

DIÁRIO OFICIAL DA UNIÃO

Publicado em: 26/12/2023 | Edição: 244 | Seção: 1 | Página: 25

Órgão: Ministério da Cultura/Fundação Cultural Palmares

Comitê Interno de Governança

RESOLUÇÃO FCP Nº 18, DE 22 DE DEZEMBRO DE 2023

O PRESIDENTE DO COMITÊ INTERNO DE GOVERNANÇA DA FUNDAÇÃO CULTURAL PALMARES, no uso das atribuições que lhe confere o art. 1º, XIII, da Portaria nº 64, de 24 de março de 2020, Resolução CIGFCP nº 07, de 12 de agosto de 2021 e o deliberado na 3ª Reunião Ordinária do dia 20 de dezembro de 2023, resolve:

Art. 1º Aprovar a Metodologia de Gestão de Riscos da Fundação Cultural Palmares da Fundação Cultural Palmares, na forma do Anexo desta Resolução.

Art. 2º Esta Resolução entra em vigor em 02 de janeiro de 2024.

JOÃO JORGE SANTOS RODRIGUES

ANEXO

METODOLOGIA DE GESTÃO DE RISCOS DA FUNDAÇÃO CULTURAL PALMARES

1. INTRODUÇÃO

Este documento apresenta a metodologia de gestão de riscos da Fundação Cultural Palmares - FCP, em conformidade com a Portaria nº 64, de 24 de março de 2020, que cria o Comitê Interno de Governança da entidade, pautada com as diretrizes dispostas na Resolução CIGFCP nº 07, de 12 de agosto de 2021, que aprova a Política de Gestão de Riscos, e em observância as demais normas que regem a matéria.

A metodologia abrange a definição de conceitos, diretrizes, atribuição de papéis e responsabilidades dos gestores, o detalhamento do processo de gerenciamento de riscos, a definição da Matriz de Riscos e o apetite a risco da FCP. Também, tem por parâmetro a ABNT NBR ISO 31000:2018, por se tratar de um normativo padrão internacional que fornece princípios e diretrizes genéricas, contudo, possibilita que seja adaptado a especificidade de cada organização.

A metodologia implementada pela FCP permitirá gerar um fluxo ordenado de ações de modo a avaliar, identificar, analisar, tratar, monitorar e comunicar os riscos da entidade. Quando efetivada e mantida de acordo com as diretrizes estabelecidas nesta norma será mais um mecanismo de controle de prevenção e proteção para o alcance dos objetivos da entidade.

O processo de gerenciamento de riscos de maneira estrita, consiste nas seguintes etapas (ISO 31000:2018): a) estabelecimento do contexto; b) identificação de riscos; c) análise de riscos em impacto e probabilidade; d) avaliação de riscos em categorias (pequeno, moderado, alto e crítico); e) tratamento de riscos; f) comunicação e consulta; g) monitoramento e análise crítica; e h) registro e relato. Em que pese se tenham essas fases, na prática o processo é iterativo e incremental, isto é, realizado em fases de revisão onde agrega-se e refina-se as informações de forma contínua a cada ciclo.

Para o gerenciamento dos riscos é necessário o mapeamento dos processos como etapa prévia, uma vez que é nessa etapa que são estudadas as entradas, as saídas, os fornecedores e os clientes do processo (Análise SIPOC), bem como o fluxograma do processo.

A metodologia foi elaborada pela equipe da Coordenação-Geral de Gestão Estratégica e posteriormente foi aprovada no âmbito do Comitê Interno de Governança da Fundação Cultural Palmares, por meio da Reunião Ordinária/Extraordinária de XXX.

O gerenciamento de riscos será executado pelas unidades administrativas da FCP, de forma integrada aos processos oriundos das competências regimentais e do planejamento estratégico, levando em consideração a cultura organizacional da entidade, abrangendo os níveis estratégico, tático e operacional.



2. FUNDAMENTO LEGAL

a) Lei n.º 7.668, de 22 de agosto de 1988, que autoriza o Poder Executivo a constituir a Fundação Cultural Palmares - FCP e dá outras providências.

b) Decreto n.º 11.203, de 21 de setembro de 2022, que aprova o Estatuto e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança da Fundação Cultural Palmares e remaneja e transforma cargos em comissão e funções de confiança.

c) Instrução Normativa Conjunta MPOG e CGU n.º 1, de 10 de maio de 2016 - Dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo Federal;

d) Decreto n.º 9.203, de 22 de novembro de 2017 - Dispõe sobre a política de governança da administração pública federal direta, autárquica e fundacional;

e) Portaria FCP n.º 64, 24 de março de 2020 - Institui o Comitê Interno de Governança da FCP, alterada pelas Portarias n.º 104, de 29 de maio de 2020 e n.º 71, de 09 de março de 2021; e

f) Resolução CIGFCP n.º 07, de 12 de agosto de 2021, aprova a Política de Gestão de Riscos da Fundação Cultural Palmares.

3. CONCEITOS

Para fins deste documento, consideram-se os seguintes conceitos:

accountability: conjunto de procedimentos adotados pelas organizações públicas e pelos indivíduos que as integram, os quais evidenciam sua responsabilidade por decisões tomadas e ações implementadas, incluindo a salvaguarda de recursos públicos, a imparcialidade e o desempenho das organizações;

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

agente responsável pela gestão de riscos: servidor, funcionário, empregado ou colaborador em exercício na FCP que atue na Gestão de Risco dos processos organizacionais sob sua responsabilidade;

Coordenação-Geral de Gestão Estratégica - CGE: unidade que tem a finalidade de orientar, sistematizar e padronizar a identificação, a avaliação e a adoção de controles (respostas aos eventos de riscos) dos processos das unidades administrativas da FCP. Também tem a responsabilidade de acompanhar a evolução e melhorias do Programa de Integridade da Fundação;

controles internos da gestão: conjunto de regras, procedimentos, diretrizes, protocolos, rotinas de sistemas informatizados, conferências e trâmites de documentos e informações, entre outros, operacionalizados de forma integrada pela direção e pelo corpo de servidores das organizações, destinados a enfrentar os riscos e fornecer segurança razoável e suficiente para o alcance dos objetivos estratégicos. Também visa:

a) execução ordenada, ética, econômica, eficiente e eficaz das operações;

b) cumprimento das obrigações de accountability;

c) cumprimento das leis e regulamentos aplicáveis; e

d) salvaguarda dos recursos para evitar perdas, mau uso e danos.

