analisar e avaliar os riscos à integridade.

Aos gestores de riscos compete, em relação aos processos ou projetos organizacionais sob sua responsabilidade:

- Implementar a Política de Gestão de Riscos e Controles Internos;
- Assegurar que o risco seja gerenciado de acordo com a Política de Gestão de Riscos da organização;
- Identificar, analisar e avaliar os riscos;
- Propor respostas aos riscos e as respectivas medidas de controles internos a serem implementadas;
- Monitorar a evolução dos níveis de riscos e a efetividade das medidas de controles implementadas;
- Informar a Coordenação-Geral de Governança e Planejamento sobre mudanças significativas no curso do monitoramento dos riscos; e
- Responder às requisições da Coordenação-Geral de Governança e Planejamento ou qualquer instância superior, acerca de informações para elaboração de relatórios gerenciais.

Por fim, **todos os servidores e colaboradores** da CAPES tem por competência:

- O monitoramento da evolução dos níveis de riscos corporativos e da efetividade das medidas de controles internos implementadas nos processos e projetos organizacionais em que estiverem envolvidos ou que tiverem conhecimento,
- Caso sejam identificadas mudanças ou fragilidades nos processos ou projetos organizacionais, o colaborador deverá reportar imediatamente o fato ao gestor de riscos do processo ou projeto em questão.

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 de gestão de riscos.

A gestão de riscos preserva e agrega valor à organização, contribuindo significativamente para a realização de suas metas de desempenho, objetivos e cumprimento de sua missão, representando mais do que um mero conjunto de procedimentos e políticas de controle.

O processo de gestão de riscos 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 envolvem identificar, analisar, avaliar, priorizar e responder aos riscos significativos, mediante controles ou outras respostas, além de monitorar e comunicar o desempenho da gestão de riscos. (ABNT e TCU, 2018).

Assim, a Metodologia de Gestão de Riscos da CAPES serve como base para a implementação da gestão de riscos na instituição. No entanto, as legislações pertinentes que abordam temas específicos, como as relacionadas a licitações, prestação de contas de convênios e contratos deverão ser observados.

3.1. Etapas

As etapas que envolvem 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, que estabelece:

> *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 ao lado:

Figura 3 - Operacionalização da Gestão de Riscos

Fonte: Elaboração Própria

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

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 objetiva estabelecer os objetivos prioritários no gerenciamento de riscos. 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 (estratégico, operacional, programa, projeto etc.).

Dessa forma, é importante deixar claro cada objetivo priorizado, o escopo, os objetivos pertinentes e o alinhamento aos objetivos operacionais.

No âmbito da CAPES, os objetivos a serem atingidos e a forma de alcançá-los estão estabelecidos no Plano Estratégico Institucional (PEI), que compreende a missão, os valores, os objetivos estratégicos para o ciclo de quatro anos, representados no mapa estratégico. Aos objetivos estratégicos se vinculam os indicadores, metas e portfólio de projetos. Para o alcance desses objetivos estratégicos, a entidade dispõe dos processos organizacionais organizados em uma Cadeia de Valor conforme a finalidade (macroprocessos finalísticos, de governança e de apoio). Dentro de cada macroprocesso, é considerado ainda o processo crítico, que é aquele cujo resultado impacta diretamente nas entregas do macroprocesso da organização.

Os processos críticos da entidade se constituem como elemento base para a gestão de riscos, tendo em vista o impacto que terão para o alcance dos objetivos estratégicos. Nesses termos, a gestão de riscos tem a integração com o planejamento estratégico, atendendo ao que está estabelecido em sua Política de Gestão de Riscos e Controles Internos.

Figura 4 - Perspectiva da Gestão de Riscos na CAPES

Fonte: Elaboração Própria

Por último, serão analisados os critérios mais importantes com base nos quais os níveis de riscos serão observados, considerando as escalas de consequências ou impactos. Também será determinado se o nível de risco é tolerável ou aceitável, e se as ações de tratamento são necessárias, ou seja, as diretrizes para a priorização e tratamento de resposta a riscos.

