MANUAL DE GESTÃO DE RISCOS AUDIN/INEP

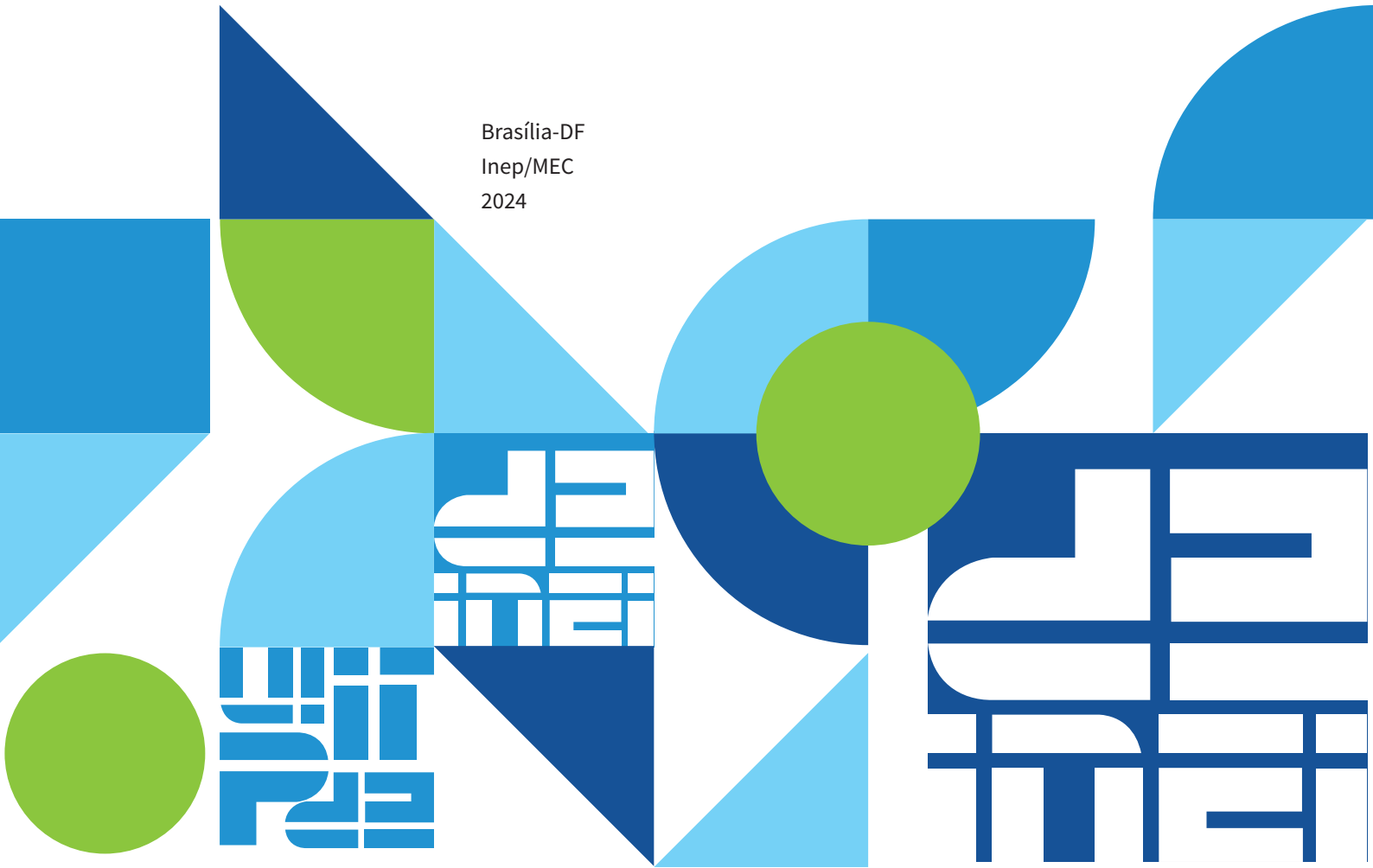
REPÚBLICA FEDERATIVA DO BRASIL

MINISTÉRIO DA EDUCAÇÃO | **MEC**

INSTITUTO NACIONAL DE ESTUDOS E PESQUISAS EDUCACIONAIS ANÍSIO TEIXEIRA | **INEP**

MANUAL DE GESTÃO DE RISCOS AUDIN/INEP

Brasília-DF
Inep/MEC
2024



PRESIDÊNCIA DO INEP

AUDITORIA INTERNA
Anderson Soares Furtado Oliveira
Cleuber Moreira Fernandes
Cristina Lopes Ribeiro Escórcio
Johanes Severo dos Santos
Joilma Sant'Anna Favero
José Valdo de Oliveira Junior
Katharine Mota de A. Bonfim
Lenice Medeiros
Luiz Claudio Senna Costa
Rafaela Rodrigues Marques
Thais Cristine Sousa da Silva

DIRETORIA DE ESTUDOS EDUCACIONAIS (DIRED)

COORDENAÇÃO-GERAL DE EDITORAÇÃO E PUBLICAÇÕES (CGEP)
Priscila Pereira Santos

DIVISÃO DE PERIÓDICOS (DPE)
Roshni Mariana de Mateus

DIVISÃO DE PRODUÇÃO EDITORIAL (DPR)
Ricardo Cézar Blezer

APOIO EDITORIAL
Janaína da Costa Santos

REVISÃO LINGUÍSTICA
Nadine Ribeiro

NORMALIZAÇÃO
Nathany Brito Rodrigues

PROJETO GRÁFICO CAPA/MIOLO
Marcos Hartwich/Raphael C. Freitas

DIAGRAMAÇÃO E ARTE-FINAL
Érika Janaína de Oliveira Saraiva

REVISÃO GRÁFICA
José Miguel do Santos

ESTA PUBLICAÇÃO DEVERÁ SER CITADA DA SEGUINTE FORMA:

BRASIL. Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira (Inep). *Manual de Gestão de Riscos Audin/Inep*. Brasília, DF: Inep, 2024.