evento: um ou mais incidentes ou ocorrências, provenientes dos ambientes interno ou externo, ou mudança em um conjunto específico de circunstâncias, podendo também consistir em algo não acontecer;

gestão de riscos: processo de natureza permanente, estabelecido, direcionado e monitorado pela alta administração, que contempla as atividades de identificar, avaliar e gerenciar potenciais eventos que possam afetar a entidade, destinado a fornecer segurança razoável quanto à realização de seus objetivos;

gestor de risco e controle: agente responsável pelo gerenciamento do risco no âmbito de suas unidades organizacionais, quer seja o coordenador geral, diretor ou cargo equivalente, quer seja o agente operacional a frente da execução do processo;



governança pública: conjunto de mecanismos de liderança, estratégia e controle postos em prática para avaliar, direcionar e monitorar a atuação da gestão, com vistas à condução de políticas públicas e à prestação de serviços de interesse da sociedade;

matriz de risco: ferramenta para classificar e apresentar riscos definindo faixas para impacto e probabilidade;

medida de controle: medida aplicada, no âmbito da FCP, para mitigar ou eliminar os riscos e aumentar a probabilidade de que os objetivos e as metas organizacionais sejam alcançados;

nível do risco: medida da importância ou significância do risco, considerando a probabilidade de ocorrência do evento e o seu impacto;

objeto de gestão de riscos: qualquer processo de trabalho, atividade, projeto ou ação de plano institucional, assim como os recursos que dão suporte para a efetivação dessas iniciativas e para o alcance dos objetivos estratégicos da FCP;

planejamento estratégico: O planejamento estratégico consiste em um processo de reflexão, análise e tomada de decisão acerca dos grandes objetivos de uma organização e dos meios que serão utilizados para alcançá-los. Por meio dele, a instituição desenvolve autoconhecimento e promove uma orientação estratégica comum para todos os seus colaboradores, com a definição da sua Missão (razão de existir), sua Visão (projeção bem-sucedida da organização no futuro) e seus Valores (princípios mais relevantes que devem permear sua atuação).

política de gestão de riscos: declaração das intenções e diretrizes gerais de uma organização relacionadas à Gestão de Riscos;

processo: conjunto de ações e atividades interrelacionadas, que são executadas para alcançar produto, resultado ou serviço predefinido;

risco: possibilidade de que um evento afete o alcance de objetivos estratégicos;

riscos institucionais: riscos priorizados e elencados para serem monitorados pela alta administração;

risco inerente: risco a que a entidade está exposta sem considerar quaisquer ações de controle que possam reduzir a probabilidade de sua ocorrência ou seu impacto;

risco residual: risco a que a entidade está exposta após a implementação de controles para o tratamento do risco; e

tolerância ao risco: disposição da organização ou parte interessada em suportar o risco após o tratamento do risco a fim de atingir seus objetivos. Pode ser influenciada por requisitos legais ou regulatórios.

tratamento dos riscos: permitir a construção do Plano de Implantação das Ações de Controle dos Riscos (ou Plano de Ação). Trata-se de um documento que organiza as atividades a serem realizadas para a adequada implantação dos controles previstos na Matriz de Riscos. Busca-se estabelecer o tratamento dos riscos, por meio de ações de caráter imediato, curto, médio ou longo prazo, ou de aperfeiçoamento contínuo.

4. PRINCÍPIOS

Em conformidade com a Política de Gestão de Riscos da CGE, e de acordo com a norma ABNT NBR ISO 31.000: 2018, constituem princípios da gestão de riscos:

I - proteção do ambiente organizacional;

II - melhoria contínua dos processos da organização;

III - visão sistêmica, estruturada e oportuna, subordinada ao interesse público;

IV - qualidade e tempestividade das informações;

V - transparência;

VI - uniformidade de procedimentos;

VII - dinamismo e interatividade;



VIII - alinhamento à gestão estratégica;

IX - estabelecimento de procedimentos de controle interno proporcionais ao risco observada a relação custo-benefício, e destinados a agregar valor à organização;

X - estabelecimento de níveis de exposição a riscos adequados; e

XI - utilização do mapeamento de riscos para o apoio à tomada de decisão e à elaboração do planejamento estratégico.

5. OBJETIVOS

A Metodologia é uma ferramenta capaz de auxiliar os gestores públicos no processo de tomada de decisão, a fim de assegurar a devida aplicação dos recursos públicos e, conseqüentemente, a efetividade das políticas públicas. Seus objetivos são:

I - aumentar a probabilidade de alcance dos objetivos institucionais, reduzindo riscos a níveis aceitáveis;

II - apoiar a tomada de decisão dos gestores, com informações tempestivas e suficientes a respeito dos riscos a que a organização está exposta;

III - promover uma gestão proativa;

IV - melhorar a eficácia e a eficiência operacional;

V - melhorar a governança; e

VI - agregar valor à organização por meio da melhoria dos processos de tomada de decisão e do tratamento adequado dos riscos dos impactos negativos decorrentes de sua materialização

6. RESPONSABILIDADE

Para melhor compreensão das responsabilidades em gestão de riscos da FCP, propõe-se o Modelo de Três Linhas de Defesa, do IIA - The Institute of Internal Auditors (2020) (Figura 1), o qual apresenta de forma simples e eficaz papéis e responsabilidades essenciais e suas competências. No entanto, competências específicas estão discriminadas na Resolução nº 7 de 2021 que aprova a Política de Gestão de Riscos da Fundação Cultural Palmares.



Nessa estrutura em que todos têm alguma responsabilidade, atuam como elementos centrais: (i) os gestores dos riscos, (ii) os especialistas em controles internos, gestão de riscos e conformidade, (iii) os auditores internos e os órgãos de governança.

O modelo envolve pessoas e setores diversos, formando uma estrutura clara, com transparência na comunicação e na distribuição de funções, conforme detalhamento a seguir:

a) Primeira Linha: são os gestores em seus respectivos âmbitos e escopos de atuação, os responsáveis pelos processos de trabalho, projetos, atividades e ações desenvolvidos nos níveis estratégicos, táticos ou operacionais. Compete aos gestores como Primeira Linha:

I - Escolher os processos, projetos, atividades e ações que terão seus riscos gerenciados e tratados, observada a Política de Gestão de Riscos;

II - Definir os níveis de risco aceitáveis e elaborar os planos de ação para o tratamento dos riscos, considerando a declaração de apetite a riscos do órgão;

III - Realizar o acompanhamento da evolução dos níveis de risco e da efetividade dos planos de ação;

b) Segunda Linha: composta pelos responsáveis pelo controle interno, gestão de riscos e conformidade da organização, que têm como objetivo apoiar os gestores dos riscos para que cumpram com suas responsabilidades de Primeira Linha, fornecendo conhecimento e ferramentas adequadas. Compete aos responsáveis pelo controle interno, gestão de riscos e conformidade da organização, como Segunda Linha:

I - Apoiar a Primeira Linha na implantação, monitoramento e melhoria dos controles internos estabelecidos na gestão de riscos;

II - Monitorar os riscos que impactam o alcance dos objetivos estratégicos;

III - Avaliar a adequação, a suficiência e a eficácia do processo de gestão de riscos, revisando a política e a metodologia de gestão de riscos sempre que necessário;

IV - Assessorar os órgãos de governança nos temas técnicos acerca da gestão de riscos.

c) Terceira Linha: composta pela auditoria interna, que tem o papel de fazer uma avaliação objetiva e independente dos controles e da gestão de riscos. Compete à auditoria interna, como Terceira Linha:

I - Avaliar as atividades da Primeira e Segunda Linhas no que tange à eficácia dos controles internos e da gestão de riscos, assessorando-os quanto às melhores práticas;

II - Verificar a conformidade das atividades executadas com a Política de Gestão de Riscos;

III - Avaliar o desempenho da gestão de riscos, com o objetivo de promover a melhoria contínua dos processos.