Conforme apresentado anteriormente no item “Responsabilidades e Competências”, é de competência da Coordenação-Geral de Governança e Planejamento coordenar a implementação da Política e Metodologia de Gestão de Riscos e Controles Internos, nos termos definidos pelos Comitês de Governança da CAPES.

3.1.2. ENTENDIMENTO DO CONTEXTO

ETAPA 1 – Entendimento do contexto

Etapa em que o contexto interno e externo do objeto de gestão de riscos é analisado.

O entendimento do contexto objetiva identificar e compreender os fatores do ambiente interno e externo à organização no qual o objeto de gestão de riscos se encontra inserido.

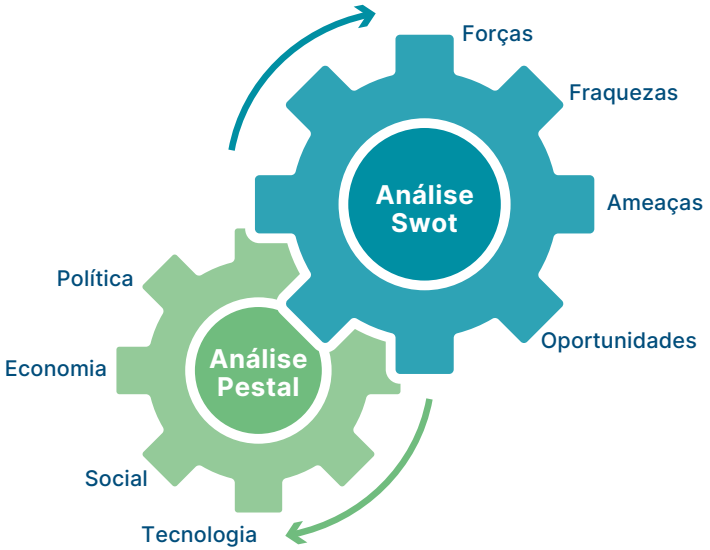
Nessa etapa, é necessário realizar um relato conciso sobre a vinculação aos objetivos organizacionais e uma análise dos fatores internos e externos do ambiente, utilizando a análise SWOT. As informações a serem levantadas sobre o objeto incluem: a vinculação ao plano estratégico, os objetivos do objeto, as partes interessadas, a legislação pertinente, a previsão orçamentária, o fluxo do processo, a infraestrutura, os principais problemas do passado, os recursos humanos utilizados, os sistemas informatizados, entre outros.

O levantamento das partes interessadas pode ser realizado por meio da análise de stakeholders, da matriz RACI e da matriz de responsabilidades. As partes interessadas devem ser incluídas em cada etapa ou ciclo do processo de gestão de riscos, por meio de um processo de comunicação eficaz. Dessa forma, suas expectativas e preocupações podem ser compreendidas de maneira mais aprofundada, promovendo um maior engajamento e soluções construtivas.

Ferramentas para essa etapa:

- Análise SWOT
- Análise PESTEL

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 eventos de risco são identificados, são levantadas as possíveis causas e consequências; e são classificados 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).

Para identificar os riscos, é necessário que seja levado em consideração o entendimento do contexto, realizado na etapa anterior, além de outros fatores, como: as

fontes de riscos, áreas de impactos, as mudanças nos contextos interno e externo, os cenários etc. Informações pertinentes, apropriadas e atualizadas são importantes na identificação dos riscos.

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.

A identificação dos riscos é caracterizada pela identificação do evento de risco, das causas e das consequências.

CAUSAS:
São as condições que possibilitam a ocorrência de um evento. Podem ter origem tanto no ambiente interno quanto externo. É composta pela **fonte + vulnerabilidade.**

EVENTO DE RISCO:
Possibilidade de ocorrência de um evento que possa impactar o cumprimento do objetivo do objeto.

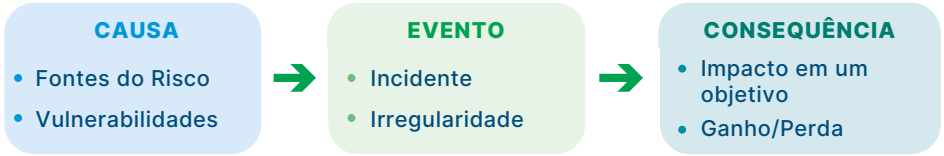
CONSEQUÊNCIA:
É o resultado decorrente de um evento de risco sobre os objetivos do objeto.