SUMÁRIO

ESTA PUBLICAÇÃO POSSUI SUMÁRIO INTERATIVO
PARA RETORNAR AO SUMÁRIO, CLIQUE NO NÚMERO DA PÁGINA EM CADA SEÇÃO

1 INTRODUÇÃO

Este documento apresenta os fundamentos, a estrutura e a Metodologia de Gestão de Riscos da Unidade de Auditoria Interna do Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira (Audin/Inep).

A gestão de riscos da Audin tem como propósito geral subsidiar a tomada de decisão, contribuindo para o alcance da sua missão institucional, que guarda estreita relação com o objetivo presente no Planejamento Estratégico Institucional (PEI) 2020-2023 do Inep:

> *Fortalecer os mecanismos de governança, integridade e gestão estratégica:* Promover a eficiência operacional por meio da execução de mecanismos de governança, da integridade e da gestão estratégica, com vistas à correção de eventuais desvios por meio da identificação e gerenciamento dos riscos inerentes a esses processos. (Brasil. Inep, 2022).

Dessa maneira, destaque-se que os principais objetivos da gestão de riscos da Audin são:

- Aumentar a probabilidade de atingimento dos objetivos;
- Atentar para a necessidade de se gerenciar riscos em todo o Inep;
- Melhorar a governança;
- Fornecer informações relevantes para a tomada de decisão e o planejamento;
- Melhorar os controles internos da unidade;
- Melhorar a eficácia e eficiência operacional.

Conceitualmente, segundo a ABNT (2018), o risco é o efeito da incerteza nos objetivos, e, de acordo com a Instrução Normativa Conjunta MP/CGU nº 1/2016, risco é a possibilidade de ocorrência de um evento que venha a ter impacto no cumprimento dos objetivos, sendo medido em termos de impacto e probabilidade.

A gestão de riscos, por sua vez, segundo a ABNT (2018) é definida como atividades coordenadas para dirigir e controlar uma organização no que se refere a riscos. Gerenciar riscos é um processo contínuo, realizado para identificar e tratar eventos em potencial, cuja ocorrência poderá afetar positiva ou negativamente o alcance dos objetivos institucionais.

Portanto, este documento estrutura a gestão de riscos dos processos de trabalho da Audin, em especial aqueles relacionados à sua atividade-fim, serviços de auditoria. O documento também é um instrumento elaborado com o objetivo de direcionar, de forma coordenada, a gestão dos riscos a partir de procedimentos simplificados e passíveis de evidenciação, com vistas a reduzir os riscos que possam comprometer a atuação da Audin e a entrega de resultados de alta qualidade.

2 Fundamentos da Gestão de Riscos da Audin

2.1 Parâmetros legais e frameworks

A base teórico-conceitual da Metodologia de Gestão de Riscos da Audin está pautada em frameworks internacionais, normativos e referências nacionais de gestão de riscos e controles internos, entre os quais destacam-se:

- COSO - ERM – Gerenciamento de Riscos Corporativos – Estrutura Integrada, 2017;
- ABNT NBR ISO 31.000:2009, Gestão de Riscos – Princípios e Diretrizes;
- ABNT NBR ISO 31010:2012, Gestão de Riscos – Técnicas para o processo de avaliação de riscos;
- ABNT NBR ISO 31.000:2018, Gestão de Riscos – Princípios e Diretrizes;
- Instrução Normativa Conjunta CGU/MP nº 1, de 10/5/2016;
- *Declaração de posicionamento do IIA*: as três linhas de defesa no gerenciamento eficaz de riscos e controles.

Com o objetivo de destacar a importância da gestão de riscos no processo de definição da estratégia da organização e na condução de seus resultados, o Committee of Sponsoring Organizations of the Treadway Commission (COSO) 2017 aumentou o foco em gestão de riscos, e foi intitulado Gerenciamento de Riscos Corporativos – Estrutura Integrada.

Nessa mesma direção, em 2018 foi atualizada a norma ABNT NBR ISO 31000:2009, Gestão de Riscos – Princípios e Diretrizes, com o objetivo de disseminar princípios e diretrizes para a gestão de riscos, aplicáveis a organizações de qualquer setor.

No âmbito do Poder Executivo Federal, o marco regulatório que orienta os órgãos e as entidades públicas à estruturação de mecanismos de controles internos, gestão de riscos e governança é a Instrução Normativa Conjunta MPOG/CGU nº 1, de 10 de maio de 2016, em que são apresentados conceitos, princípios, objetivos e responsabilidades relacionados aos temas.

No Inep, o tema está balizado pela Política de Governança, Integridade, Riscos e Controles Internos (PGIRC), instituído por meio da Portaria nº 565, de 28 de dezembro de 2022.