6.1 Método aplicado para definição de responsabilidade

As competências específicas dos atores da gestão de risco estão discriminadas na Resolução nº 7 de 2021 que aprova a Política de Gestão de Riscos da Fundação Cultural Palmares e estão disponíveis na Matriz RACI abaixo (Quadro 1).

A Matriz RACI é um método de discernimento dos atores da Gestão de Riscos, ou seja ela tem a função de avaliar a distinção entre os diferentes papéis por meio do reconhecimento dos seguintes atores:

R: quem executa a atividade;

A: quem aprova a tarefa ou produto. Pode delegar a função, mas mantém a responsabilidade;

C: quem pode agregar valor ou é essencial para a implementação; e

I: quem faz o controle, mas não precisa necessariamente se envolver na decisão.

Quadro 1 - Matriz RACI da Gestão de Riscos na FCP.



Atividades	Atores do processo			
	CIGFCP	CGE	GRs	Auditoria
Definir a matriz de risco	A	R	C	I
Definir o apetite ao risco	A	R	C	I
Definir diretrizes para priorização e tratamento dos riscos	A	R	C	I
Priorização de projetos/processos de trabalhos/serviços	A	C	R	I
Estabelecer o contexto geral	A	C	R	I
Identificar os riscos	A	C	R	I
Analisar os riscos	A	C	R	I
Avaliar os riscos	A	R	C	I
Tratar os riscos	A	C	R	I
Monitorar e realizar análise	A	R	C	R

7. MAPEAMENTO DOS PROCESSOS ORGANIZACIONAIS PARA DEFINIÇÃO DO OBJETO DA GESTÃO DE RISCO

7.1. Análise do Escopo do Processo

De forma a possibilitar a integração da Gestão de Riscos à Gestão de Processos, primeiro foi necessário compreender de forma detalhada os processos, uma vez que os processos serão o objeto de gerenciamento dos riscos.

Esse trabalho trará melhorias substanciais para ambas atividades, gestão de processos e gestão de riscos, como por exemplo, melhor entendimento das etapas e dos fluxos dos processos e assim melhor controle de riscos nos pontos críticos; melhor entendimento do papel dos atores e das suas responsabilidades e ainda, visualização adequada das etapas para melhor dimensionamento do custo operacional e temporal dos processos.

Além desses benefícios, tanto a gestão de processos como a gestão de riscos colaboram para a mesma finalidade, isto é, o alcance dos objetivos estratégicos por meio de Planos de Ação com focos distintos, melhoria do processo e tratamento de riscos. Dessa forma, optou-se por integrar ambos os processos, buscando uma otimização do tempo, custo operacional e redução no impacto para as áreas executoras.

A estratégia adotada foi entrevistar cada área da entidade para levantamento de todas as atividades realizadas e identificação dos conjuntos de atividades que correspondem aos processos. Dentre os critérios para identificação dos processos estão: (i) a identificação de conjuntos de atividades que tenham interface com outras unidades da entidade ou público-alvo, (ii) normas reguladoras próprias e (iii) procedimentos específicos.

Nessa etapa é necessário que se avalie e confirme os processos para realizarmos um mapeamento dos processos da entidade, que consiste em descrever o fluxo de trabalho, objetivos, etapas, procedimentos, atividades, recursos humanos, equipamentos, sistemas de informação e materiais requeridos, entradas e saídas. Esses dados serão descritos na Planilha Diagrama de Escopo e Interface do Processo - DEIP (Figura 3).

Cabe ressaltar que esse passo fornece as saídas dos processos, o que é essencial para definir os eventos de riscos que podem afetar seus objetivos, uma vez que a ocorrência do risco acarreta na impossibilidade de obtenção da saída do processo (Figura 4).

7.2. Modelagem do Processo

A modelagem do processo é representada por um fluxograma (Figura 5). O fluxograma é uma representação gráfica de como o trabalho acontece e tem a função de simplificar ao entendimento sobre as tarefas. Ele é elaborado com o auxílio da ferramenta Bizagi.

Figura 5 - Exemplo de Fluxograma do Processo

Para facilitar a elaboração do fluxograma será solicitado inicialmente o preenchimento da planilha Lista de Tarefas do Processo (Figura 6).

Figura 6 - Lista de Tarefas do Processo para elaboração do fluxograma.

Assim que concluído os passos descritos acima, análise do escopo e fluxograma, será possível visualizar a carteira de processos de toda a entidade, bem como todas as tarefas e interfaces entre as diferentes áreas da entidade. Esses dados auxiliam o levantamento de riscos por permitirem a fácil identificação de pontos críticos e a reflexão mais objetiva sobre os riscos que prejudicam ou impedem a obtenção das saídas dos processos.

8. ETAPAS DA METODOLOGIA DE GESTÃO DE RISCO

O processo de gerenciamento de riscos, segundo a ISO 31000:2018 (Figura 7) contém as seguintes etapas:

Figura 7 - Diagrama do processo de gestão de riscos da norma ABNT NBR ISO 31000:2018 - Diretrizes

a) Escopo, Critério e Contexto: conhecer os objetivos organizacionais e os processos a eles relacionados, assim como definir os contextos internos e externos a serem levados em consideração ao gerenciar os riscos;

b) Identificação do risco - corresponde a aplicação do processo sistemático para compreender o que pode acontecer, como, quando e por quê;

c) Análise do risco - se relaciona com a compreensão de cada risco, suas consequências e probabilidades;

d) Avaliação do risco - envolve tomada de decisão sobre o nível do risco e prioridade de atenção através da aplicação do critério desenvolvido na ocasião em que o contexto foi estabelecido.

e) Tratamento do risco - se refere ao processo pelo qual os controles existentes são aperfeiçoados ou novos controles são desenvolvidos e implementados. Compreende a avaliação e seleção de opções, o que inclui análise de custos e benefícios e avaliação de novos riscos que podem ser



gerados a partir de cada opção e, desse modo, priorizando e implementando o tratamento selecionado segundo o processo planejado.

f) Os elementos "Comunicação e Consulta", "Monitoramento e Análise Crítica" e "Registro e Relato" são considerados agentes de ação contínua do processo de gestão de riscos. A comunicação e consulta implica no envolvimento das partes interessadas internas e externas a organização, objetivando considerar seus pontos de vista, conhecendo seus objetivos por meio de envolvimento planejado. O "Monitoramento e a Análise Crítica" preveem a tomada de ação no momento em que surgirem novos riscos que mudem os riscos existentes, como produto de mudança nos objetivos organizacionais ou nos ambientes interno e externo. O "Registro e Relato" são os mecanismos apropriados para relatar e documentar os fatos apropriadamente.

