



**UNIVERSIDADE
ESTADUAL DO CEARÁ**



**GOVERNO DO
ESTADO DO CEARÁ**
*Secretaria da Ciência, Tecnologia
e Educação Superior*

MANUAL DE GESTÃO DE RISCOS E CONTROLES INTERNOS

FUNDAÇÃO UNIVERSIDADE ESTADUAL DO CEARÁ

ASSESSORIA DE CONTROLE INTERNO – ASCOI/FUNECE

AGOSTO – 2025

Universidade Estadual do Ceará - Uece

Avenida Silas Munguba, 1700 Campus Itaperi – CEP: 60.714.903

Fortaleza-CE • Telefone: (85) 3101.XXXX



**UNIVERSIDADE
ESTADUAL DO CEARÁ**



**GOVERNO DO
ESTADO DO CEARÁ**

*Secretaria da Ciência, Tecnologia
e Educação Superior*

1. INTRODUÇÃO

A Fundação Universidade Estadual do Ceará, com a elaboração do Manual de Gestão de Riscos e Controles Internos, tem como escopo nortear os Gestores, além de obedecer à Instrução Normativa nº 003/2015 do Tribunal de Contas do Estado do Ceará – TCE, como evidência de Procedimentos de Controle, que se refere às políticas e ações de natureza preventiva ou de detecção, para gerenciamento de riscos e alcance dos objetivos da Instituição, através de sua formalização e ampla divulgação entre as esferas organizacional da FUNECE.

A construção deste Manual é de suma importância, tendo em vista que a Assessoria de Controle Interno, por meio de suas atividades de controle, consiste em ferramenta gerencial para a Administração, buscando propiciar efetividade à gestão e assegurar a transparência das ações emanadas pelo Poder Público e dos valores despendidos para custear tais ações. Ademais, salienta-se que o Tribunal de Contas do Estado do Ceará – TCE orienta que, na Prestação de Contas Anual, seja apresentado o Manual de Controle Interno como evidência de Procedimentos de Controle.

O gerenciamento de riscos no setor público ainda é um grande desafio a ser alcançado, havendo necessidade não apenas de estruturas e processos, mas também de uma cultura de gerenciamento de riscos que contribua para a organização atingir seus objetivos de forma aprimorada. As responsabilidades e deveres do gestor em relação ao bem público exigem a adoção de práticas e estratégias eficazes de gestão de riscos.

Eventos que causam incertezas e venham a impactar o alcance dos objetivos estratégicos, são inerentes a qualquer organização, seja ela pública ou privada, oriundos de fatores econômicos, sociais, legais, tecnológicos, operacionais, entre outros. A gestão de riscos tem a função de assegurar que a instituição atinja seus objetivos, além de ser uma importante ferramenta para ajudar na tomada de decisões e na redução ou na eliminação de retrabalhos.

Este manual objetiva estabelecer e estruturar as etapas necessárias para a operacionalização da Gestão de Riscos, em cumprimento ao que estabelece o Decreto nº 33.805, de 09 de novembro de 2020, que institui a Política de Gestão de Riscos – PGR do Poder Executivo do Estado do Ceará e a Portaria nº 05/2021 – CGE/CE, que institui a Metodologia de Gerenciamento de Riscos do Poder Executivo do Estado do Ceará.

Diante de todo exposto, visa-se incentivar e disponibilizar de forma padronizada, simples e rápida todas as informações pertinentes para proceder, de forma planejada e organizada, à aplicação dos instrumentos de gestão de riscos no âmbito FUNECE.

2. DOS PRINCÍPIOS, OBJETIVOS E DIRETRIZES DA POLÍTICA DE GESTÃO DE RISCOS DA FUNECE

2.1. A Política de Gestão de Riscos da FUNECE observará princípios que orientam sobre suas características, comunicam o seu valor e explicitam seus propósitos, conforme seguem:

- I – agregar e proteger valor;
- II – apoiada e gerenciada pela alta gestão e por todos da organização;
- III – ser parte integrante dos processos organizacionais;
- IV – subsidiar a tomada de decisões;
- V – considerar ameaças e oportunidades;
- VI – ser estruturada e processada de forma personalizada e proporcional aos contextos interno e externo da organização;
- VII – ser baseada nas informações disponíveis, oportunas e claras para as partes interessadas;
- VIII – considerar fatores humanos e culturais;
- IX – sistemática, estruturada, abrangente e oportuna;
- X – transparente e inclusiva;
- XI – dinâmica, iterativa e capaz de reagir a mudanças; e
- XII – fomentar a melhoria contínua da organização.

2.2. A Política de Gestão de Riscos da FUNECE tem como objetivos:

- I – aumentar a probabilidade de atingimento dos objetivos organizacionais;
- II – fomentar uma gestão proativa;
- III – atentar para a necessidade de se identificar e tratar riscos dos processos críticos em toda a organização;
- IV – facilitar a identificação de oportunidades e ameaças;
- V – prezar pelas conformidades legal e normativa dos processos organizacionais;
- VI – melhorar a prestação de contas à sociedade;
- VII – melhorar a governança;
- VIII – estabelecer uma base confiável de informações para a tomada de decisão;
- IX – melhorar o ambiente de controle interno;
- X – alocar e utilizar eficazmente os recursos para o tratamento de riscos;
- XI – melhorar a eficácia e a eficiência operacional;
- XII – melhorar a prevenção de perdas e a gestão de incidentes;
- XIII – minimizar perdas;
- XIV – melhorar a aprendizagem organizacional; e
- XV – aumentar a capacidade de adaptação a mudanças.

