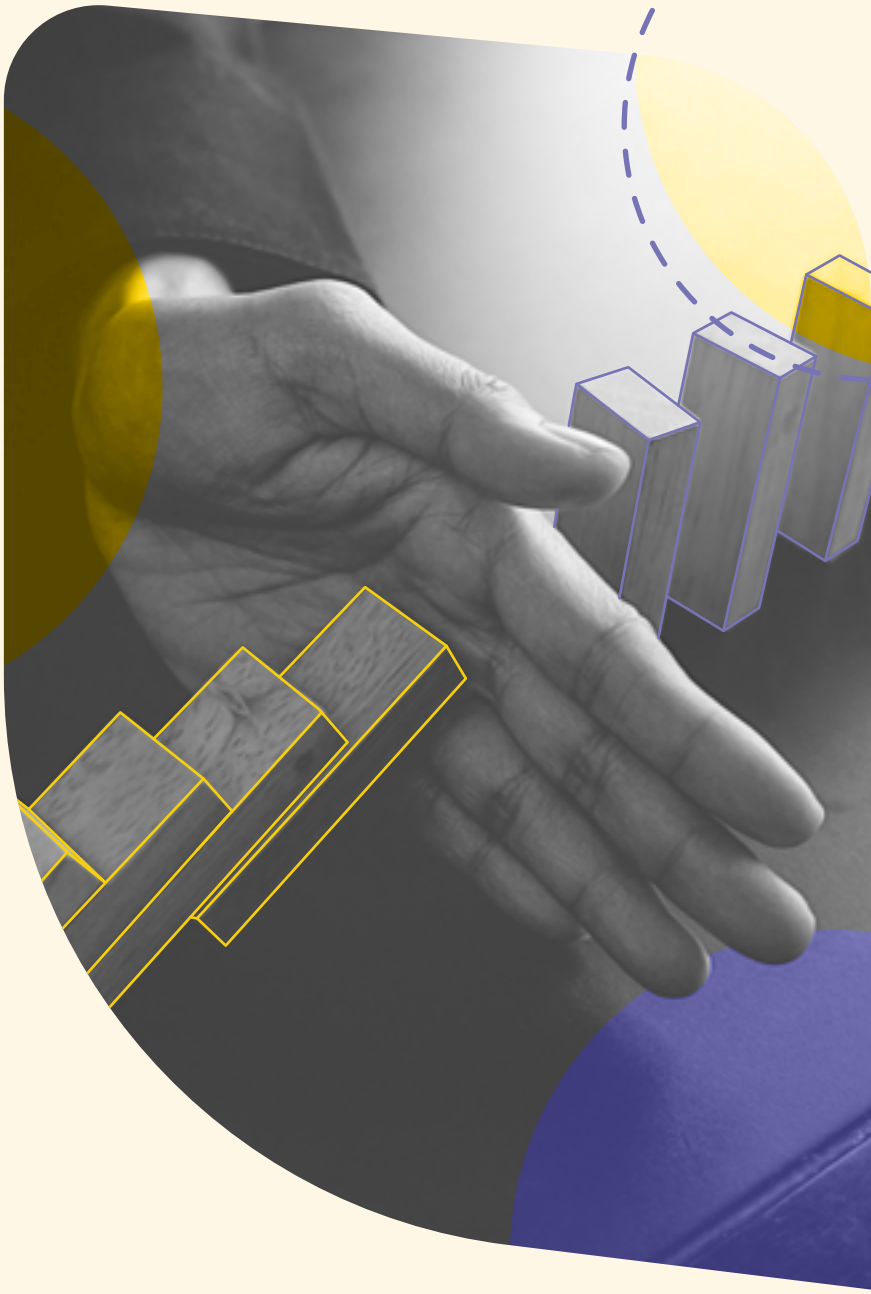


Manual de
Gestão de Riscos e Controles Internos

Escola de Saúde Pública do Ceará

Ceará
Governo do Estado
Secretaria da Saúde

Escola de Saúde Pública do Ceará

CEARÁ
GOVERNO DO ESTADO
SECRETARIA DA SAÚDE

Manual de
Gestão de Riscos e Controles Internos

Este manual foi elaborado com base no *"**Guia Prático para Implementação da Gestão de Riscos no Poder Executivo Estadual do Ceará**"* (CGE/2024), adaptado ao contexto da ESP/CE e redigido segundo as orientações da Política Estadual de Linguagem Simples (Lei nº 18.246, de 01 de dezembro de 2022).

Fortaleza-CE
2025

Escola de Saúde Pública do Ceará

CEARÁ
GOVERNO DO ESTADO
SECRETARIA DA SAÚDE

Missão, Visão e Valores

Escola de Saúde Pública do Ceará
Paulo Marcelo Martins Rodrigues (ESP/CE)

2024 - 2027

QUEM SOMOS E ONDE VAMOS CHEGAR

Missão

Promover o desenvolvimento de excelência da força de trabalho em Saúde por meio da Educação Permanente, apoiado pela ciência, inovação e tecnologia, visando o fortalecimento do SUS e à melhoria da qualidade de vida das pessoas.