Para registro dos riscos levantados será utilizada a "Planilha documentadora de Riscos", que é um documento em formato "xls" apensado a este manual. Este arquivo contém diversas abas as quais deverão ser preenchidas e impressas em pdf. A citada planilha é de autoria do TCU, na qual estão inseridos critérios para análise do impacto e probabilidade do risco, bem como fórmulas para ponderação dos fatores de impacto e probabilidade.

A execução do processo de gerenciamento de riscos, na FCP, acompanhará, o ciclo do planejamento estratégico. O processo de gerenciamento de riscos deverá ser executado integralmente, após à definição do planejamento estratégico para o período.

Ao alinhar o calendário de ambas as iniciativas, estimula-se a sinergia entre os instrumentos, visto que há fases que se retroalimentam nesses processos. Por exemplo, a formulação da estratégia prevê a realização de diagnóstico organizacional e priorização de iniciativas e processos que devem direcionar a fase de escopo, contexto e critério, do gerenciamento de riscos.

A reunião de análise estratégica, de periodicidade anual, que revisita iniciativas, processos, planos táticos e indicadores, também fornece subsídios para o monitoramento e controle do processo de gerenciamento de riscos, podendo redundar, inclusive, em novas iterações do processo.

Nesse sentido, será elaborado relatório anual acerca do monitoramento dos riscos mencionados e o Plano de Gestão de Riscos será quadrienal e em consonância ao Plano Estratégico Institucional.



8.1. Escopo, Contexto e Critérios

Segundo a ISO 31000:2018, o propósito do estabelecimento do escopo, contexto e critérios é personalizar a gestão de riscos, permitindo um processo de avaliação de riscos eficaz e um tratamento de riscos apropriado.

8.1.1. Escopo

Definir o escopo significa circunscrever os elementos básicos que nortearão a execução do processo de gerenciamento de riscos, como por exemplo: (i) Objetivos e decisões que precisam ser tomadas; (ii) Resultados esperados das etapas a serem realizadas no processo; (iii) Tempo, localização, inclusões e exclusões específicas; (iv) Ferramentas e técnicas apropriadas para o processo de avaliação de riscos; (v) Recursos requeridos, responsabilidades e registros a serem mantidos; (vi) Relacionamentos com outros projetos, processos e subprocessos.

Será priorizada a aplicação do gerenciamento de riscos no nível estratégico, por isso serão avaliados os processos que contribuem diretamente para o alcance dos objetivos estratégicos. Nos próximos ciclos poderão ser levantados os riscos à nível operacional, de programa, de projeto e ou de atividades.

Para tratamento serão priorizados os riscos que ameaçam os objetivos estratégicos. Em ordem de prioridade serão avaliados processos e riscos segundo as seguintes condições:

1. Se possui recomendações e/ou determinações de órgãos como, Ministério Público, Tribunais, Controladoria Geral da União, Tribunal de Contas da União, Procuradoria Federal junto a FCP e Auditoria Interna;
2. Se integra serviço prestado pela FCP;
3. Se requer qualificação técnica específica;

4. Se é dependente de recursos tecnológicos específicos;
5. Se possui reclamações registradas na Ouvidoria; e
6. Se possui denúncias registradas e associadas à sua execução.

A análise desses critérios definirá os processos prioritários para tratamento imediato.

8.1.2. Contexto

O contexto consiste no levantamento dos aspectos externos e internos do ambiente no intuito de compreender os fatores que podem interferir no alcance dos objetivos estratégicos da entidade.

O ambiente interno envolve aspectos como governança, estrutura organizacional, funções, alçadas e responsabilidades, políticas, estratégias, capacidades, competência, sistemas de informação, processos decisórios e cultura organizacional.

O ambiente externo envolve aspecto social, político, econômico, legal, regulatório, financeiro, tecnológico, econômico, ambiental, relações com partes interessadas externas e suas percepções e valores.

Para avaliação e registro do Contexto utilizar-se-á a ferramenta Análise SWOT - Strengths (pontos fortes), Weaknesses (pontos fracos), Opportunities (oportunidades para o seu negócio) e Threats (Ameaças). No português é conhecida como análise FOFA (Forças, Oportunidades, Fraquezas e Ameaças - Figura 8). A análise SWOT é feita de modo específico para cada processo e ciclo, uma vez que a mudança de ambiente/contexto pode mudar os riscos, ou seja, em determinados contextos pouco hostis, um risco potencial pode deixar de sê-lo.

Figura 8 - Esquema e definições da Ferramenta Análise SWOT para avaliação do contexto. Fonte: ENAP, 2018.

A avaliação do contexto será registrada na Planilha Documentadora de Riscos (Arquivo em excel apensado a este documento), Aba 2 - Ambiente e Fixação de Objetivos (Figura 9), conforme modelo abaixo:

Figura 9 - Ambiente e Fixação de Objetivos

8.1.3. Critérios

No processo de gerenciamento de riscos os critérios são termos de referência contra os quais a significância de um risco é avaliada para dizer se um risco é tolerável ou aceitável (ABNT, 2009). Os critérios são baseados nos objetivos organizacionais, no contexto externo e interno e ainda podem ser derivados de normas e políticas.

Definir os critérios ajuda a apoiar a tomada de decisão, e significa especificar a quantidade, o tipo de risco e a significância do risco que a organização pode assumir em relação aos objetivos.

8.1.3.1. Matriz de Appetite a Riscos

Define o nível de risco que a organização está preparada para buscar, manter ou assumir. No caso da FCP, riscos com níveis de significância menor que 10 (pequeno, moderado e parte dos altos) serão aceitáveis (Figura 10). Já os riscos com níveis de significância maior ou igual à 10, que são parte dos níveis alto e crítico, serão considerados inaceitáveis e um plano de ação deverá ser proposto ao CGIFCP e o tratamento do risco deve ocorrer imediatamente. Abaixo apresenta-se a matriz de risco com impacto e probabilidade e níveis de risco:

Figura 10 - Matriz de risco com impacto e probabilidade e níveis de risco aceitáveis e não aceitáveis (³10, em destaque)

8.2. Identificação de Riscos

Esta etapa tem como finalidade desenvolver uma lista abrangente de eventos de risco que podem ter impacto no alcance dos objetivos, categorizando-os e identificando causas e potenciais consequências.