Assim, a gestão de riscos da Audin busca o alinhamento com os principais frameworks do mercado e com a legislação afeta ao tema.

2.2 Conceitos

Para fins deste documento, consideram-se os seguintes conceitos extraídos do artigo 6º da PGIRC:

I - agente público: todo aquele que por força de lei, contrato ou qualquer outro ato jurídico preste serviço de natureza permanente, temporária, excepcional ou eventual ao Inep, ainda que não remunerado, inclusive, os ocupantes de cargos em comissão, funções de confiança ou gratificadas e membros dos órgãos estatutários.

II - apetite ao risco: nível de risco que o Inep está disposto a aceitar;

III - controles internos de gestão: conjunto de regras, procedimentos, diretrizes, protocolos, rotinas de sistemas informatizados, conferências e trâmites de documentos e informações, entre outros, operacionalizados de forma integrada, destinados a enfrentar os riscos e fornecer segurança razoável e que os objetivos organizacionais serão alcançados.

IV - gestão de risco: processo de natureza permanente, estabelecido, direcionado e monitorado pela alta administração, que contempla as atividades de identificação, avaliação e gerenciamento de potenciais eventos que possam afetar a organização, destinado a fornecer segurança razoável quanto à realização de seus objetivos;

V - gestor de riscos: pessoa, papel ou estrutura organizacional com autoridade e responsabilidade para gerenciar um risco;

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

VII - medida de controle: medida aplicada, no âmbito do Inep, para tratar os riscos e aumentar a probabilidade de que os objetivos e as metas organizacionais sejam alcançados;

VIII - prestação de contas (accountability): conjunto de procedimentos adotados pelo Inep e pelas pessoas que o integram para evidenciar as responsabilidades inerentes a decisões tomadas e ações implementadas, incluindo a salvaguarda de recursos públicos, a imparcialidade e o desempenho;

IX - programa de integridade: conjunto de medidas e mecanismos institucionais de promoção à ética, correição e transparências que visam garantir a preponderância do interesse público sobre os interesses privados no âmbito das ações e decisões adotadas em uma instituição pública;

X - risco: possibilidade de ocorrência de um evento que venha a ter tenha impacto no cumprimento atingimento dos objetivos, sendo o risco é medido em termos de impacto e de probabilidade; e

XI - tolerância ao risco: nível de variação aceitável quanto à realização dos objetivos.

(Brasil. Inep, 2022, grifo nosso).

3 Estrutura de Gestão de Riscos da AUDIN

Segundo a norma ISO 31000:2018, o propósito da Estrutura de Gestão de Riscos é apoiar a organização na integração da gestão de riscos em atividades significativas e em funções. A eficácia da gestão de riscos dependerá da sua integração na governança e em todas as atividades da organização, incluindo a tomada de decisão. Isso requer apoio das partes interessadas, em particular da alta direção.

Sobre o tema, a Audin segue as diretrizes estabelecidas para a gestão de riscos, conforme estabelece o artigo 12 da PGIRC:

I – a atuação da gestão de riscos deve ser dinâmica e formalizada por meio de metodologias, normas, manuais e procedimentos, sempre que possível baseados em referências e experiências reconhecidas, com apoio inequívoco e comprometimento da alta administração;

II - as metodologias e as ferramentas implementadas devem possibilitar a obtenção de informações úteis à elaboração do planejamento estratégico, à tomada de decisão para a consecução dos objetivos institucionais e para o gerenciamento e a manutenção dos riscos dentro de padrões definidos e à melhoria contínua dos processos organizacionais;

III - a medição do desempenho da gestão de riscos deve ser realizada mediante atividades contínuas ou de avaliações independentes ou a combinação de ambas;

IV - a capacitação dos agentes públicos que exercem cargo, função ou emprego no Inep, em gestão de riscos deve ser desenvolvida de forma continuada, por meio de soluções educacionais, em todos os níveis;

V - o desenvolvimento e a implementação de atividades de controle da gestão devem considerar a avaliação de mudanças, internas e externas, que contribuam para identificação e avaliação de vulnerabilidades que impactam os objetivos estratégicos, táticos e operacionais ; e

VI - os procedimentos de controles internos da gestão devem ser proporcionais aos riscos e baseados na relação custo-benefício e na agregação de valor à instituição. (Brasil. Inep, 2022).

Na concepção da estrutura para gerenciar riscos, a Audin define a responsabilização de seus agentes (seção 3.1), a forma de integração dos processos organizacionais (seção 3.2), os recursos necessários (seção 3.3) e as formas de comunicação (seção 3.4) no âmbito de sua gestão de riscos.

A implementação e avaliação da Estrutura de Gestão de Riscos ocorre por meio da comparação da gestão de riscos da Audin com as bases normativas, os frameworks, os contextos de governo e da Audin, a percepção de servidores, entre outros.

Com o entendimento de que os resultados da implementação e avaliação podem impactar a estrutura e a metodologia de gestão de riscos da Audin, é prevista uma revisão anual desses componentes, a fim de promover melhorias. Porém, mudanças no contexto do Inep também podem provocar a necessidade de atualizações de forma antecipada.