Uma sintaxe muito utilizada para designar os riscos é:

Devido a [causa]	+	poderá ocorrer [evento de 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 levar a atraso no pagamento das bolsas.

A referida sintaxe está representada graficamente abaixo:



Para facilitar a identificação das causas, é importante identificar as possíveis fontes de risco, conforme exemplos abaixo:

Quadro 1 - Fontes de Causa x 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.

Fontes de Risco	Vulnerabilidades
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, é possível classificá-los em categorias, para melhor compreensão e organização dos riscos. No quadro a seguir, é possível observar a tipologia de riscos.

Quadro 2 - 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.

3.1.4. IDENTIFICAÇÃO DOS CONTROLES

ETAPA 3 – Identificação dos controles

Etapa em que são levantados os controles já estabelecidos para determinado evento de risco.

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 dos controles tem como objetivo identificar quais controles já estão sendo utilizados para mitigar os riscos identificados na etapa anterior. Nesta fase, os controles são apenas identificados e listados, proporcionando mais clareza na avaliação que será realizada na próxima etapa, quando os níveis de risco inerente e residual serão calculados.

Os controles identificados devem ser classificados em três tipos: preventivos, corretivos e detectivos.

Quadro 3 - 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 risco. *Exemplos: Monitoramento*

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 inerente e residual

O cálculo de nível de risco é composto por dois cálculos: Cálculo do Risco Inerente e Cálculo do Risco Residual, conforme definição descrita no quadro a seguir:

Quadro 4 - Tipos de Risco

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

3.1.5.1. CÁLCULO DO NÍVEL INERENTE

Para calcular o nível de risco inerente, é necessário avaliar a probabilidade de sua ocorrência e o impacto no caso de materialização do evento de risco, considerando que não há nenhum controle em vigor. Nesse contexto, a função de risco é definida como:

Figura 6 - Função do Risco Inerente

Fonte: Elaboração Própria

Os níveis de riscos inerentes são determinados com base no resultado da combinação dos níveis de probabilidade e impacto.

Importante!

O levantamento dos controles, efetuados na etapa anterior, auxilia na clareza do que é um controle, facilitando na avaliação da probabilidade e impacto, desconsiderando a existência desses controles.

Escala de Probabilidade

Para avaliar a probabilidade de ocorrência de um determinado risco, utiliza-se uma escala estabelecida com 5 níveis de risco, suas classificações e descrições, conforme apresentado na Tabela a seguir:

Tabela 5 - Escala de Probabilidade

Níveis	Probabilidade	Descrição
1	Muito baixa	Improvável. O evento poderá ocorrer em situações excepcionais, mas não há histórico disponível de sua ocorrência ou são raros os casos práticos onde se percebe a ocorrência deste tipo de evento.
		Chance de acontecer ou frequência observada menor que 10%
2	Baixa	Pouco provável. O evento poderá ocorrer de forma inesperada ou casual, pois o histórico conhecido aponta para baixa frequência de ocorrência deste tipo de evento.
		Chance de acontecer ou frequência observada entre 10 e 30%
3	Média	Possível. O evento pode ocorrer em algum momento, pois o histórico de ocorrência conhecido indica moderadamente essa possibilidade.
		Chance de acontecer ou frequência observada entre 30 e 60%
4	Alta	Provável. O evento é esperado, provavelmente ocorrerá na maioria das circunstâncias, pois o histórico conhecido indica fortemente essa possibilidade.
		Chance de acontecer ou frequência observada entre 60 e 80%
5	Muito alta	Praticamente certa. O evento é frequente, ocorre repetidamente, seu histórico indica claramente essa possibilidade.
		Chance de acontecer ou frequência observada entre 80 e 100%

Fonte: Elaboração própria.

Escala de Impacto

Para avaliar o impacto do evento de risco nos objetivos do plano, utiliza-se uma escala de impacto.