2.3. O gerenciamento de riscos deverá contemplar, no mínimo, as seguintes etapas:

- I – comunicação e consulta: realização de atividades a fim de assegurar que os responsáveis pela implementação do processo de gestão de riscos e as partes interessadas compreendam os



fundamentos sobre os quais as decisões são tomadas e as razões pelas quais ações específicas são requeridas;

II – entendimento do contexto: identificação dos objetivos da organização e compreensão dos contextos externo e interno a serem considerados no gerenciamento de riscos;

III – identificação de riscos: elaboração de lista abrangente de riscos com base nos eventos que possam evitar, atrasar, prejudicar ou impedir a realização dos objetivos associados aos processos organizacionais;

IV – análise de riscos: identificação das possíveis causas, consequências e os controles existentes para prevenir a ocorrência de riscos e diminuir o impacto de suas consequências;

V – avaliação de riscos: identificação de quais riscos necessitam de tratamento e qual a prioridade para a implementação do tratamento;

VI – tratamento de riscos: definição das opções de 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;

VII – monitoramento e análise crítica: verificação e supervisão crítica contínua, visando identificar mudanças no desempenho requerido ou esperado para determinar a adequação, suficiência e eficácia da gestão de riscos; e

VIII – registro e relato: atividades referentes ao registro documental e relato das atividades por meio de mecanismos apropriados para fornecer informações para tomada de decisão.

3. DAS ÁREAS DE ATUAÇÃO

O gerenciamento de riscos na FUNECE, conforme Decreto Estadual nº 33.805/2020, deverá contemplar as seguintes áreas de atuação:

I – estratégica;

II – tática; e

III – operacional.

Será definido, por meio de portaria, as áreas de atuação responsáveis pelo gerenciamento de riscos, constituindo-se preferencialmente da seguinte forma:

I – área de atuação estratégica: comitê executivo ou de integridade ou outra instância de decisão colegiada;

II – área de atuação tática: assessoria de controle interno

III – área de atuação operacional: responsáveis pelos processos organizacionais e seus colaboradores.

As áreas de atuação responsáveis pelo gerenciamento de riscos deverão manter fluxo regular e constante de comunicação.

4. DA ESTRUTURA DA GESTÃO DE RISCOS E DOS CONTROLES INTERNOS



4.1. O Sistema de Controle Interno no âmbito da FUNECE é exercido de forma descentralizada, estruturado nas seguintes linhas de defesa:

I – primeira linha: composta pela gestão da própria entidade, responsável pela entrega de produtos e/ou serviços aos clientes da organização, incluindo funções de apoio. É responsável pelo gerenciamento de riscos, incluindo controles internos da gestão. Deve estabelecer e manter estruturas e processos apropriados de forma a atingir os objetivos da organização e garantir a conformidade com os normativos legais e éticos vigentes;

II – segunda linha: constituída pelas funções de supervisão, monitoramento, inclusive da regularidade, e assessoramento quanto a aspectos relacionados ao gerenciamento de risco, incluindo os controles internos da gestão, Comitê de Integridade e Assessoria Jurídica, atuando, entre outras, como facilitadores da implementação de práticas eficazes de gerenciamento de riscos por parte da primeira linha;

III – terceira linha: constituída pelas atividades de avaliação e de consultoria realizadas pela Controladoria e Ouvidoria Geral do Estado, de forma independente e objetiva, sobre a adequação e eficácia da governança e do gerenciamento de risco, incluindo os controles internos da gestão, desenhada para adicionar valor e melhorar as operações no âmbito do Poder Executivo, sem prejuízo da competência da Procuradoria-Geral do Estado.

4.2. Os controles internos são o conjunto de regras, procedimentos, diretrizes, protocolos, rotinas de sistemas informatizados, conferências e trâmites de documentos e informações, entre outros, destinados a mitigar os riscos e fornecer segurança razoável na consecução da missão da FUNECE.

4.2.1. Os controles internos são operados por todos os agentes públicos responsáveis pela condução de atividades e tarefas no âmbito dos processos finalísticos e de apoio da FUNECE.

4.2.2. Os controles internos devem ser efetivos e consistentes com a natureza, complexidade e risco das operações realizadas, baseando-se no gerenciamento de riscos integrado ao processo de governança da FUNECE.

4.3. Os controles internos devem integrar as atividades, planos, ações, políticas, sistemas, recursos e esforços de todos que trabalhem na organização, sendo projetados para fornecer segurança razoável de que a organização atingirá seus objetivos e missão.

4.3.1. A existência de objetivos claros é pré-requisito para a eficácia do funcionamento dos controles internos.

4.4. Os controles internos não devem ser implementados de forma circunstancial, mas de modo contínuo, como uma série de ações que permeiam as atividades da organização, em consonância com o planejamento estratégico da FUNECE.

4.4.1. Os controles internos devem ser sistematicamente avaliados e, se necessário, revistos para garantir sua eficiência, eficácia e efetividade.



5. DA METODOLOGIA DE GERENCIAMENTO DE RISCOS DA FUNECE

Neste capítulo abordaremos sobre a metodologia de gestão de riscos a ser aplicada no âmbito da FUNECE, elaborada com base no Decreto nº 33.805, de 09 de novembro de 2020, que institui a Política de Gestão de Riscos – PGR do Poder Executivo do Estado do Ceará e a Portaria nº 05/2021 – CGE/CE, que institui a Metodologia de Gerenciamento de Riscos do Poder Executivo do Estado do Ceará.

Vale ressaltar que o preenchimento da matriz de riscos possibilita aos servidores e colaboradores uma visão detalhada de cada etapa do processo facilitando a identificação de possíveis eventos de riscos, as suas causas e possíveis consequências. Essa possibilidade de identificação, análise e tratamento dos riscos agrega grande valor a tomada de decisão dos gestores e proporciona a busca de soluções visando ao atingimento dos objetivos e metas estratégicas da FUNECE de forma mais eficiente, eficaz e efetiva.