3.1 Competências

O artigo 23 da PGIRC determina que todos os agentes públicos em exercício no Inep, em todos os níveis e unidades, são responsáveis pela gestão dos riscos inerentes ao exercício de suas atribuições, bem como pelo monitoramento da evolução dos níveis de riscos e da efetividade das medidas de controles implementadas nos processos organizacionais em que estiverem envolvidos ou de que tiverem conhecimento, devendo exercer as atividades de sua competência em estrita consonância com os princípios e objetivos dispostos no capítulo IV da Portaria n° 565. Nesse contexto, compete à Audin a gestão dos riscos inerentes às suas atividades.

Segundo o artigo 20 da PGIRC, as atribuições relativas à governança, gestão de riscos e integridade são de competência do Comitê de Governança Institucional (CGI), sendo que, conforme as atribuições previstas no inciso VIII do artigo 9º do anexo I do Decreto nº 11.204, de 21 de setembro de 2022, compete à Assessoria de Governança e Gestão Estratégica (AGGE) promover a capacitação contínua e o compartilhamento de melhores práticas de governança, de gestão estratégica, de integridade, de gerenciamento de riscos, de ética e de controle.

O gestor de riscos na Audin é o assistente técnico, responsável por todas as etapas do processo de gestão de riscos.

3.2 Integração aos processos organizacionais da Audin

No intuito de melhor gerenciar os riscos da Audin, entende-se como necessário trabalhar de forma detalhada a gestão de processos. Por esse motivo, primeiro será realizado o mapeamento de processos e, posteriormente, o gerenciamento de riscos.

Assim, o gerenciamento de riscos irá acontecer de forma sucedânea ou concomitante ao mapeamento de processos, sendo a estratégia adotada até que todos os processos tenham sido gerenciados, momento em que a Audin deverá adotar critérios de priorização próprios para a seleção dos processos que, anualmente, serão cobertos pela gestão de riscos. Essa metodologia deverá ser atualizada na ocasião, de forma a incluir tais critérios.

De forma geral, visualizam-se as seguintes melhorias: entendimento das etapas, dos fluxos dos processos e do papel dos atores responsáveis; otimização das etapas dos processos; dimensionamento do custo operacional (horas-homem) e temporal dos processos; e automação de partes dos processos.

3.3 Recursos

O auditor-chefe deve designar equipe para participar das etapas do processo de gerenciamento de riscos. Essa equipe deve ser composta por servidores que conheçam o processo, seus objetivos, contextos, atores envolvidos, resultados e controles já existentes.

Além disso, é importante a participação de servidores com conhecimento acerca da Metodologia de Gestão de Riscos da Audin. O auditor-chefe irá apoiar, sempre que possível, o processo através do direcionamento de capacitações e participação ativa no trabalho.

3.4 Comunicação

A comunicação sobre o processo de gerenciamento de riscos e seus resultados deve ser conduzida de maneira formal, por meio de relatórios anuais ao CGI e ao presidente do Inep. As demais comunicações sobre a gestão de riscos serão realizadas através da elaboração de banners e materiais impressos, publicações na intranet, painéis gerenciais (Business Intelligence) etc.

4 Metodologia de Gestão de Riscos

A Metodologia de Gestão de Riscos objetiva estabelecer e estruturar as etapas necessárias para a operacionalização da gestão de riscos na Audin, por meio da definição de um processo de gerenciamento de riscos. Segundo o artigo 13 da PGIRC, a operacionalização da gestão de riscos deverá contemplar, no mínimo, as seguintes etapas:

> I – estabelecimento do contexto: etapa em que são identificados os objetivos relacionados ao processo organizacional e definidos os contextos externo e interno a serem levados em consideração ao gerenciar riscos;
>
> II – identificação de riscos: etapa em que são identificados possíveis riscos para objetivos associados aos processos organizacionais;
>
> III – análise de riscos: etapa em que são identificadas as possíveis causas e consequências do risco;
>
> IV – avaliação de riscos: etapa em que são estimados os níveis dos riscos identificados;
>
> V – priorização de riscos: etapa em que são definidos quais riscos terão suas respostas priorizadas, levando em consideração os níveis calculados na etapa anterior;
>
> VI – tratamento dos riscos: etapa em que são definidas as respostas aos riscos, de forma a adequar seus níveis ao apetite estabelecido para os processos organizacionais, além da escolha das medidas de controle associadas a essas respostas; e

> VII – comunicação e monitoramento: etapa que ocorre durante todo o processo de gerenciamento de riscos e é responsável pela integração de todas as instâncias envolvidas, bem como pelo monitoramento contínuo da própria Gestão de Riscos, com vistas a sua melhoria. (Brasil. Inep, 2022).

A Metodologia de Gestão de Riscos da Audin é orientada ao processo organizacional e obedece a um modelo de aplicação integrado à gestão de processos.

Assim, a metodologia utilizou como referenciais técnicos os manuais de gestão de riscos da Controladoria-Geral da União (CGU) e do Tribunal de Contas da União (TCU). O ciclo de gestão de riscos adotado pela Audin é o utilizado pela CGU, como segue:

FIGURA 1

CICLO DA METODOLOGIA DE GESTÃO DE RISCOS DA AUDIN

Fonte: *Metodologia de Gestão de Riscos* (Brasil. CGU, 2021).

A gestão de riscos é multidisciplinar, motivo pelo qual o trabalho ganha qualidade quando desenvolvido de forma coletiva, com o envolvimento e participação de pessoas que conhecem o processo priorizado.