Visão

Até 2027, ser reconhecida pela sociedade como uma escola de saúde pública de excelência na formação e qualificação da força de trabalho para o Sistema Único de Saúde (SUS).

Valores

Comprometimento com o SUS;
Eficiência e sustentabilidade;
Ética;
Humanização;
Inclusão e diversidade;
Inovação e conhecimento;
Transparência;
Valorização das pessoas.

Mapa Estratégico da ESP/CE
Clique e acesse

GOVERNADOR DO ESTADO DO CEARÁ
Elmano de Freitas da Costa

VICE-GOVERNADORA DO ESTADO DO CEARÁ
Jade Afonso Romero

SECRETÁRIA DA SAÚDE DO ESTADO DO CEARÁ
Tânia Mara Silva Coelho

SUPERINTENDENTE DA ESCOLA DE SAÚDE PÚBLICA DO CEARÁ
Luciano Pamplona de Góes Cavalcanti

COORDENADORA DA ASSESSORIA DE DESENVOLVIMENTO INSTITUCIONAL E COMUNICAÇÃO
Geni Carmem Clementino Alves

COORDENADORA DA ASSESSORIA JURÍDICA
Maria Elci Moreira Galvão

COORDENADORA DA ASSESSORIA DE CONTROLE INTERNO E OUVIDORIA
Dellane Emanuelle Pinheiro Gadelha Damasceno

COORDENADOR DA ASSESSORIA DE DESENVOLVIMENTO EDUCACIONAL
Henrique Luis do Carmo e Sá

DIRETORA DE PÓS-GRADUAÇÃO EM SAÚDE
Olivia Andrea Alencar Costa Bessa

DIRETORA DE EDUCAÇÃO PERMANENTE E PROFISSIONAL EM SAÚDE
Suzyane Cortês Barcelos

DIRETOR DE INOVAÇÃO, CIÊNCIA E TECNOLOGIA EM SAÚDE
Francisco Sales Ávila Cavalcante

DIRETORA ADMINISTRATIVA-FINANCEIRA
Selma Carvalho do Nascimento Aquino

GERENTE DE RESIDÊNCIA MÉDICA
Alciléa Leite de Carvalho

GERENTE DE RESIDÊNCIA MULTIPROFISSIONAL
Kellyane Munick Rodrigues Soares

GERENTE DE PÓS-GRADUAÇÃO EM SAÚDE
Lígia Lucena Gonçalves Medina

GERENTE DE EDUCAÇÃO PROFISSIONAL EM SAÚDE
Vanessa Alencar de Araújo

GERENTE DE EDUCAÇÃO PERMANENTE EM SAÚDE
Érika de Oliveira Nicolau

GERENTE DE PESQUISA EM SAÚDE
Zilvanir Fernandes de Queiroz

GERENTE DE INOVAÇÃO
Cristiane Buhamra Abreu

GERENTE FINANCEIRA
Julianne Débora Rebouças da Silva

GERENTE DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO
Irlene Alves Rodrigues

GERENTE DE GESTÃO DE PESSOAS
Leilanne Maria Costa Lima

GERENTE DE SELEÇÕES PÚBLICAS
Humberto Fontenelle de Albuquerque Neto

GERENTE ADMINISTRATIVO
Carlos Roberto Menescal Maia

GERENTE DA SECRETÁRIA ACADÊMICA
Ana Lúcia Barreto Xenofonte

Ficha Técnica

Manual de Gestão de Riscos e Controles Internos

Realização/Instituição Responsável

Escola de Saúde Pública do Ceará (ESP/CE)

Equipe Técnica

Elaboração

Janaina Silva Torres
Paulo Cesar Rodrigues Amoreira
Dellane Emanuelle Pinheiro Gadelha Damasceno
Hanna Rafaela de Lima Vieira

Apoio Técnico

Controladoria e Ouvidoria Geral do Estado do Ceará (CGE/CE)

Produção Editorial

Comunicação Institucional da ESP/CE

Diagramação

Rafael Medeiros Campos

Supervisão Técnica

Elon Nepomuceno

Imagens e Ilustrações

Freepik

Dados da Publicação

Fortaleza-CE • 2025

ESCOLA DE SAÚDE PÚBLICA DO CEARÁ PAULO MARCELO MARTINS RODRIGUES (ESP/CE)
Av. Antônio Justa, 3161, Meireles
Fortaleza-CE • CEP: 60.165-090
E-mail: esp@esp.ce.gov.br
/espceara
www.esp.ce.gov.br

Sumário

Apresentação

A Escola de Saúde Pública do Ceará (ESP/CE) reconhece a importância de ter uma gestão eficiente, transparente e alinhada às melhores práticas do setor público, usando formas de trabalho que ajudam a prevenir riscos, melhorar processos e tomar decisões com mais segurança.