Conforme o art. 6º do Decreto nº 33.805, de 09 de novembro de 2020, que institui a Política de Gestão de Riscos – PGR do Poder Executivo do Estado do Ceará, são necessárias, no mínimo, as seguintes etapas:

- I – comunicação e consulta: realização de atividades a fim de assegurar que os responsáveis pela implementação do processo de gestão de riscos e as partes interessadas compreendam os fundamentos sobre os quais as decisões são tomadas e as razões pelas quais ações específicas são requeridas;
- II – entendimento do contexto: identificação dos objetivos da organização e compreensão dos contextos externo e interno a serem considerados no gerenciamento de riscos;
- III – identificação de riscos: elaboração de lista abrangente de riscos com base nos eventos que possam evitar, atrasar, prejudicar ou impedir a realização dos objetivos associados aos processos organizacionais;
- IV – análise de riscos: identificação das possíveis causas, consequências e os controles existentes para prevenir a ocorrência de riscos e diminuir o impacto de suas consequências;
- V – avaliação de riscos: identificação de quais riscos necessitam de tratamento e qual a prioridade para a implementação do tratamento;
- VI – tratamento de riscos: definição das opções de 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;
- VII – monitoramento e análise crítica: verificação e supervisão crítica contínua, visando identificar mudanças no desempenho requerido ou esperado para determinar a adequação, suficiência e eficácia da gestão de riscos; e
- VIII – registro e relato: atividades referentes ao registro documental e relato das atividades por meio de mecanismos apropriados para fornecer informações para tomada de decisão.

A metodologia de Gestão de Riscos da FUNECE é orientada a processo organizacional e obedece a um modelo de aplicação descentralizado. Com isso, as áreas de atuação operacional podem executar o gerenciamento de riscos em processos sob sua responsabilidade, desde que



obedecidas às diretrizes e orientações apresentadas neste documento. O resultado desse processo deve ser informado à área de atuação tática do órgão ou entidade, que o reportará à área de atuação estratégica.

6. DOS PROCESSOS DE GESTÃO DE RISCOS

6.1. SELEÇÃO DO PROCESSO ORGANIZACIONAL

Nesta primeira etapa, os gestores da FUNECE deverão:

- Selecionar os processos organizacionais que serão objeto do processo de gerenciamento de riscos, de acordo com o estabelecido no §2º, do art. 6º, do Decreto nº 33.805, de 09 de novembro de 2020, que estabelece a Política de Gestão de Riscos - PGR (preferencialmente os processos organizacionais mais críticos); e
- Identificar os responsáveis por cada processo organizacional selecionado, com auxílio da área de atuação tática.

O responsável pelo processo organizacional será responsável pelo seu gerenciamento de riscos e implementará as respostas aos riscos e as medidas de tratamento e controle definidas para o processo organizacional sob sua responsabilidade.

6.2. ESTABELECIMENTO DO CONTEXTO

A análise do contexto consiste em compreender o ambiente externo e interno no qual o objeto de gestão de riscos se encontra inserido e em identificar parâmetros e critérios a serem considerados no processo de gestão de riscos. Para tanto, é necessário avaliar informações sobre documentos, leis, normativos, planos estratégicos, políticas e cenários.

Nesta etapa, a área de atuação operacional, auxiliada pela área de atuação tática, deverá identificar, pelo menos:

- Descrição resumida do processo organizacional. A descrição é um breve relato sobre o processo que permite compreender o seu fluxo, a relação entre os atores envolvidos e os resultados esperados;
- Área responsável pelo processo organizacional;
- Ciclo médio do processo organizacional (em dias);
- Sistemas tecnológicos que apoiam o processo organizacional;
- Partes interessadas no processo organizacional, podendo ser internas ou externas;
- Fluxo (mapa) do processo organizacional;
- Objetivos do processo organizacional. É importante apontar quais objetivos são alcançados pelo processo organizacional. Se possível, devem ser indicados o objetivo geral e os objetivos específicos do processo, considerando perspectivas estratégicas, temporais, relacionais, financeiras, orçamentárias, metas, entre outras. Para identificação dos objetivos, pode-se buscar responder à questão “O que deve ser atingido nas diversas dimensões para se concluir que o processo ocorreu com sucesso?”;
- Relação de objetivos estratégicos da organização alcançados pelo processo;
- Justificativa para o gerenciamento de riscos no processo organizacional. Apresentar os motivos que levaram a implementar o gerenciamento de riscos no processo organizacional. A



criticidade do processo organizacional que impacta diretamente no atingimento dos objetivos estratégicos pode ser uma das justificativas para gerenciá-lo;

- Leis e regulamentos relacionados ao processo organizacional;
- Informações sobre o contexto externo do processo organizacional, considerando cenário atual ou futuro, oportunidades e ameaças relacionadas, percepções das partes interessadas externas e outros fatos relevantes;
- Informações sobre o contexto interno do processo organizacional, considerando políticas, objetivos, diretrizes e estratégias que o impactam, forças e fraquezas relacionadas, percepções das partes interessadas internas, principais ocorrências de problemas e outros fatos relevantes;
- Periodicidade máxima do ciclo do processo de gerenciamento de riscos (inciso V do art. 10, do Decreto nº 33.805, de 09 de novembro de 2020, que estabelece a Política de Gestão de Riscos - PGR). A área deve propor qual o prazo necessário para a realização de novo processo de gerenciamento de riscos no processo organizacional. O ciclo de revisão do processo de gerenciamento de riscos de processos organizacionais deve ocorrer entre 1 e 2 anos;
- Apetite a risco da área para o processo organizacional, caso seja diferente do proposto neste documento (quadro 6). O apetite a risco é o nível de risco que uma organização está disposta a aceitar.

6.3. IDENTIFICAÇÃO DOS RISCOS

Considerando o resultado da etapa de Entendimento do Contexto, o fluxo do processo organizacional, e a partir de sua experiência, a área de atuação operacional, com auxílio da área de atuação tática, deve construir uma lista abrangente de eventos que podem evitar, atrasar, prejudicar ou impedir o cumprimento dos objetivos do processo organizacional ou das suas etapas críticas (eventos de risco ou riscos). Tal atribuição é um processo iterativo, dinâmico e que não se encerra, uma vez que as atividades estão constantemente sendo aprimoradas e os cenários a que essas atividades ou processos estão submetidos estão constantemente mudando e sendo aprimorados, o mesmo ocorrendo com os seus controles internos.

Os riscos podem ser identificados a partir de perguntas, como:

- 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, e, para tanto, podem ser utilizadas as seguintes questões:

- O evento é um risco que pode comprometer claramente um objetivo do processo organizacional?