As informações produzidas durante o ciclo apresentado na Figura 1 devem ser registradas na Matriz de Riscos, conforme modelo disponível na base de conhecimento da Audin no Sistema Eletrônico de Informações (SEI). As bases da matriz devem ser mantidas sempre atualizadas e serão utilizadas para viabilizar o painel de gerenciamento de riscos da Audin.

4.1 Plano de gerenciamento de riscos (ordem de serviço)

Entende-se por Plano de Gestão de Riscos todo o planejamento e trabalho necessários que antecedem a execução das etapas de gerenciamento de riscos. Para ter êxito nas etapas posteriores, é necessário que, nessa etapa, definam-se os seguintes pontos:

- Processos a serem gerenciados;
- Grupo de Gerenciamento de Riscos (GGR);
- Atividades e produtos a serem desenvolvidos;
- Cronograma de trabalho.

4.2 Entendimento do contexto

O processo priorizado é estudado e analisado levando-se em consideração o ambiente interno e externo da Audin. Quanto maior a amplitude e profundidade empreendida no entendimento do contexto, maior a chance de se identificar riscos relevantes e aumentar a exatidão na avaliação da probabilidade de impacto. Minimamente, as seguintes informações precisam ser consideradas:

- Objetivos ou resultados do processo;
- Fluxos de trabalho relevantes para o alcance dos objetivos/resultados;
- Papéis e responsabilidades das pessoas envolvidas;
- Principais fatores internos e externos que podem afetar o alcance dos objetivos/resultados (pessoas, sistemas informatizados, estruturas organizacionais, legislação, recursos, stakeholders etc.).

4.3 Identificação de riscos

A identificação de riscos consiste na atividade sistemática de encontrar, reconhecer e descrever os riscos que podem afetar a capacidade de uma área ou organização atingir seus objetivos. Uma cobertura abrangente e precisa dos possíveis riscos é fundamental para poder avaliá-los e desenvolver estratégias de resposta eficazes.

Considerando o resultado da etapa de entendimento do contexto, o fluxo do processo organizacional, a partir da experiência da equipe técnica designada, deve apresentar uma lista abrangente de eventos (riscos) que podem evitar, atrasar, prejudicar ou impedir o cumprimento dos objetivos do processo organizacional ou das suas etapas críticas.

De acordo com Brasil. CGU (2021, p. 23), algumas questões podem ser levantadas a fim de identificar os riscos de uma unidade. Como preceitua o Manual, as perguntas podem ser:

- Quais eventos podem EVITAR o atingimento de um ou mais objetivos do processo organizacional?
- Quais eventos podem ATRASAR o atingimento de um ou mais objetivos do processo organizacional?
- Quais eventos podem PREJUDICAR o atingimento de um ou mais objetivos do processo organizacional?

- Quais eventos podem IMPEDIR o atingimento de um ou mais objetivos do processo organizacional?
- Os eventos identificados inicialmente podem ser analisados e revisados, reorganizados, reformulados e até eliminados nesta etapa.
- *Dica*: Os problemas do passado podem muitas vezes serem vistos como possíveis riscos futuros. Portanto, sugere-se iniciar a lista de riscos a partir desses problemas.

Ainda, o documento supracitado indica que aqueles eventos identificados e analisados como riscos do processo devem indicar:

- Objetivo do processo/subprocesso impactado pelo risco;
- Categoria do risco, entre as definidas para a Audin:
    - Operacional: eventos que podem comprometer as atividades da Audin, normalmente associados a falhas, deficiência ou inadequação de processos internos, pessoas, infraestrutura e sistemas;
    - Legal: eventos derivados de alterações legislativas ou normativas que podem comprometer as atividades da [Audin];
    - Financeiro/orçamentário: eventos que podem comprometer a capacidade da [Audin] de contar com os recursos orçamentários e financeiros necessários à realização de suas atividades, ou eventos que possam comprometer a própria execução orçamentária, como atrasos no cronograma de licitações;
    - Integridade: eventos relacionados a corrupção, fraudes, irregularidades e/ou desvios éticos e de conduta que podem comprometer os valores e padrões preconizados pela [Audin] e a realização dos objetivos. (Brasil. CGU, 2021, p. 23).

Nesse contexto, há também os riscos estratégicos – aqueles eventos que podem afetar os aspectos estratégicos da unidade, impactando no atingimento dos objetivos e resultados definidos no plano de negócio – além do risco de imagem voltado diretamente à reputação da unidade. Outro fator preponderante é a causa que leva à ocorrência desses riscos.

Para isso, a Metodologia da CGU indica que para identificação das causas é importante realizar uma análise das diversas fontes de riscos existentes no processo, tais como:

- Processos: decorrente de diretrizes estratégicas e da formalização/modelagem de processos, incluídos os métodos, procedimentos e regulamentações de planejamento, execução, controle e monitoramento. Os mecanismos de comunicação e repositório de conhecimento também se enquadram nesta fonte.
- Pessoas: decorrente de operações humanas, em que são requeridas condutas apropriadas, competências, conhecimentos e habilidades.
- Externa: decorrente do ambiente externo à organização, como desastres naturais, conjuntura político-econômica e imprevisibilidade de fornecedores.
- Infraestrutura: decorrente dos recursos de infraestrutura física ou lógica (sistemas de TI) da organização.
- Recursos humanos ou financeiros: decorrente da disponibilidade de recursos humanos ou financeiros.