Tabela 6 - Escala de Impacto

Níveis	Impacto	Descrição
1	**Muito baixo**	Impacto mínimo. Não altera o alcance dos objetivos do projeto ou a alteração é insignificante.
2	**Baixo**	Impacto pequeno. Comprometem muito pouco o alcance dos objetivos do projeto, é de fácil reparação/recuperação.

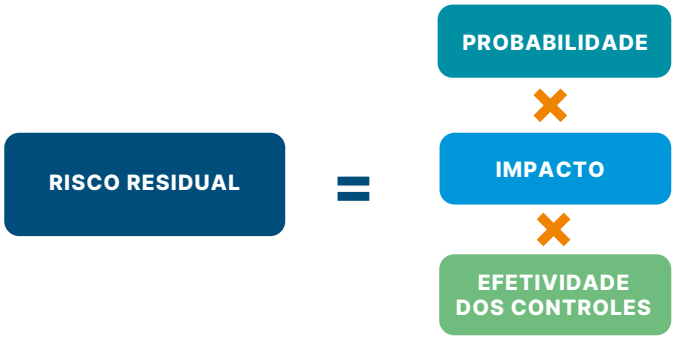
Níveis	Impacto	Descrição
3	**Médio**	Impacto moderado. Compromete razoavelmente o alcance dos objetivos, porém é possível a reparação/ recuperação.
4	**Alto**	Impacto significativo. Compromete a maior parte do atingimento dos objetivos do projeto, de difícil reparação/recuperação.
5	**Muito Alto**	Impacto catastrófico. Compromete totalmente ou quase totalmente de forma irreversível os objetivos do projeto, sem possibilidade de reparação.

Fonte: Elaboração própria.

3.1.5.2. CÁLCULO DO RISCO RESIDUAL

Considerando a análise prévia para o cálculo do risco inerente, os controles implementados devem ser avaliados quanto à sua efetividade, resultando no nível de risco residual.

Figura 7 - Função do Risco Residual



Fonte: Elaboração própria.

Para calcular a efetividade dos controles, deve ser utilizada a seguinte tabela:

Tabela 7 - Efetividade dos Controles

	Descrição	Fator de avaliação
Inexistente	Controles inexistentes, mal implementados ou mal desenhados. Não funcionam para mitigar o risco.	**1**
Fraco	Existem controles, mas não são sistematizados, são aplicados caso a caso e dependem da confiança no conhecimento de outras pessoas. Mitigam minimamente os riscos.	**0,8**
Mediano	Existem controles, mas não contemplam todos os aspectos relevantes, pois há deficiência no desenho do controle e/ou nas ferramentas utilizadas. Mitigam parcialmente o risco.	**0,6**
Satisfatório	Existem controles, são implementados sistematicamente, possuem um bom desenho e/ou ferramenta, mas ainda são passíveis de aperfeiçoamento. Mitigam de forma satisfatória os riscos.	**0,4**
Forte	Existem controles consolidados, tratam todos os aspectos relevantes do risco. Mitigam o máximo possível do risco.	**0,2**

Fonte: Elaboração própria.

O desenho do controle refere-se à adequação do procedimento e sua formalização.

3.1.5.3. CLASSIFICAÇÃO DO NÍVEL DE RISCO

Os níveis de risco inerente e residual serão classificados de acordo com as faixas mencionadas abaixo:

Quadro 5 - Classificação do Nível de Risco

Classificação	Faixa
Risco baixo/pequeno	1 a 3,99
Risco médio/moderado	4 a 6,99
Risco alto	7 a 12,99
Risco crítico/extremo	13 a 25

Fonte: Elaboração própria.

A matriz de riscos, também conhecida como mapa de calor, é uma ferramenta que classifica qualitativamente os níveis de impacto e probabilidade dos riscos. Esta matriz está dividida em quatro áreas, que representam os níveis de risco como pequeno, moderado, alto e crítico. Para esta análise, foram utilizadas cinco escalas distintas tanto para o impacto quanto para a probabilidade, conforme ilustrado a seguir:

Quadro 6 - 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.