Recomenda-se que todos os riscos sejam incluídos no processo de identificação, mesmo aqueles provenientes de ambientes não controlados pela FCP (ou seja, potenciais ameaças externas), uma vez que, quando um risco não é identificado, ele não pode ser analisado ou tratado.



Identificar o risco implica em reconhecer os eventos que podem impedir o alcance dos objetivos e também identificar os efeitos de ocorrência do risco e as causas (Figura 11), isto é, as condições potenciais que podem originar o risco ou que viabilizem sua concretização.

(Fonte: CAIXA - Guia prático de linhas de defesa. Ciclo anual de gerenciamento de riscos)

Os riscos, bem como causas, efeitos e controles serão inseridos na aba 3 da Planilha Documentadora de Riscos, a qual tem a seguinte aparência (Figura 12):

Figura 12 - Planilha Documentadora de Riscos. Aba 3. Mapa de Riscos

8.2.1. Definição das Técnicas para levantamento do risco com as equipes

Há várias técnicas disponíveis para identificação de riscos e essas podem ser combinadas. Para escolha das técnicas leva-se em consideração o grau de maturidade da organização; as especificidades do setor; a natureza do processo; e o nível de aprofundamento desejado.

Algumas das técnicas mais conhecidas que podem ser sugeridas para a realização do levantamento desses componentes são: Brainstorming, questionários, entrevistas, checklist, análise SWOT (forças, fraquezas, oportunidades e ameaças), análise de dados históricos, análise de premissas, opiniões especializadas, necessidades das partes interessadas e diagramas de causa e efeito. Essas técnicas estão descritas em ABNT. ISO/IEC 31010:2012.

Neste primeiro ciclo de levantamento de riscos serão realizadas entrevistas com gestores (com ou sem equipe), onde será utilizado brainstorming motivados pelas perguntas descritas no diagrama abaixo (Figura 13), na ordem indicada em cada quadro. Durante a entrevista é essencial que todos os participantes possam visualizar todo o diagrama durante o encontro.

Figura 13 - Diagrama utilizado durante as entrevistas para visualização das perguntas e para registro dos riscos, causas, efeitos e controles. (Fonte: Autoria própria)

O encontro inicia-se com a pergunta: 1) que eventos impedem ou prejudicam o alcance das saídas? Após registros das respostas dos eventos de riscos realiza-se 2) um momento de reflexão e realocação dos eventos que são causas no quadro correspondente, pois neste primeiro momento é comum que parte dos eventos mencionados se mostrem como causas dos demais. Prossegue-se com 3) a solicitação e registro dos efeitos e então 4) verifica-se se todas os eventos de risco têm causas relacionadas já registradas, caso não tenham, registra-se as causas faltantes. 4) Passa-se a etapa de registros dos controles atualmente realizados e por último 5) Registra-se as ações de tratamento que devem ser tomadas caso o risco ocorra e também as ações de controle que ainda não são tomadas.

8.2.2. Categorização dos Riscos

Quanto à categorização dos riscos, os eventos podem se enquadrar em alguma das classificações abaixo:

- **Estratégico:** eventos que possam impactar o cumprimento da missão da FCP, das metas ou dos objetivos estratégicos, caso venham a ocorrer. Incluem riscos legais, isto é, eventos derivados de alterações legislativas ou normativas que podem comprometer as atividades do órgão ou entidade.

- **Operacional:** eventos que podem comprometer as atividades da unidade. Normalmente estão associados a falhas, deficiência ou inadequação de processos, pessoas, infraestrutura e sistemas, afetando a gestão eficaz e eficiente dos processos organizacionais;

- **Orçamentário:** eventos que podem comprometer a capacidade da FCP de contar com recursos orçamentários e financeiros necessários à realização de suas atividades, ou eventos que possam comprometer a execução orçamentária, como atrasos no cronograma de licitações;

- **Reputação:** eventos que podem comprometer a confiança das partes interessadas em relação à capacidade da FCP em cumprir sua missão institucional, interferindo diretamente na reputação da agência;

- **Integridade:** eventos que podem afetar a probidade da gestão dos recursos públicos e das atividades da organização, causados pela falta de honestidade e desvios éticos.

- **Fiscal:** eventos que podem afetar negativamente o equilíbrio das contas públicas.



· Conformidade: eventos que podem afetar o cumprimento de leis, regulamentos e contratos aplicáveis;

8.3. Análise de Riscos

Alcançada a identificação dos riscos bem como suas causas, efeitos e controles, passa-se a etapa de análise dos riscos em impacto e probabilidade.

O resultado final dessa etapa atribuirá a cada risco identificado uma classificação, tanto para a probabilidade como para o impacto do evento, cuja combinação determinará o nível do risco e consiste na conjunção dos pesos do impacto, analisado em 5 categorias, e da probabilidade, também avaliada em 5 categorias (Figura 10), acima apresentado.

A análise de riscos é feita duas vezes, uma primeira vez examina-se os parâmetros de Impacto e Probabilidade sem considerar os controles existentes (Risco Inerente ou potencial) e uma segunda vez, na segunda vez, examina-se os mesmos parâmetros de Impacto e Probabilidade considerando-se os controles já existentes (Risco residual).

O Nível de Risco Inerente: É o nível do risco sem considerar quaisquer controles que podem reduzir a probabilidade da sua ocorrência ou o seu impacto. Nível de Risco Residual - RR é o nível de risco remanescente, após se analisarem os possíveis controles existentes que podem reduzir a probabilidade da sua ocorrência ou o seu impacto (Figura 14).

O nível de RI é obtido por meio do produto aritmético entre a Probabilidade (P) e o Impacto (I).

Figura 14 - Diagrama de riscos

Os registros serão realizados nas Abas 4 e 5 da Planilha Documentadora de Riscos, a qual tem a seguinte aparência (Figura 15):

Figura 15 - Planilha Documentadora de Riscos. Aba 4. Cálculo de Risco Inerente e Aba 5. Cálculo de Risco Residual

8.3.1. Análise dos riscos inerentes em impacto e probabilidade

Para análise do impacto são examinados 6 parâmetros (Figura 16), conforme as 5 categorias já mencionadas: 1) esforço da gestão para gerenciamento do risco identificado (Peso 15%); 2) nível de ação para regularização do processo caso o risco ocorra (Peso 17%); 3) amplitude de disseminação na mídia caso o risco ocorra (Peso 12%); 4) nível de interferência nos objetivos estratégicos (Peso 18%); 5) Nível de intervenção hierárquica para lidar com as consequências do risco (Peso 13%) e 6) impacto financeiro-orçamentário do risco caso ocorra quando for possível reconhecer o impacto financeiro-orçamentário.