Deve-se considerar, também, aspectos relacionados à utilização de tecnologias ultrapassadas e/ou produtos obsoletos, que podem ser um reflexo da falta de investimento em tecnologia da informação. Dessa forma, as consequências desses processos podem ser compreendidas em virtude do resultado da ocorrência do risco, que afeta diretamente o objetivo do processo.

4.4 Identificação e avaliação dos controles

Após a identificação dos riscos, causas e consequências, é necessário identificar quais controles estão presentes no processo para mitigar os riscos identificados. Essa avaliação é importante para evitar replicação de esforços e avaliar se os controles existentes são necessários e suficientes para manter os riscos dentro do nível de tolerância estabelecido.

De acordo com Brasil. CGU (2021, p. 24), os controles devem ser classificados em:

- Controles preventivos: controles existentes e que atuam sobre as possíveis causas do risco, com o objetivo de prevenir a sua ocorrência. Exemplos de controles preventivos: requisitos/checklist definidos para o processo e capacitação dos servidores envolvidos no processo.
- Controles de atenuação e recuperação: controles existentes executados após a ocorrência do risco, com o intuito de diminuir o impacto de suas consequências. Exemplos de controles de atenuação e recuperação: plano de contingência; tomada de contas especiais; procedimento apuratório.
- Controles detectivos: controles existentes que atuam na detecção da materialização de um risco ou de sua iminência. Exemplos de controles de detecção: indicadores; termômetros; sensores.

É necessário realizar um estudo mais aprofundado dos mecanismos de controle adotados no processo, com a finalidade de identificar controles ineficazes e/ou ineficientes. Para isso, Brasil. CGU (2021) recomenda que algumas perguntas sejam respondidas:

1– Os controles presentes no processo/subprocesso estão associados aos riscos identificados?

Essa pergunta ajudará tanto na identificação de outros controles quanto na de outros possíveis riscos. Além disso, caso seja identificado controle ao qual a equipe técnica não consiga identificar um risco associado, é possível que tal controle seja uma burocracia excessiva.

2 – Os controles identificados são eficazes, ou seja, eles reduzem o risco inerente ao nível desejado? Caso a resposta seja negativa, é possível corrigir esses controles de forma a torná-los eficazes?

Essa pergunta ajudará a avaliar os controles existentes no processo. As informações aqui obtidas deverão ser utilizadas na construção do Plano de Tratamento de forma a otimizar os controles presentes, seja excluindo ou corrigindo os controles ineficazes.

3 – O custo financeiro e/ou operacional de cada um dos controles identificados se justifica perante os riscos mitigados?

Essa pergunta ajudará a identificar controles que, apesar de mitigarem riscos, apresentam um custo financeiro e/ou operacional aquém do ideal, ou seja, não são eficientes. Os controles identificados nessa pergunta são fortes candidatos a serem substituídos por controles mais otimizados. O resultado dessa pergunta também será utilizado na construção do Plano de Tratamento dos Riscos.

> É importante que seja feita uma associação entre os controles preventivos detectados e suas respectivas causas, assim como uma associação entre os controles de atenuação e recuperação e suas respectivas consequências. Essa associação será importante para a geração de relatórios gerenciais e alimentação do painel de riscos. (Brasil. CGU, 2021, p. 25).

4.5 Cálculo do nível de risco

Nesta etapa, também conhecida como análise dos riscos, busca-se desenvolver uma compreensão sobre a probabilidade de ocorrência e o impacto causado ao processo, se o evento incerto se concretizar. Esses parâmetros definem o nível de risco, que será utilizado posteriormente na priorização dos riscos para tratamento com base no apetite e na tolerância ao risco estabelecidos.

O cálculo do nível de risco levará em consideração as escalas qualitativas de probabilidade e o impacto apresentadas nos Quadros 1 e 2, respectivamente, que foram extraídas do *Manual de gestão de riscos do TCU*.

QUADRO 1

ESCALA DE PROBABILIDADE

Probabilidade	Descrição da probabilidade
Raro	Acontece apenas em situações excepcionais. Não há histórico conhecido do evento ou não há indícios que sinalizem sua ocorrência.
Pouco provável	O histórico conhecido aponta para baixa frequência de ocorrência no prazo associado ao objetivo.
Provável	Repete-se com frequência razoável no prazo associado ao objetivo ou há indícios que possa ocorrer nesse horizonte.
Muito provável	Repete-se com elevada frequência no prazo associado ao objetivo ou há muitos indícios que ocorrerá nesse horizonte.
Praticamente certo	Ocorrência quase garantida no prazo associado ao objetivo.

Fonte: Elaborado pela Audin/Inep com base no *Manual de gestão de riscos do TCU* (Brasil. TCU, 2020).

QUADRO 2

ESCALA DE IMPACTO

Impacto	Descrição do impacto nos objetivos, caso o evento ocorra
Muito baixo	Compromete minimamente o atingimento do objetivo; para fins práticos, não altera o alcance do objetivo/resultado.
Baixo	Compromete em alguma medida o alcance do objetivo, mas não impede o alcance da maior parte do objetivo/resultado.
Médio	Compromete razoavelmente o alcance do objetivo/resultado.
Alto	Compromete a maior parte do atingimento do objetivo/resultado.
Muito alto	Compromete totalmente ou quase totalmente o atingimento do objetivo/resultado.

Fonte: Elaborado pela Audin/Inep com base no Manual de gestão de riscos do TCU (Brasil. TCU, 2020).