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

3.1.6. APETITE A RISCOS

No contexto da avaliação do processo organizacional, a unidade tem a prerrogativa de estabelecer faixas de classificação distintas das indicadas na Metodologia de Gestão de Riscos da CAPES, visando refletir de forma mais precisa o nível de tolerância ao risco desse processo. Conforme a Portaria CAPES nº 301/2022, o apetite ao risco é definido como o "nível de risco que a unidade

está disposta a aceitar". De acordo com o art. 8º, inciso II da Portaria de Gestão de Riscos da entidade, esse apetite deve ser estabelecido pelo Comitê Interno de Governança.

Portanto, é fundamental determinar a disposição da unidade em aceitar riscos no início do processo de gestão de riscos organizacionais. Uma vez definida, a unidade declara que todos os riscos dentro da faixa de tolerância podem ser aceitos, com a possibilidade de justificar a priorização no tratamento. Os riscos que excederem essa faixa serão tratados e monitorados, estando também sujeitos a justificativas caso não sejam abordados.

Dessa forma, estabelecer o apetite de riscos ajuda a organização a definir a quantidade de risco com a qual está disposta a conviver e o quanto precisa gerenciar. O apetite de riscos permite que as organizações determinem até que ponto estão dispostas a assumir riscos para inovar na busca de seus objetivos.

3.1.7. RESPOSTA AOS RISCOS

ETAPA 5 – Resposta aos riscos

Etapa em que, a partir dos níveis de risco residual calculados, são tomadas as decisões para responder aos riscos.

A etapa de resposta aos riscos é aquela em que serão definidas as ações a serem tomadas em relação aos riscos identificados. A faixa de classificação do risco residual deve ser considerada na definição da atitude do gestor em relação à priorização do tratamento.

As ações recomendadas para cada classificação do risco são:

Quadro 7 - Ações recomendadas para cada classificação do risco

Classificação do Nível de risco	Ações
Risco baixo/pequeno	Dentro do apetite a risco. Não é necessário implementar novo controle. Podem existir oportunidades de diminuir os controles.
Risco médio/moderado	Dentro do apetite a risco. É necessário monitorar a efetividade dos controles existentes. Podem ser implementados outros controles que tenham custo/benefício adequado.
Risco alto	Acima do apetite a risco. É necessário adotar alguma medida de controle em um período determinado.
Risco crítico/extremo	Muito acima do apetite a risco. É necessário adotar uma medida de controle imediata.

Fonte: Elaboração Própria

Neste momento, são oferecidas quatro opções de respostas aos riscos, dentre elas: Mitigar, Compartilhar, Evitar e Aceitar.

Quadro 8 - Opções de respostas aos riscos

Opção de Respostas	Descrição
Mitigar	Mitigar o risco significa implementar controles com o objetivo de reduzir a probabilidade ou o impacto dos riscos, atuando nas suas causas ou consequências. Esse processo normalmente ocorre quando o risco está classificado fora do apetite ao risco, buscando trazê-lo para dentro desse limite. É importante avaliar se o custo-benefício da implementação do controle é adequado.
Compartilhar	Compartilhar o risco pode ser realizado por meio de terceirização ou contratação de seguros, visando reduzir tanto o impacto quanto a probabilidade do risco. Essa abordagem normalmente ocorre 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.

3.1.8. ELABORAÇÃO DO PLANO DE AÇÃO

ETAPA 6 – Elaboração do plano de ação

Etapa em que são especificadas as ações selecionadas para responder aos riscos.

A elaboração do plano de ação consiste em especificar, em um documento próprio, os tratamentos a serem implementados para os riscos cujas respostas definidas na etapa anterior foram mitigar ou compartilhar.

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

Figura 8 - Plano de Ação

Os riscos, em ordem de prioridade;
As medidas de tratamento (controles)
A classificação das medidas de tratamento (controle preventivo, corretivos e detectivos)
Os objetivos e benefícios esperados com cada medida de tratamento;
A unidade organizacional responsável por colocar a proposta em prática;
Outras unidades organizacionais envolvidas na implementação, ou seja, aquelas que participam da execução das medidas de tratamento;
O servidor ou cargo responsável pela implementação;
Uma breve explicação sobre como as medidas serão postas em prática;
As datas planejadas para o início e conclusão da implementação;
O status atualizado da proposta.