- O evento é um risco ou uma falha no desenho do processo organizacional?
- À luz dos objetivos do processo organizacional, o evento identificado é um risco ou uma causa para um risco?
- O evento é um risco ou uma fragilidade em um controle para tratar um risco do processo organizacional?

6.4. ANÁLISE DE RISCOS

A análise de riscos visa a promover o entendimento do nível de risco e de sua natureza, identificar suas possíveis causas e consequências e os controles existentes para prevenir sua ocorrência e diminuir o impacto de suas consequências.

Para eventos identificados como riscos do processo organizacional (tópico 6.3), a área de atuação operacional, com auxílio da área de atuação tática, deve indicar:

- Etapa e objetivo do processo organizacional que são impactados pelo risco;
- Categoria do risco, dentre as definidas para o órgão ou entidade:
- Operacional: eventos que podem comprometer as atividades do órgão ou entidade, normalmente associados a falhas, deficiências ou inadequação de processos internos, pessoas, infraestrutura e sistemas;
- Legal: eventos derivados de alterações legislativas ou normativas que podem comprometer as atividades do órgão ou entidade;
- Financeiro/orçamentário: eventos que podem comprometer a capacidade do órgão ou entidade 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 à corrupção, fraudes, irregularidades e/ou desvios éticos e de conduta que podem comprometer os valores e padrões preconizados pelo órgão ou entidade e a realização de seus objetivos.
- Causas do risco: motivos que podem promover a ocorrência do risco;
- Consequências do risco: resultados provocados pelo risco que afetam os objetivos do processo organizacional;
- 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 organizacional;
- 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 especial; procedimento apuratório.

NOTA 01: Análise de riscos

A análise de riscos pode ser realizada em diversos momentos, tais como no início de um novo projeto como parte da gestão contínua, ou como um estudo do que pode ocorrer após os riscos terem sido tratados. Normalmente, a análise verifica e compara o nível atual de riscos com os controles existentes.



O Apêndice I deste documento traz o modelo de planilha para o registro de informações produzidas na etapa de Identificação e Análise do Risco (colunas 1 a 8).

6.5. AVALIAÇÃO DE RISCOS

Nesta etapa, a área de atuação operacional, com auxílio da área de atuação tática, e a área de atuação estratégica deverão:

- Calcular o risco inerente, a partir de critérios de probabilidade e impacto (área de atuação operacional com auxílio da área de atuação tática);
- Classificar o risco dentro das faixas apresentadas no quadro 3 (área de atuação operacional com auxílio da área de atuação tática);
- Avaliar a eficácia dos controles internos existentes, em relação aos objetivos do processo organizacional (área de atuação estratégica);
- Calcular o nível de risco residual (área de atuação operacional com auxílio da área de atuação tática).

NOTA 02: Risco Inerente e risco residual

Risco inerente é o risco a que uma organização está exposta sem considerar quaisquer medidas de controle que reduzam ou possam reduzir a probabilidade de sua ocorrência ou de seu impacto.

Risco residual é o risco a que uma organização está exposta após a implementação de medidas de controle para o tratamento do risco.

Os quadros 1 e 2 trazem as escalas de probabilidade e impacto, respectivamente:

Quadro 1: Escala de Probabilidade

PROBABILIDADE	DESCRIÇÃO DA PROBABILIDADE, DESCONSIDERANDO OS CONTROLES	PESO
Muito baixa	Improvável (Em situações excepcionais, o evento poderá até ocorrer, mas nada nas circunstâncias indica essa possibilidade).	1
Baixa	Rara.(De forma inesperada ou casual, o evento poderá ocorrer, pois as circunstâncias pouco indicam essa possibilidade).	2
Média	Possível (De alguma forma, o evento poderá ocorrer, pois as circunstâncias indicam moderadamente essa possibilidade).	5
Alta	Provável (De forma até esperada, o evento poderá ocorrer, pois as circunstâncias indicam fortemente essa possibilidade).	8
Muito Alta	Praticamente certa (De forma, inequívoca, o evento	10

	ocorrerá pois, as circunstâncias indicam claramente essa possibilidade).	
--	--	--

Quadro 2: Escala de Impacto

IMPACTO	DESCRIÇÃO DO IMPACTO NOS OBJETIVOS (ESTRATÉGICOS, OPERACIONAIS, DE INFORMAÇÃO/COMUNICAÇÃO/ DIVULGAÇÃO OU DE CONFORMIDADE) DO PROCESSO ORGANIZACIONAL, CASO O EVENTO OCORRA	PESO
Muito baixa	Mínimo impacto nos objetivos do processo organizacional.	1
Baixa	Pequeno impacto nos objetivos do processo organizacional.	2
Médio	Moderado impacto nos objetivos do processo organizacional, porém recuperável.	5
Alto	Significativo impacto nos objetivos do processo organizacional, de difícil reversão.	8
Muito Alto	Catastrófico impacto nos objetivos do processo organizacional, de forma irreversível.	10

6.5.1. CÁLCULO DO RISCO INERENTE

A multiplicação entre os valores de probabilidade (quadro 1) e impacto (quadro 2) define o nível do risco inerente que, como citado na Nota 02, é o nível do risco sem considerar quaisquer controles que reduzem ou podem reduzir a probabilidade da sua ocorrência ou do seu impacto.

$$RI = NP \times NI$$

Em que:

RI = nível do risco inerente

NP = nível de probabilidade do risco

NI = nível de impacto do risco

6.5.2. CLASSIFICAÇÃO DO RISCO INERENTE DENTRO DE FAIXAS DE RISCO

A partir do resultado do cálculo feito no tópico 6.5.1., o risco pode ser classificado dentro das seguintes faixas:

Quadro 3: Classificação do Risco

Classificação	Faixa
Risco Baixo – RB	0 - 9,99



Risco Médio	10 - 39,99
Risco Alto – RA	40 - 79,99
Risco Extremo – RE	80 - 100

A seguinte matriz apresenta os possíveis resultados da combinação das escalas de probabilidade e impacto.