O nível de risco adotado difere do usualmente utilizado, que é calculado pelo produto de probabilidade e impacto. Optou-se por utilizar a matriz proposta pelo TCU, cujo nível de risco é dado pelo número inscrito em cada célula da matriz, que não é obtido por meio de fórmula matemática. São 25 possíveis níveis de risco, em que cada nível está associado a uma estimativa de probabilidade e de impacto. Dessa forma, o impacto considerado mais importante do que a probabilidade. Um evento de impacto muito alto e de probabilidade de ocorrência muito baixa requer maior atenção do que o oposto, um evento de probabilidade muito alta e impacto muito baixo. As matrizes simétricas, que utilizam o produto da pontuação "probabilidade x impacto", consideram como do mesmo nível os riscos desse exemplo.

QUADRO 3

MATRIZ DE RISCOS

IMPACTO	**Muito alto**	15	19	22	24	25
	Alto	10	14	18	21	23
	Médio	6	9	13	17	20
	Baixo	3	5	8	12	16
	Muito Baixo	1	2	4	7	11
		Raro	**Pouco provável**	**Provável**	**Muito provável**	**Praticamente certo**
		PROBABILIDADE				

Fonte: Adaptação do Manual de gestão de riscos do TCU (Brasil. TCU, 2020, p. 27).

Os riscos cujos níveis de exposição estiverem posicionados nas células em vermelho do Quadro 3 são considerados críticos (alto risco), das células amarelas são riscos de importância mediana e, nas células verdes, estão localizados os riscos de baixa relevância.

Na definição do nível de risco, devem ser considerados os controles existentes, de forma a refletir a probabilidade e impacto atual do risco.

4.6 Respostas aos riscos

Nesta etapa, devem ser considerados os valores dos níveis de riscos residuais (riscos reais) calculados na etapa anterior para a priorização dos riscos e otimização das ações de tratamento.

A faixa de classificação do risco deve ser considerada para a definição da atitude da Audin em relação à priorização para tratamento.

Segundo o inciso II do artigo 6º da PGIRC, apetite a risco é "nível de risco que a unidade está disposta a aceitar". É importante que o apetite a risco do processo seja estabelecido no início do gerenciamento de riscos. O Quadro 4 mostra, por classificação, quais ações devem ser adotadas em relação ao risco.

QUADRO 4

ATITUDE PERANTE O RISCO, PARA CADA CLASSIFICAÇÃO

Classificação	Ação necessária
Risco Baixo (verde)	Nível de risco dentro do apetite a risco, não exigem medidas de tratamento. Se já existir algum controle implementado, avaliar o custo x benefício de se manter.
Risco Médio (amarelo)	Nível de risco dentro do apetite a risco. Geralmente nenhuma medida especial é necessária, porém requer atividades de monitoramento específicas e atenção da Audin nos controles existentes para manter o risco nesse nível.
Risco Alto (vermelho)	Nível de risco acima do apetite a risco. Qualquer risco nesse nível requer atenção especial do auditor-chefe. Deve ser tratado por meio de controles eficazes e eficientes e mantido sob monitoramento constante.

Fonte: Adaptação de Brasil. TCU (2018).

Para cada evento incerto cujo nível de risco esteja acima do apetite a risco da Audin, deve ser adotada uma ou mais medidas de tratamento, conforme Quadro 5, para reduzir a probabilidade ou impacto.

As medidas de tratamento podem incidir sobre as causas (probabilidade) ou consequências (impacto). Para tratar as causas, são identificadas as medidas preventivas que possam minimizar ou evitar a ocorrência do evento indesejado. Da mesma forma, deve-se identificar ações que podem ser implementadas para atenuar os efeitos negativos que eventualmente um risco pode causar ao processo, impedindo-o de alcançar seus objetivos.

QUADRO 5

MEDIDAS DE TRATAMENTO DO RISCO

Medida de Tratamento	Descrição
Mitigar	As medidas mitigadoras consistem na adoção de controles, como o redesenho de processos, a realocação de pessoas, a realização de ações de capacitação, o desenvolvimento ou aperfeiçoamento de soluções de TI, a adequação da estrutura organizacional, a elaboração de um normativo, entre outros.
Compartilhar	Um risco normalmente é compartilhado quando a implementação de controles não apresenta uma relação custo x benefício adequada. Na Audin, pode-se compartilhar o risco por meio de contratação de terceiros, auditorias compartilhadas, entre outras medidas.
Evitar	Um risco normalmente é evitado quando a implementação de controles não apresenta relação custo x benefício adequada ou não há formas de compartilhar o risco. Na Audin, evitar o risco pode significar a não realização de trabalhos cuja complexidade ou amplitude superem a capacidade da Audin, tanto em termos de competências técnicas quanto disponibilidade de força de trabalho.
Aceitar	Um risco normalmente é aceito quando seu nível está nas faixas de apetite a risco (baixo ou médio). Nessa situação, nenhum novo controle precisa ser implementado para mitigar o risco.

Fonte: Adaptação de Brasil. CGU (2021).

O Plano de Ação do ponto de vista do gerenciamento de riscos é um plano para a implementação das medidas de tratamento. Por isso, deve conter, pelo menos:

- Medida(s) de tratamento contemplada(s) e o risco relacionado que deseja tratar;
- Objetivos/benefícios esperados por medida de tratamento;
- Responsável pela implementação;
- Breve descrição sobre a implementação;
- Custo estimado para implementação;
- Data prevista para início da implementação;
- Data prevista para o término da implementação.