Fonte: Elaboração própria.

Nesta etapa, é necessário implementar ações de controle preventivo e corretivo, conforme a classificação apresentada na etapa de controle.

Dentre as medidas de tratamento que podem ser inseridas nessa etapa, destacam-se: realocação de pessoal, realização de ações de capacitação, desenvolvimento ou aprimoramento de soluções de TI, readequação da estrutura organizacional e outras ações pertinentes.

O tratamento de riscos proposto deve levar em consideração a relação custo-benefício e a viabilidade das ações.

Os planos de ação devem ser discutidos com as partes interessadas, que devem estar conscientes dos riscos remanescentes. Esses planos também devem prever a periodicidade de monitoramento.

Por fim, os planos de ação devem ser aprovados pelo Comitê Interno de Governança (CIG).

3.1.8.4. IMPLEMENTAÇÃO DO PLANO DE AÇÃO

A execução do plano de ação demanda a colaboração da unidade encarregada do processo organizacional, bem como de outras unidades envolvidas no processo ou cujas ações estejam dentro de sua competência.

A responsabilidade principal pela implementação do plano de ação é da unidade responsável pelo processo organizacional.

3.1.9. 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 9 - 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. Assim, a instituição consegue comunicar-se de maneira eficaz com seu público externo, fortalecendo sua reputação e credibilidade.

3.1.10. 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 eficácia da gestão de riscos. Portanto, o monitoramento deve ser realizado de forma 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 monitoramento estão detalhados no quadro a seguir, que define a periodicidade e a responsabilidade pelo monitoramento:

Quadro 10 - Plano de Monitoramento

Objetivo do monitoramento	Objeto do monitoramento	Quando deverá ocorrer	Quem é o responsável
Revisão	Riscos estratégicos	quando da revisão Planejamento estratégico ou quando houver mudança relevante de contexto	Comitê Interno de Governança
	Política de Gestão de Riscos	a cada 2 anos, sendo a primeira após 1 ano do início da implementação da metodologia	CGGOV
	Metodologia de Gestão de Riscos	a cada 2 anos, sendo a primeira após 1 ano do início da sua implementação	CGGOV
Acompanhamento da implementação	Plano de Gestão de Riscos	de forma contínua, ou no mínimo a cada 1 ano	CGGOV
	Planos de Ação	de forma contínua ou no mínimo a cada 6 meses	Gestor de riscos, assessorado pela CGGOV
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 risco, assessorado pela CGGOV

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.

O monitoramento do funcionamento do Sistema de Gestão de Riscos (SGR/CAPES) é responsabilidade da Coordenação-Geral de Governança e Planejamento (CGGOV), dos coordenadores setoriais e da alta administração da entidade. É importante ressaltar que a gestão de riscos realizada no âmbito das unidades deve ser acompanhada pelo respectivo gestor de riscos de cada uma delas.

4. Considerações Finais

A metodologia de Gestão de Riscos desenvolvida pela CAPES, com o apoio da Unidade de Auditoria Interna (AUD) e da Coordenação-Geral de Governança e Planejamento (CGGOV), representa um significativo avanço para o fortalecimento da governança e do desempenho organizacional da instituição. Ao estabelecer um processo estruturado em nove etapas, a Fundação reafirma seu compromisso em adotar uma abordagem proativa e alinhada aos seus objetivos estratégicos, visando subsidiar a sistematização e a padronização da gestão de riscos na entidade. Além disso, pretende-se fomentar uma cultura de boas práticas na gestão de riscos para melhorar a tomada de decisão gerencial.

A metodologia adotada pela entidade incorpora boas práticas reconhecidas pela ISO 31000. Ademais, está em conformidade com a Instrução Normativa Conjunta CGU/MP nº 01, de 10 de maio de 2016, e com o Decreto nº 9.203, de 22 de novembro de 2017, que dispõe sobre a política de governança da administração pública federal direta, autárquica e fundacional.