Quadro 4: Matriz de Riscos

IMPACTO	Muito Alto 10	10 RM	20 RM	50 RA	80 RE	100 RE
	Alto 8	8 RB	16 RM	40 RA	64 RA	80 RE
	Médio 5	5 RB	10 RM	25 RM	40 RA	50 RA
	Baixo 2	2 RB	4 RB	10 RM	16 RM	20 RM
	Muito Baixo 1	1 RB	2 RB	5 RB	8 RB	10 RM
		Muito Baixa 1	Baixa 2	Média 5	Alta 8	Muito Alta 10
		PROBABILIDADE				

Fonte: Portaria CGE nº 05/2021

6.5.3. AVALIAÇÃO DA EFICÁCIA DOS CONTROLES INTERNOS EXISTENTES

Após a classificação do risco (tópico 6.5.2), a área de atuação estratégica deve avaliar a eficácia dos controles internos existentes, em relação aos objetivos do processo organizacional. Para isso, é necessário verificar se os controles apontados durante a etapa de Análise dos Riscos (tópico 6.4) têm auxiliado no tratamento adequado desses riscos. O quadro 5 mostra os níveis de avaliação da eficácia dos controles existentes:

Quadro 5: Níveis de Avaliação dos Controles Internos Existentes

NÍVEL DE EFICÁCIA DOS CONTROLES INTERNOS	DESCRIÇÃO	FATOR DE AVALIAÇÃO DOS CONTROLES
Inexistente	Controles inexistentes, mal desenhados ou mal implementados, isto é, não funcionais.	1



Fraco	Controles têm abordagens ad hoc ¹ , tendem a ser aplicados caso a caso, a responsabilidade é individual, havendo elevado grau de confiança no conhecimento das pessoas.	0,8
Mediano	Controles implementados, mitigam alguns aspectos do risco, mas não contemplam todos os aspectos relevantes do risco devido a deficiências no desenho ou nas ferramentas utilizadas.	0,6
Satisfatório	Controles implementados e sustentados por ferramentas adequadas e, embora passíveis de aperfeiçoamento, mitigam o risco satisfatoriamente	0,4
Forte	Controles implementados podem ser considerados a “melhor prática”, mitigando todos os aspectos relevantes do risco.	0,2

6.5.4. CÁLCULO DO RISCO RESIDUAL

Após a avaliação dos controles existentes (tópico 6.5.3), a área de atuação operacional deverá calcular o risco residual. Como citado na Nota 02, o risco residual é o risco a que uma organização está exposta após a implementação de medidas de controle para o tratamento do risco.

O nível de risco residual corresponde ao valor final da multiplicação entre o valor do risco inerente e o fator de avaliação dos controles internos existentes.

$$RR = RI \times FC$$

Em que:

RR = nível do risco residual

RI = nível do risco inerente

FC = fator de avaliação dos controles existentes

O valor de risco residual pode fazer com que o risco se enquadre em uma faixa de classificação de risco (quadro 3) diferente da faixa definida para o risco inerente.

O Apêndice I deste documento traz o modelo de planilha para o registro de informações produzidas na etapa de Avaliação de Riscos (colunas 9 a 13).

NOTA 03: Revisão do processo organizacional em novo ciclo do processo de gerenciamento de riscos.

¹Controle ad-hoc: baseia-se na utilização de mecanismos não formais que promovem o controle, normalmente em ambientes muito dinâmicos e de grande complexidade.



De forma geral, nos ciclos seguintes do processo de gerenciamento de riscos do processo organizacional, deve-se considerar o nível de risco inerente calculado no 1º ciclo e reavaliar os controles para o cálculo do risco residual.

A comparação entre os níveis de riscos residuais de diferentes ciclos objetiva identificar se os controles definidos nos Planos de Tratamento estão sendo eficazes para tratar o risco.

7. DO TRATAMENTO DE RISCOS

7.1. PRIORIZAÇÃO DOS RISCOS PARA TRATAMENTO

Nesta etapa, a área de atuação operacional, com auxílio da área de atuação tática, identificará quais riscos serão priorizados para tratamento. Para isso, devem ser considerados os valores dos níveis de riscos residuais calculados na etapa anterior (tópico 6.5.4).

A faixa de classificação do risco residual deve ser considerada para a definição da atitude da área de atuação operacional em relação à priorização para tratamento. O quadro 6 mostra, por faixa de classificação, quais ações devem ser adotadas em relação ao risco e suas exceções.

Quadro 6: Atitude perante o risco para cada classificação

FAIXA DE CLASSIFICAÇÃO DO RISCO RESIDUAL	AÇÃO NECESSÁRIA	EXCEÇÃO
Risco Baixo	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.	Caso o risco seja priorizado para implementação de medidas de tratamento, essa priorização deve ser justificada pelo responsável pelo processo.
Risco Médio	Nível de risco dentro do apetite a risco. Geralmente nenhuma medida especial é necessária, porém requer atividades de monitoramento específicas e atenção da área na manutenção de respostas e controles para manter o risco nesse nível, ou reduzi-lo sem custos adicionais.	Caso o risco seja priorizado para implementação de medidas de tratamento, essa priorização deve ser justificada pelo responsável pelo processo.
Risco Alto	Nível de risco além do apetite a risco. Qualquer risco nesse nível deve ser comunicado ao gestor da área e ter uma ação tomada em período determinado. Postergação de medidas só com autorização do gestor da área em comum acordo com	Caso o risco não seja priorizado para implementação de medidas de tratamento, a não priorização deve ser justificada pelo responsável



	responsável pelo processo.	pelo processo.
Risco Extremo	Nível de risco muito além do apetite a risco. Qualquer risco nesse nível deve ser comunicado à área de atuação estratégica e ao responsável pelo processo e ter uma resposta imediata. Postergação de medidas só com autorização da área de atuação estratégica.	Caso o risco não seja priorizado para implementação de medidas de tratamento, a não priorização deve ser justificada pelo responsável pelo processo e aprovada pela área de atuação estratégica

NOTA 04: Sobre o Apetite a Risco do Processo Organizacional

Segundo o inciso XIII, do art. 3º, do Decreto nº 33.805, de 09 de novembro de 2020, que estabelece a Política de Gestão de Riscos - PGR, apetite a risco é o “nível de risco que uma organização está disposta a aceitar”.