Figura 16 - Aspectos analisados para compreender o Impacto do Risco na organização conforme Planilha Documentadora de Riscos (TCU):

Na análise da probabilidade do risco serão consideradas as seguintes frequências e pesos (Figura 17): 1) Muito baixa para eventos de risco que podem ocorrer apenas em circunstâncias excepcionais, isto é em menos de 10% das vezes em que o processo associado ocorre; 2) Baixo para eventos que podem ocorrer em algum momento, isto é, de 10 a 30 % das vezes; 3) Média para eventos que devem ocorrer em algum momento, isto é de 30% a 50% das vezes; 4) Alta para evento que provavelmente ocorra na maioria das circunstâncias, isto é entre 50% e 90% das vezes; Muito alta para eventos esperados que ocorram na maioria das circunstâncias, ou seja em mais de 90% das vezes em que o processo associado acontece.

Figura 17 - Frequências e classificação analisados para o Probabilidade do Risco conforme Planilha documentadora de Riscos (TCU).

8.3.2 Análise dos riscos residuais em impacto e probabilidade

Nesta etapa analisa-se os riscos segundo os mesmos parâmetros utilizados para análise de riscos inerentes, mas agora ao refletir sobre Impacto e Probabilidade deve considerar os controles já existente. Esta última análise corresponde ao risco residual.

Ao analisar Impacto e Probabilidade é necessário registrar as etapas nas duas abas correspondentes da Planilha Documentadora de Riscos para que o cálculo do nível de risco seja feito ao multiplicar a nota do impacto pela nota da probabilidade levantadas nas duas etapas anteriores, isto é de



análise do risco inerente e do risco residual.

8.4. Avaliação de Riscos

8.4.1. Classificação do risco em 4 classes de acordo com a magnitude

A avaliação de riscos visa comparar o nível de risco encontrado durante a etapa de análise com os critérios de risco definidos, utilizando os resultados como subsídio para a tomada de decisões sobre quais riscos necessitam ser tratados ou não, e com que prioridade.

O resultado de Risco Inerente, bem como o resultado do Risco Residual, obtidos pelo produto de cada valor de probabilidade e impacto, pode então, ser classificado em termos de magnitude em 4 classes (Figura 18).

Figura 18 - Classes de avaliação do risco

A matriz de risco (Figura 19) é gerada quando são combinados o impacto e a probabilidade. Esta classificação é obtida quando preenchemos a Planilha Documentadora de Riscos (Arquivo em excel apensado a este documento).

Figura 19 - Matriz de riscos com categorias por nível de magnitude: Pequeno (verde); Moderado (amarelo), Alto (vermelho) e Crítico (preto).

8.5. Avaliação dos controles existentes

Os controles são essenciais para redução do impacto e da probabilidade de ocorrência do risco. Por isso, a definição de controles preventivos, corretivos e/ou compensatórios é de grande importância para aumentar as chances de alcance dos objetivos estratégicos e operacionais.

Uma vez identificados conjuntamente com os Riscos na primeira etapa, cabe agora indicar o nível de maturidade dos controles conforme segunda as classes predefinidas na Planilha Documentadora de Riscos.

Os Controles podem ser classificados quanto ao desenho em: (1) Não há sistema de Controle; (2) Há procedimento de controle para algumas atividades, porém informais; (3) Controles não foram planejados formalmente, mas são executados de acordo com a experiência dos servidores; (4) É desenhado um sistema de controle integrado adequadamente planejado, discutido e documentado. O sistema de controle vigente é eficaz, mas não prevê revisões periódicas; (5) O sistema de controle é eficaz na gestão de riscos (adequadamente planejado, discutido, testado e documentado com correções ou aperfeiçoamentos planejados de forma tempestiva).

Realiza-se também a classificação dos controles quanto a operação dos controles em: (1) Controle não executado; (2) Controle parcialmente executado e com deficiências; (3) Controle parcialmente executado; (4) Controle implantado e executado de maneira periódica e quase sempre uniforme. Avaliação dos controles é feita com alguma periodicidade; (5) Controle implantado e executado de maneira uniforme pela equipe e na frequência desejada. Periodicamente os controles são testados e aperfeiçoados.

8.6. Tratamento de Riscos

8.6.1. Preenchimento do Plano de ação para tratamento dos Riscos Inaceitáveis

Esta etapa tem como finalidade selecionar a resposta (tratamento) a ser adotada, para cada risco avaliado, de acordo com o Nível de Risco Residual, com o apetite a riscos, com o contexto da FCP ou custo do controle, conforme o quadro a seguir (Quadro 2).

Quadro 2 - Estratégia de Resposta ao Risco. Fonte: Metodologia de Gestão de Riscos (CGU, 2018, adaptado)

Opções de tratamento	Descrição
Aceitar	Um risco normalmente é aceito quando seu nível está nas faixas de apetite a risco. Nessa situação, nenhum novo controle precisa ser implementado para mitigar o risco.
Reduzir	Essa estratégia normalmente é escolhida quando é classificado como "Alto" ou "Crítico". A implementação de controles deve apresentar um custo/benefício adequado. Reduzir o risco significa implementar controles que possam minimizar as causas ou as consequências dos riscos, identificadas anteriormente



Compartilhar	Um risco normalmente é compartilhado quando é classificado como "Alto" ou "Crítico", mas a implementação de controles não apresenta um custo/benefício adequado. Pode-se compartilhar o risco por meio de terceirização ou apólice de seguro, por exemplo.
Evitar	Um risco normalmente é evitado quando é classificado como "Alto" ou "Crítico", e a implementação de controles apresenta um custo muito elevado, inviabilizando sua mitigação, ou não há entidades dispostas a compartilhar o risco com a FCP. Evitar o risco pode significar encerrar ou deixar de implementar o processo organizacional. Nesse caso, essa opção deve ser aprovada pelo Comitê Interno de Governança - CIGFCP.

Selecionada a resposta mais adequada ao tratamento de cada risco, a fase seguinte consistirá na elaboração dos planos de ação, e estabelecer os prazos para a implementação das iniciativas deles constantes. Os planos de ação podem implicar a adoção de novos controles ou a modificação de controles já existentes e deverão considerar:

- A eficácia das ações já existentes;
- As restrições organizacionais, técnicas e estruturais;
- Os requisitos legais;
- A análise custo/benefício;
- As ações a serem realizadas;
- As prioridades; e
- O cronograma de execução. O Plano de Tratamento de Riscos contemplará todos os planos de ação propostos, de acordo com os riscos identificados.