Na aplicação desta metodologia, é fundamental registrar, organizar, documentar e referenciar os dados e informações considerados. Isso visa evidenciar o embasamento dos resultados, subsidiar a aprovação pelos atores competentes e produzir um histórico dos fatos que serão importantes para futuras ações dos gestores.

Com o intuito de melhorar continuamente o processo de gestão de riscos, esta metodologia estará em constante aperfeiçoamento. Portanto, feedbacks após a aplicação pelas unidades da entidade serão essenciais para seu aprimoramento.

Recomenda-se a realização de projetos-piloto pelas unidades da entidade para a implantação do processo de gestão de riscos, utilizando esta metodologia e suas ferramentas de suporte. A partir das experiências piloto, os gestores e equipes adquirirão maior expertise e segurança para prosseguir com a aplicação nos demais objetos da gestão de riscos priorizados pelas unidades.

A implementação desta metodologia permitirá à entidade identificar, avaliar e gerenciar de forma efetiva os riscos que possam afetar o cumprimento de sua missão e o alcance de suas metas. Além disso, 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 demonstra seu compromisso com a melhoria contínua de seus processos e com a busca pela excelência na prestação de serviços públicos. Espera-se que a adoção desta metodologia de Gestão de Riscos e Controles Internos seja um passo importante para consolidar a Fundação como uma instituição de 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.

BLUMEN, Abrão; SILVA, Valmir Leôncio da; SALES, Eurípedes (Coords.). **Controle interno como suporte estratégico de governança no setor público.** 1. ed. Belo Horizonte: Fórum, 2015. 106 p. (Coleção Fórum Contas Públicas).

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.

COSO – COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION. **Controle Interno – Estrutura integrada: sumário executivo e estrutura.** Tradução de PriceWatherhouseCoopers e Instituto dos Auditores Internos do Brasil. São Paulo: The IIA Brasil e PwC, 2013. Disponível em: <http://www.iiabrasil.org.br/new/2013/downs/coso/COSO_ICIF_2013_Sumario_Executivo.pdf>.

GAO – UNITED STATES GOVERNMENT ACCOUNTABILITY OFFICE. **Standards for Internal Control in the Federal Government.** United States of America, 2014.

HILL, Stephen. **Guia sobre a gestão de riscos no serviço público.** Tradução de Luís Marcos B. L. de Vasconcelos. Cadernos ENAP, Brasília, n. 30, 2006.

INSTRUÇÃO NORMATIVA CONJUNTA Nº 1, DE 10 DE MAIO DE 2016. Dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo federal. Disponível em: <https://ufu.br/legislacoes/instrucao-normativa-conjunta-mpcgu-no-012016>.

INTOSAI – INTERNATIONAL ORGANIZATION OF SUPREME AUDIT INSTITUTIONS. **GOV 9130 – Guidelines for Internal Controls Standards for the Public Sector. Further Information on Entity Risk Management.** PSC Subcommittee on Internal Control Standards. [s.l.]: INTOSAI, 2007.

MINISTÉRIO DA EDUCAÇÃO. **Política de Gestão de Riscos e Controles Internos da Fundação Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - CAPES.** Portaria nº 301, de 22 de dezembro de 2022. Disponível em: <http://cad.capes.gov.br/ato-administrativo-detalhar?idAtoAdmElastic=10443#anchor>.

MIRANDA, Rodrigo Fontenelle de A. I**mplementando a gestão de riscos no setor público.** Belo Horizonte: Fórum, 2017.

TCU – TRIBUNAL DE CONTAS DA UNIÃO. **Portaria Segecex nº 9, de 18 de maio de 2017. Aprova o documento "Roteiro de Auditoria de Gestão de Riscos"**. Brasília: TCU, 2017.

UK – UNITED KINGDOM. **The Orange Book: Management of risk – Principles and concepts.** Norwich: HM Treasury, 2004. Disponível em: <www.who.int/management/general/risk/managementofrisk.pdf>.

CAPES

MINISTÉRIO DA EDUCAÇÃO

GOVERNO FEDERAL
BRASIL
UNIÃO E RECONSTRUÇÃO