Caso o órgão ou entidade opte por estabelecer apetite a risco diferente do proposto nesta metodologia, a área de atuação operacional deverá defini-lo com auxílio da área de atuação tática.

Neste caso, é importante que o apetite a risco seja estabelecido no início do processo de gerenciamento de riscos e aprovado pela área de gestão estratégica.

Uma vez definido, a organização declara que:

- todos os riscos cujos níveis estejam dentro da(s) faixa(s) de apetite a risco podem ser aceitos, e uma possível priorização para tratamento deve ser justificada;
- todos os riscos cujos níveis estejam fora da(s) faixa(s) de apetite a risco serão tratados e monitorados, e uma possível falta de tratamento deve ser justificada.

O Apêndice I deste documento traz o modelo de planilha para o registro de informações produzidas na etapa de Priorização dos Riscos para Tratamento (colunas 14 a 16).

8. DA DEFINIÇÃO DE RESPOSTAS AOS RISCOS

Esta etapa objetiva definir as opções de tratamento para os riscos priorizados na etapa anterior (tópico 7.1).

Cada risco priorizado deve ser relacionado a uma opção de tratamento. A escolha da opção depende do nível do risco, conforme apresenta o quadro 7.

Quadro 7: Opções de tratamento do risco

OPÇÃO DE TRATAMENTO	DESCRIÇÃO
Mitigar	Um risco normalmente é mitigado quando é classificado como “Alto” ou “Extremo”. A implementação de controles, neste caso, apresenta



	um custo/benefício adequado. Mitigar o risco significa implementar controles que possam diminuir as causas ou as consequências dos riscos, identificadas na etapa de Identificação e Análise de Riscos.
Compartilhar	Um risco normalmente é compartilhado quando é classificado como “Alto” ou “Extremo”, mas a implementação de controles não apresenta um custo/benefício adequado. Pode-se compartilhar o risco por meio de terceirização ou apólice de seguro.
Evitar	Um risco normalmente é evitado quando é classificado como “Alto” ou “Extremo” e a implementação de controles apresenta um custo muito elevado, inviabilizando sua mitigação, ou não há entidades dispostas a compartilhar o risco. Evitar o risco significa encerrar o processo organizacional. Nesse caso, essa opção deve ser aprovada pela área de atuação estratégica.
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.

Se a opção de tratamento do risco for MITIGAR, devem ser definidas medidas de tratamento e controle para esse risco. Essas medidas devem ser capazes de diminuir os níveis de probabilidade e/ou de impacto do risco a um nível dentro ou mais próximo possível das faixas de apetite a risco (risco “Baixo” ou “Médio”).

9. DA DEFINIÇÃO DE MEDIDAS DE TRATAMENTO E CONTROLE E ELABORAÇÃO DO PLANO DE TRATAMENTO

A área de atuação operacional, com auxílio da área de atuação tática, elaborará um plano de ação – Plano de Tratamento – para a implementação das medidas de tratamento e controle dos riscos nos processos organizacionais objeto do gerenciamento de risco. Esse plano de tratamento deve conter, pelo menos:

- Evento de risco que se deseja tratar;
- Projeto ou ação que implementará um conjunto de medidas de tratamento e controle;
- Medida(s) de tratamento e controle contemplada(s) no projeto ou ação;
- Objetivos/benefícios esperados com a implementação da(s) medida(s) de tratamento e controle;
- Área organizacional responsável pela implementação da(s) medida(s) de tratamento e controle;
- Áreas organizacionais corresponsáveis pela implementação da(s) medida(s) de tratamento e controle, isto é, áreas envolvidas na implementação dessa(s) medida(s);
- Servidor responsável pela implementação das medidas de tratamento e controle, que também deverá monitorar e reportar sua evolução;



- Breve descrição sobre a implementação: como será implementada a medida de tratamento e controle;
- Custo estimado para a implementação;
- Data prevista para início da implementação;
- Data prevista para o término da implementação;
- Situação/acompanhamento da implementação das medidas de tratamento e controle contempladas no projeto ou ação.

Se as iniciativas definidas no Plano de Tratamento envolverem mais de uma área, o responsável pelo processo de gerenciamento de riscos deve encaminhar a proposta de plano para que essas áreas validem as iniciativas de que participarem.

Após sua elaboração, o Plano de Tratamento deve ser aprovado pela área de atuação estratégica.

NOTA 05: Proposição de novos controles

É importante que, em uma primeira abordagem da elaboração do Plano de Tratamento, avalie-se a necessidade de melhorar ou extinguir controles já existentes. 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 Apêndice II deste documento traz um modelo de Plano de Tratamento.

10. DA VALIDAÇÃO DO RESULTADO DO PROCESSO DE GERENCIAMENTO DE RISCOS

O resultado do processo de gerenciamento de riscos (entendimento do contexto, identificação de riscos, análise de riscos, avaliação de riscos, tratamento de riscos e definição de respostas aos riscos) de cada processo organizacional selecionado deve ser avaliado e validado pela área de atuação estratégica do órgão ou entidade.

Após a validação do resultado, a área de atuação estratégica deve:

- Encaminhar esse resultado às áreas do órgão ou entidade para conhecimento;
- Incluir as iniciativas previstas no Plano de Tratamento nas metas e atividades das respectivas áreas;
- Encaminhar o Plano de Tratamento aprovado às áreas corresponsáveis pelas iniciativas para que estas também incluam as ações em suas metas e atividades.

11. DA IMPLEMENTAÇÃO DO PLANO DE TRATAMENTO

A implementação do Plano de Tratamento envolve a participação da área responsável pelo processo organizacional e das áreas corresponsáveis, caso existam outras áreas envolvidas na implementação das medidas de tratamento e controle.