Os Planos de Ação conterão, pelo menos os seguintes itens (Figura 20) (e devem ser preenchidos em aba própria da Planilha Documentadora de Riscos (Aba 6. Plano de Ação) conforme ilustrado abaixo:

- Objetivos/benefícios esperados;
- Unidade organizacional responsável pela implementação dos planos de ação e unidade(s) interveniente(s);
- Gestor de Riscos responsável;
- Breve descrição sobre a implementação;
- Data prevista para início da implementação;
- Data prevista para o término, se for o caso; e
- Status dos planos de ação.



Figura 20 - Apresentação do Plano de Ação na Planilha Documentadora de Riscos

Cabe ao Gestor de Risco a submissão ao Comitê interno de governança da FCP - CIGFCP, o plano de ação para os riscos considerados inaceitáveis, isto é, os riscos residuais com classificação de magnitude Crítico ou Alta (³10) conforme matriz de risco (Figura 10). Todos os riscos (pequenos, moderados, altos e críticos) devem ter uma resposta preenchida na aba correspondente (Aba 6. Plano de Ação), no entanto apenas os Riscos classificados como inaceitáveis devem ter um plano de ação submetido ao CIGFCP para avaliação e decisão quanto ao tratamento a ser dado.

Se as iniciativas do plano de ação envolverem mais de uma unidade, o Gestor de Riscos responsável deve encaminhar a proposta do plano para os Gestores de Riscos das unidades envolvidas, para que estes validem as iniciativas das quais fizeram parte. É importante ressaltar que o tratamento a ser implementado pode ser uma nova fonte de risco e deve ser tratado em conjunto com sua implementação.

O Gestor de Risco formaliza, o CIGFCP aprova, e a CGE monitora os planos de ação, confirmando o responsável para cada iniciativa de tratamento e prazos acordados, que é de 6 meses para os riscos considerados inaceitáveis. A CGE, juntamente com os Gestores de Riscos, deve verificar se as medidas adotadas estão sendo eficazes, bem como atualizar o CIGFCP da execução do plano para os riscos considerados inaceitáveis.

Cabe ao Gestor de Risco, responsável pelo tratamento, atualizar o progresso das iniciativas do plano de ação e comunicar à CGE.

Após a execução da iniciativa de tratamento, é possível que permaneça algum risco residual. Este deve ser confrontado com o apetite a riscos definido, a fim de verificar se está compreendido no nível "Aceitável". Caso negativo, deverá ser adotado um plano de ação para tratamento do risco residual.

É necessário avaliar a necessidade de melhorar ou extinguir controles já existentes. Somente após essa avaliação podem ser propostos novos controles, caso ainda haja necessidade de redução do nível de risco.

O próximo quadro mostra a atitude a ser tomada, de acordo com o Nível de Risco residual (Quadro 3) encontrado:

Quadro 3 - Atitude perante o risco para cada Nível de Risco Residual. Fonte: Metodologia de Gestão de Riscos (CGU, 2018, adaptado)

Classificação	Ação necessária	Exceção
Risco pequeno	Nível de risco dentro do apetite a risco, mas é possível que existam oportunidades de maior retorno que podem ser exploradas assumindo-se mais riscos, avaliando a relação custo x benefício, como diminuir o nível de controles. Indica que o risco inerente já está dentro da tolerância a risco.	Caso o risco seja priorizado para implementação de medidas de tratamento, essa priorização deve ser justificada pelo Gestor de Riscos e aprovada pelo CIGFCP.
Risco Moderado	Nível de risco dentro do apetite a risco. Geralmente nenhuma medida especial é necessária, porém requer atividades de monitoramento específicas e atenção da unidade na manutenção de respostas e controles para manter o risco nesse nível, ou reduzi-lo sem custos adicionais. Indica que o risco residual já está dentro da tolerância a risco, mas deve se buscar reduzi-lo.	Caso o risco seja priorizado para implementação de medidas de tratamento, essa priorização deve ser justificada pelo Gestor de Riscos e aprovada pelo CIGFCP.
Risco Alto	Risco Alto Nível de risco além do apetite a risco. Qualquer risco nesse nível deve ser comunicado ao Núcleo de Gestão de Riscos e ter uma ação tomada em período determinado. Postergação de medidas só com autorização do CIGFCP. Indica que o risco residual será reduzido a um nível compatível com a tolerância a riscos.	Caso o risco não seja priorizado para implementação de medidas de tratamento, a não priorização deve ser justificada pelo Gestor de Riscos e aprovada pelo CIGFCP.
Risco Crítico	Nível de risco muito além do apetite a risco. Qualquer risco nesse nível deve ser comunicado ao Comitê Interno de Governança e ter uma resposta imediata, construção de Plano de ação e tratamento em até 6 meses. Postergação de medidas só com autorização do CIGFCP. Indica que nenhuma opção de resposta foi identificada para reduzir a probabilidade e o impacto a nível aceitável. Para identificação do tipo de resposta, isto é se deve evitar o processo ou prosseguir com o processo adicionando-se mais controles, deve-se avaliar se o custo do processo que gera o risco é desproporcional ou se a capacidade de lidar com o risco é muito limitada.	Caso o risco não seja priorizado para implementação de medidas de tratamento, a não priorização deve ser justificada pelo Gestor de Riscos e aprovada pelo CIGFCP.



8.7. Comunicação e Consulta

8.7.1. Comunicação dos Riscos Identificados

A comunicação consiste em um processo interativo de troca de informações e opiniões, envolvendo a organização e seus participantes, e as partes interessadas externas. Por sua vez, a consulta constitui-se em um processo de comunicação informativa entre a organização e as partes interessadas, antes de se tomar uma decisão ou definir um posicionamento em relação a uma determinada questão.

Muito do envolvimento das pessoas e unidades na gestão de riscos é influenciado por ações de comunicação e consulta eficazes. Conseqüentemente, essas devem ser mantidas durante todas as fases do processo de gerenciamento de riscos.

A comunicação e a consulta têm como objetivo principal facilitar a troca de informações, levando em consideração os aspectos de confidencialidade, integridade e confiabilidade e deve ser realizada contando, minimamente, com os seguintes instrumentos:

Plano de comunicação - No início de um novo ciclo de execução do processo de gerenciamento de riscos, é necessária a definição, em um documento estruturado, dos elementos-chave concernentes à comunicação como finalidade, destinatários, responsáveis, tipo e periodicidade das ações de comunicação que serão promovidas.

Registro das ocorrências de riscos - caso um evento de risco venha a ocorrer, devem ser registradas informações relativas ao fato, tais como descrição do evento ocorrido, impactos e prejuízos causados aos objetivos estratégicos e ao alcance das metas que permitam a construção de uma base histórica para avaliação da maturidade da instituição com relação à sua gestão de riscos.