É importante que, em uma primeira abordagem da elaboração do Plano de Ação, avalie-se a necessidade de melhorar ou extinguir controles já existentes, utilizando os resultados da etapa "Identificação e avaliação dos controles". Somente depois dessa avaliação, e se ainda identificada a necessidade de redução do nível do risco, podem ser propostos novos controles, observados sempre critérios de eficiência e eficácia da sua implementação.

O plano de ação para a implementação das medidas de tratamento dos riscos deve ser considerado na elaboração do Plano Anual de Auditoria Interna (Paint), a fim de reservar capacidade operacional para a realização das ações necessárias.

4.6 Validação dos resultados

Os resultados das etapas anteriores devem ser apresentados à equipe da Audin em oficinas, para compartilhar as informações produzidas e coletar contribuições. A Matriz de Riscos e o Plano de Ação devem ser aprovados pelo auditor-chefe e comunicados ao CGI e ao presidente do Inep.

4.7 Comunicação e monitoramento

Segundo a ISO 31000:2018, durante todas as etapas do processo de gerenciamento de riscos, é importante comunicar-se com as partes interessadas.

Além da comunicação já apresentada nas etapas anteriores, após elaboração do Plano de Ação, o auditor-chefe irá monitorar sua implementação por meio de painéis gerenciais, que também serão utilizados para monitorar os riscos que não demandam medidas de mitigação.

Especificamente sobre os processos Planejamento Anual Baseado em Riscos, realização de Auditoria Baseada em Riscos e Monitoramento das Recomendações da Auditoria Interna, ao final de cada ciclo, os responsáveis por esses processos devem responder um questionário sobre questões relacionadas aos respectivos riscos, de forma a promover a retroalimentação do gerenciamento de riscos. Ou seja, essas informações serão utilizadas para atualizar a Matriz de Riscos.

O auditor-chefe fará relatórios anuais às instâncias de governança com as informações sobre o gerenciamento de riscos da Audin, por meio do Relatório Anual de Atividades de Auditoria Interna (Raint).

4.8 Ciclo de reavaliação

A qualquer tempo, o auditor-chefe pode decidir por reavaliar a parte ou o todo do processo organizacional, bem como executar a metodologia completa ou em apenas algumas etapas.

Além disso, os responsáveis pelo processo sob gerenciamento de riscos, quando observarem alguma mudança no contexto ou evento que sinalize a necessidade de atualizar os riscos, devem reportar ao auditor-chefe. O gestor de riscos da Audin deve reportar eventuais necessidades de atualização dos riscos, a qualquer tempo, ao auditor-chefe.

5 REFERÊNCIAS BIBLIOGRÁFICAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). *NBR ISO 3100*: gestão de riscos: princípio e diretrizes. Rio de Janeiro, RJ: ABNT, 2009.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). *NBR ISO /IEC 31010*: gestão de riscos: técnicas para o processo de avaliação de riscos. Rio de Janeiro, RJ: ABNT, 2012.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). *NBR ISO 3100*: gestão de riscos: princípio e diretrizes. 2. ed. Rio de Janeiro, RJ: ABNT, 2018.

BRASIL. Decreto nº 11.204, de 21 de setembro de 2022. Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança do Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira e remaneja e transforma cargos em comissão e funções de confiança. *Diário Oficial da União*, Brasília, DF, 22 set. 2022. Seção 1, p. 16.

BRASIL. Controladoria-Geral da União (CGU). *Metodologia de gestão de riscos*: [versão 2.0]. Brasília, DF: CGU, 2021.

BRASIL. Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira (Inep). Planejamento estratégico Institucional 2020-2023: versão 7ª RAE. Brasília, DF: Inep, 2022a.

BRASIL. Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira (Inep). *Portaria nº 565, de 28 de dezembro de 2022*. Institui a Política de Governança, Integridade, Riscos e Controles Internos do Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira. Brasília, DF, 2022.

BRASIL. Ministério do Planejamento, Orçamento e Gestão (MPOG); BRASIL. Controladoria-Geral da União (CGU). 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. *Diário Oficial da União*, Brasília, DF, 11 maio 2016. Seção 1, p. 14.

BRASIL. Tribunal de Contas da União (TCU). *Gestão de riscos*: avaliação da maturidade. Brasília, DF: CGU, 2018.

BRASIL. Tribunal de Contas da União (TCU). *Manual de gestão de riscos do TCU*. 2. ed. Brasília, DF: TCU, 2020.

COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION (COSO). *Gerenciamento de riscos corporativos*: integrado com estratégia e performance: sumário executivo. . [S. l.], 2017.

THE INSTITUTE OF INTERNAL AUDITORS (IIA). *Declaração de posicionamento do IIA*: as três linhas de defesa no gerenciamento eficaz de riscos e controles. Lake Mary, FL: IIA, 2013.

THE INSTITUTE OF INTERNAL AUDITORS (IIA). *Modelo das 3 três linhas do IIA 2020*: uma atualização das três linhas de defesa. Lake Mary, FL: IIA, 2020.

SOUZA, K.; BRASIL, F. *Como gerenciar riscos na Administração Pública*: estudo prático em licitações. Curitiba, PR: Editora Negócios Públicos, 2017.

INEP
MINISTÉRIO DA EDUCAÇÃO