A responsabilidade primária pelo Plano de Tratamento permanece com a área responsável pelo processo organizacional. No Plano de Tratamento, deve ser indicado servidor responsável pela implementação das medidas de tratamento e controle, que também deverá monitorar e reportar a evolução destas.

12. DA COMUNICAÇÃO E CONSULTA

Durante todas as etapas do processo de gerenciamento de riscos, é importante a comunicação entre as partes interessadas.

O Decreto nº 33.805, de 09 de novembro de 2020, que estabelece a Política de Gestão de Riscos - PGR prevê em seu art. 9º, §2º:

“As áreas de atuação responsáveis pelo gerenciamento de riscos deverão manter fluxo regular e constante de comunicação.”

Dentro do escopo de um processo de gerenciamento de riscos, deve ser observada a Matriz de Responsabilidade - RACI apresentada no quadro 8.

A Matriz de Responsabilidade - RACI define as atribuições das áreas e atores dentro do processo de gerenciamento de riscos na organização. São elementos da Matriz RACI:

- Responsável (R): quem executa a atividade;
- Autoridade (A): quem aprova a tarefa ou produto. Pode delegar a função, mas mantém a responsabilidade;
- Consultado (C): quem pode agregar valor ou é essencial para a implementação;
- Informado (I): quem deve ser notificado de resultados ou ações tomadas, mas não precisa se envolver na decisão.

Durante as etapas do processo de gerenciamento de riscos do órgão ou entidade é importante que a comunicação observe os agentes ou áreas apontadas como consultados ou informados na Matriz RACI do quadro 8.

Quadro 8: Matriz RACI para o processo de gerenciamento de riscos no órgão ou entidade

Atividades	ÁREA DE ATUAÇÃO ESTRATÉGICA	ÁREA DE ATUAÇÃO TÁTICA	ÁREA DE ATUAÇÃO OPERACIONAL	GESTOR DA ÁREA RESPONSÁVEL PELO GERENCIAMENTO DE RISCOS	RESPONSÁVEL PELO GERENCIAMENTO PELO RESPONSÁVEL PELO GERENCIAMENTO DE RISCOS	COLABORADORES DO ÓRGÃO OU ENTIDADE
Selecionar processos organizacionais	A	I	C	R	C	I
Identificar os responsáveis pelos processos organizacionais	I	I	C	R	C	I
Definir os níveis de apetite a riscos dos processos organizacionais	A	C	R	C	C	I



UNIVERSIDADE
ESTADUAL DO CEARÁ



GOVERNO DO
ESTADO DO CEARÁ

Secretaria da Ciência, Tecnologia
e Educação Superior

selecionados caso sejam diferentes dos sugeridos nesta metodologia							
Realizar o Entendimento do Contexto	I	C	R	C	A	I	
Realizar a identificação dos Riscos	I	C	R	C	A	I	
Realizar a análise dos riscos	I	C	R	C	A	I	
Realizar a avaliação dos riscos – calcular risco inerente classificar o risco calcular risco residual	I	C	R	C	A	I	
Realizar a avaliação dos riscos – avaliar a eficácia dos controles internos existentes em relação aos objetivos do processo organizacional	R	I	C	C	A	I	
Realizar a identificação dos riscos que serão priorizados para tratamento	A	C	R	C	C	I	
Definir as respostas aos riscos	A	C	R	C	C	I	
Elaborar o Plano de Tratamento (medidas de tratamento e	A	C	R	C	C	I	

Universidade Estadual do Ceará - Uece

Avenida Silas Munguba, 1700 Campus Itaperi – CEP: 60.714.903

Fortaleza-CE • Telefone: (85) 3101.XXXX



controle a serem
implementadas)

Implementar o Plano de Tratamento	I	I	R	C	C	I
Realizar monitoramento	I	R	R	R	R	I
Realizar análise crítica dos níveis de riscos e da efetividade das medidas de tratamento e controle implementadas	I	R	C	C	C	I
Avaliar o desempenho do processo de gerenciamento de riscos e fortalecer a aderência dos processos organizacionais à conformidade normativa	R	C	C	C	C	I
Documentar e relatar cada etapa do processo de gerenciamento de riscos - Registro e Relato	I	R	C	C	C	I

13. DO MONITORAMENTO E ANÁLISE CRÍTICA

O monitoramento no âmbito do processo de gerenciamento de riscos deve ser realizado pela área de atuação operacional responsável pelo processo organizacional, em conjunto com a área de atuação tática, de forma a:

- Garantir que os controles sejam eficazes e eficientes;
- Analisar as ocorrências dos riscos;



- Detectar mudanças que possam requerer revisão dos controles e/ou do Plano de Tratamento;
- Identificar os riscos emergentes.

O Decreto nº 33.805, de 09 de novembro de 2020, que estabelece a Política de Gestão de Riscos - PGR, em seu art. 13, também delega a todos os servidores do órgão ou entidade a responsabilidade de comunicar a situação dos níveis dos riscos e da efetividade das medidas de controles implementadas:

Art. 13. Compete a todos os servidores do órgão ou entidade comunicar a situação dos níveis de riscos e da efetividade das medidas de controles implementadas nos processos organizacionais em que estiverem envolvidos ou que tiverem conhecimento.

Parágrafo único. Caso sejam identificadas mudanças ou fragilidades nos processos organizacionais, o servidor deverá reportar imediatamente o fato ao responsável pelo gerenciamento de riscos do processo em questão, que reportará o fato à instância de atuação tática do órgão ou entidade.

Mudanças identificadas durante o monitoramento devem ser encaminhadas à instância de atuação tática do órgão ou entidade, a quem compete supervisionar os resultados de todos os processos de gerenciamento de riscos já realizados nos processos organizacionais do órgão ou entidade.

Convém que o monitoramento e a análise crítica ocorram em todas as etapas do processo de gerenciamento de riscos. Incluem planejamento, coleta e análise de dados e informações, registro de resultados e fornecimento de retorno (feedback).