Os relatórios gerenciais de riscos de cada unidade serão submetidos ao CIGFCP a cada ciclo de monitoramento que é anual e também comporão os Planos Bianual de Gestão de Risco como produto da fase de monitoramento e controle e auxílio à tomada de decisão para o Planejamento Estratégico.

Os Planos serão aprovados por meio de Resolução, a serem publicados no Boletim de serviço Eletrônico, cuja matéria de ser encaminhada à Procuradoria Federal junto à Fundação Cultural Palmares para exame e parecer.

8.8. Monitoramento e Análise Crítica

8.8.1. Análise crítica dos riscos monitorados

A etapa de monitoramento e análise crítica constitui-se em um processo contínuo ao longo do ciclo de gestão de riscos, e sua execução tem como objetivos:

- Possibilitar a identificação de mudanças na classificação do risco e ajustar o tratamento, bem como a prioridade e os planos de ação adotados, com base na reavaliação dos contextos interno e externo;
- Assegurar o acompanhamento dos eventos de risco e seus desdobramentos;
- Acompanhar e garantir a eficácia e eficiência dos controles internos adotados;
- Possibilitar a identificação de novos riscos ou riscos residuais que não haviam sido considerados, subsidiando o ciclo de Gestão de Riscos subsequente; e
- Possibilitar a atualização e melhoria contínua do Processo de Gestão de Riscos, e de sua estrutura.

O monitoramento e análise crítica ocorrerá anualmente e definirá as necessidades, podendo inclusive, determinar a realização de novo processo de avaliação de riscos ainda durante a vigência de determinado plano de ação, caso verifique mudanças relevantes que ensejem tal medida.

As competências para a execução dessa etapa são as seguintes:

- Gestores de Risco: são responsáveis por monitorar os riscos levantados nos processos, subprocessos e projetos sob sua responsabilidade e o tratamento atribuído a eles;
- CGE: Responsável por monitorar a execução dos planos de ação definidos para tratamento dos riscos identificados pelos Gestores de Risco e suas equipes. Mudanças identificadas durante o monitoramento devem ser encaminhadas à CGE, a quem compete monitorar os resultados de todas as iniciativas de gestão de riscos da FCP. Tais alterações serão objeto de aprovação pelo CIGFCP;
- Comitê Interno de Governança: realiza a análise crítica do processo de gestão de riscos e é instância competente para aprovação dos planos de ação e de suas eventuais alterações.

A análise crítica deve ser realizada de maneira periódica, concretizada por intermédio de reuniões, feedbacks e análises que permitam a reavaliação contínua do processo de Gestão de Riscos, em busca de seu constante aperfeiçoamento. Aqui cabe registrar a recomendação da Organização para a Cooperação e Desenvolvimento Econômico OCDE (2022) que sugere para cada unidade:

- I) traduzir um repertório de riscos em questões orientadoras para apoiar os gestores no processo de identificação de riscos;
- II) desenvolver e sistematizar um repertório de riscos transversais e sinais de alerta correspondentes;



III) Identificar pontos de decisão ao longo do processo para lembrar os gestores de vieses típicos; e

IV) Oportunidade para explicar o que é risco, o que é integridade e por que a gestão de riscos é necessária.

8.9. Registro e Relato

O processo de Gestão de Riscos e seus resultados devem ser documentados e relatados por meio de mecanismos apropriados, a serem disponibilizados pela Coordenação de Gestão Estratégica. O registro e o relato visam a:

- Comunicar atividades e resultados de gestão de riscos em toda a organização;
- Fornecer informações para a tomada de decisão;
- Melhorar as atividades de gestão de riscos;
- Auxiliar a interação com as partes interessadas, incluindo aquelas com responsabilidade e com responsabilização por atividades de gestão de riscos.

Um calendário de reuniões com as diversas instâncias deve ser mantido, associado a uma produção regular de relatórios de monitoramento, a fim de estabelecer um fluxo constante de informações e monitoramento da Gestão de Riscos. Os Gestores de Riscos deverão implementar o acompanhamento da gestão de riscos em suas esferas de competência, de maneira a subsidiar, minimamente a seguinte estrutura:

- Relatório anual, produzido por CGE e Gestores de Riscos e aprovado pelo CIGFCP acerca do monitoramento dos riscos mencionados no Plano;

- Plano de Gestão de Riscos - que é um novo plano, feito quadrienal, contendo avaliação do resultado do ciclo que se encerra e abertura do seguinte com todos os riscos identificados, controles, e planos de ação para tratamento de todos os riscos identificados.

- O Plano de ação para tratamento de riscos deve ser submetido à CGE para análise e ao CIGFCP para avaliação e aprovação quando houver mudanças na magnitude de um risco e estes passarem a ser considerados inaceitáveis, isto é, com magnitude maior que 10. Caso um risco inaceitável seja detectado em qualquer momento do ano deve se produzir um plano de ação para tratamento com prazo de imediato.

O processo de gestão de riscos contará com diferentes mecanismos de documentação e comunicação que incluem, mas não estão limitados a: página da intranet da FCP, registros de pautas e atas de reuniões da CGE e CIGFCP, informes periódicos no Sistema Eletrônico de Informações - SEI.

9. REFERÊNCIAS

ABNT. ISO 31000:2009. Gestão de Riscos: Princípios e diretrizes. [Norma]. Rio de Janeiro, RJ. 2009

ABNT. ISO 31000:2018. Gestão de Riscos: Diretrizes. [Norma]. Rio de Janeiro, RJ. 2009

ABNT. ISO/IEC 31010:2012. Gestão de Riscos: Técnicas para o processo de avaliação de riscos. [Norma]. Rio de Janeiro, RJ. 2012.

ENAP. Implementando a Gestão de Riscos no Setor Público. Mod. 3 Ciclo de Gerenciamento de Riscos Corporativos. [Cartilha]. 2018.

CAIXA ECONOMICA FEDERAL. Guia prático de linhas de defesa. Ciclo anual de gerenciamento de riscos. [Manual]. Brasília, DF 2022.

CGU 2018. Metodologia de Gestão de Riscos. [Manual]. Brasília, DF jun/2018.

IIA 2020. O modelo das três linhas do IIA: uma atualização das 3 linhas de defesa. Disponível em: <https://iiabrasil.org.br/noticia/novo-modelo-das-tres-linhas-do-iaa-2020> Acesso 10 ago. de 2023.

PURDY, G. ISO 31000 2009: Setting a new standard for risk management. Risk Analysis. Vol. 30, n. 6, p. 881- 886, 2010.



OCDE. Modernizando a avaliação dos riscos para a integridade no Brasil: Rumo a uma abordagem comportamental e orientada por dados. OECD Publishing. Paris, 2022, 36 p. Disponível em: <https://doi.org/10.1787/61d7fc60-pt> . Acesso em: 14 out. 2022.

Este conteúdo não substitui o publicado na versão certificada.