14. DO REGISTRO E RELATO

É importante documentar e relatar cada etapa do processo de gerenciamento de riscos. O Registro e o Relato visam:

- Comunicar as atividades e os resultados do gerenciamento de riscos em toda a organização;
- Fornecer informações para tomada de decisão;
- Aperfeiçoar o processo de gerenciamento de riscos;
- Auxiliar a interação entre as partes interessadas, incluindo aquelas com responsabilidade e com responsabilização por atividades de gerenciamento de riscos.

A área responsável pelo processo organizacional disponibilizará as informações adequadas quanto ao gerenciamento de riscos dos processos sob sua responsabilidade a todos os níveis do órgão ou entidade e demais partes interessadas.

Cabe à instância de atuação tática requisitar aos responsáveis pelo gerenciamento de riscos dos processos organizacionais as informações necessárias para a consolidação dos dados e a elaboração dos relatórios gerenciais.

14.1. REGISTRO

É importante que as decisões relativas à criação, retenção e manuseio de informações documentadas levem em consideração o seu uso, a sensibilidade da informação e os contextos interno e externo.

Frequentemente, a documentação do processo de gerenciamento de riscos é exigida para demonstrar conformidade com requisitos legais ou para mostrar a devida diligência, devendo ser composta, preferencialmente, por:

- A descrição do contexto interno e externo;
- Papéis, responsabilidades e responsabilizações pelo gerenciamento de riscos na organização;
- O plano de comunicação e consulta;
- Procedimento sobre o processo de gerenciamento de riscos, incluindo os critérios de risco da organização, planos de tratamento de riscos, entre outras informações documentadas nas diversas etapas do processo.

14.2. RELATO

O Relato é parte integrante da governança do órgão e entidade. Tem como objetivo melhorar a qualidade da comunicação entre as partes interessadas e auxiliar a direção superior na tomada de decisões.

Diversos fatores devem ser considerados para que o relato alcance seu objetivo, dentre eles:

- Identificação das partes interessadas e suas necessidades específicas de informação;
- Custo, frequência e pontualidade do relato;
- Método de relato;
- Pertinência da informação para o alcance dos objetivos organizacionais e para a tomada de decisão.

15. DAS CONSIDERAÇÕES FINAIS

Todos os agentes públicos em exercício na FUNECE, 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 Decreto nº 33.805/2020.

O fortalecimento da integridade institucional da FUNECE deverá ser promovido por todos e para todos para que as decisões sejam baseadas no autoconhecimento e diagnose de

vulnerabilidades. Sabe-se que há uma arma poderosa para proporcionar isso, que é precisamente o gerenciamento de riscos.

Pretende-se, com a elaboração e publicação deste manual, instruir e colaborar de forma eficaz, efetiva e eficiente com a implantação de boas práticas de Gestão de Governança, Integridade, Gestão de Riscos e Controles Internos e para a tomada de decisões dos servidores, colaboradores e gestores da Fundação Universidade Estadual do Ceará.

REFERÊNCIAS

ABNT – ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO 31000:2018. Gestão de Riscos – Diretrizes. Rio de Janeiro, 2018

BRASIL. Ministério da Educação. Manual de Gestão de Riscos – MEC - 2021. Disponível em: https://www.gov.br/mec/pt-br/media/acao_informacao/copy_of_pdfManualdeGestaodeRiscosdoMEC.pdf Acessado em 28 de novembro de 2023.

CEARA. DECRETO Nº33.805, 09 de novembro de 2020. INSTITUI A POLÍTICA DE GESTÃO DE RISCOS DO PODER EXECUTIVO DO ESTADO DO CEARÁ.

CEARA. PORTARIA Nº05/2021- CGE/CE. INSTITUI A METODOLOGIA DE GERENCIAMENTO DE RISCOS DO PODER EXECUTIVO DO ESTADO DO CEARÁ.

COSO. *Committee of Sponsoring Organizations of the Treadway Commission*. Gerenciamento de Riscos Corporativos – Estrutura Integrada. 2007. Tradução: Instituto dos Auditores Internos do Brasil (Audibra) e *Pricewaterhouse Coopers Governance, Risk and Compliance*, Estados Unidos da América, 2007.

TCE-PR – TRIBUNAL DE CONTAS DO ESTADO DO PARANÁ. Manual de Gestão de Riscos. Curitiba: TCE-PR, 2019

APÊNDICE I

METODOLOGIA DE GERENCIAMENTO DE RISCOS DO PODER EXECUTIVO DO ESTADO DO CEARÁ



Identificação e Análise do Risco								Avaliação dos Riscos					Priorização dos Riscos			Resposta aos Riscos		
Processo/ Etapa (1)	Objetivo (2)	Evento de Risco (3)	Categoria (4)	Causa (5)	Consequência (6)	Preventivo (7)	Controles		Probabilidade (9)	Impacto (10)	Risco Inerente (11)	Avaliação dos Controles (12)	Risco Residual (13)	Classifi- cação (14)	Prioriza- ção (15)	Justifica- tiva (16)	Opção de tratamento (17)	Proposta de projeto ou ação para tratamento e controle do risco (18)
							Atenuação e recuperação (8)											

Fonte: Portaria CGE nº 05/2021

APÊNDICE II
METODOLOGIA DE GERENCIAMENTO DE RISCOS DO PODER EXECUTIVO DO ESTADO DO CEARÁ

PLANO DE TRATAMENTO DOS EVENTOS DE RISCO											
Evento de risco (3)	Projeto ou ação para tratamento e controle do risco (18)	Medida de Tratamento e controle	Objetivos/benefícios esperados com a medida de tratamento e controle	Área organizacional responsável pela implementação da medida de tratamento e controle	Área(s) corresponsável(is) pela implementação da medida de tratamento e controle	Servidor responsável pela implementação da medida de tratamento e controle	Descrição sobre a implementação da medida de tratamento e controle (como será implementada)	Custo estimado para implementação	Datas previstas		Situação/Acompanhamento da implementação da medida de tratamento e controle
									Início da implementação	Término da implementação	

Fonte: Portaria CGE nº 05/2021