Este Manual orienta gestores e equipes sobre como identificar, avaliar, tratar e monitorar riscos que possam atrapalhar os objetivos da instituição. Ele foi criado com base na **Política de Gestão de Riscos do Poder Executivo Estadual** (Decreto Estadual nº 33.805/2020), **Política de Gestão de Riscos da ESP/CE** (Portaria nº 33/2024) e na **Metodologia de Gerenciamento de Riscos do Poder Executivo do Estado do Ceará** (Portaria CGE nº 05/2021), entre outros, adaptados ao nosso contexto.

Este manual e toda a comunicação sobre gestão de riscos na ESP/CE seguem as diretrizes da **Política Estadual de Linguagem Simples**.

BOAS PRÁTICAS DE COMUNICAÇÃO

FRASES CURTAS

Use a ordem direta
(Sujeito > Verbo > Complemento).

ORGANIZAÇÃO VISUAL

Use títulos, listas, tabelas e fluxogramas para facilitar a leitura.

PALAVRAS CONHECIDAS

Evite termos técnicos, jargões ou siglas sem explicação.

TOM CORDIAL

A comunicação pública deve ser respeitosa e acessível.

Nosso objetivo principal é prevenir problemas e agir antes que eles ocorram, garantindo mais transparência e eficiência em nossas ações.

1. Objetivos do manual

Este manual tem como objetivos:

- **Fortalecer** a estrutura de controles internos da ESP/CE.
- **Garantir** eficácia, eficiência e transparência nos processos institucionais.
- **Prevenir** falhas, fraudes ou desperdícios que possam comprometer os resultados institucionais.
- **Promover** a cultura de integridade e responsabilidade na gestão pública, com foco em melhoria contínua.
- **Detalhar** a metodologia de gerenciamento de riscos adotada pela ESP/CE, tornando-a autoexplicativa.

2. Conceitos fundamentais

Quadro 1: Conceitos Fundamentais

Conceito	Conceito	Base Legal
Risco	É a possibilidade de um evento acontecer e afetar negativamente o alcance dos objetivos da ESP/CE.	Decreto Estadual nº 33.805/2020
Gestão de Risco	É o conjunto de ações coordenadas para definir a política e a metodologia de gerenciamento de riscos, e para aplicá-las na prática.	Decreto Estadual nº 33.805/2020
Gerenciamento de Risco	É a aplicação prática da metodologia, ou seja, o processo de identificar, analisar, avaliar, tratar e monitorar os riscos.	Portaria CGE nº 05/2021
Controle Interno	São as regras e procedimentos adotados para dar segurança de que os objetivos institucionais serão alcançados e os riscos serão gerenciados.	Portaria ESP/CE nº 33/2024

3. Controles Internos

O QUE SÃO E POR QUE SÃO IMPORTANTES?

A Gestão de Riscos e os Controles Internos andam sempre juntos. Os **Controles Internos** são as **medidas de segurança** que a ESP/CE usa para garantir que os riscos sejam mantidos sob controle e que os objetivos da Escola sejam alcançados.

O que são Controles Internos?

De forma simples, Controles Internos são o **conjunto de regras, procedimentos e ações** que existem dentro da ESP/CE para proteger a Escola e garantir que tudo funcione como planejado [1].

Eles incluem:

- **Regras e Procedimentos:** Como as tarefas devem ser feitas.
- **Diretrizes e Protocolos:** Os passos a seguir em situações específicas.
- **Rotinas de Sistemas:** As seguranças e verificações dentro dos sistemas de informática.
- **Conferências e Trâmites:** As checagens e aprovações de documentos e informações.

O objetivo principal dos Controles Internos é **mitigar os riscos**, ou seja, diminuir a chance de algo dar errado ou reduzir o impacto caso o erro aconteça [1].

Quem é responsável pelos Controles Internos?

Os Controles Internos são uma responsabilidade de **todos** [1]. Eles são operados por todos os servidores e agentes públicos que trabalham na ESP/CE, e fazem parte das atividades e tarefas diárias de cada um [1].

Referência:

[1] Art. 5º da Portaria ESP/CE nº 33/2024.

Características dos Controles Internos

Para serem eficazes, os Controles Internos devem ter as seguintes características:

Quadro 2: Conceitos Fundamentais

Característica	O que significa em linguagem simples
Efetivos e Consistentes	Devem ser adequados ao tipo de trabalho, à complexidade e ao risco das operações que estão sendo realizadas [1].
Contínuos	Não devem ser feitos apenas de vez em quando, mas sim de forma constante, integrados às atividades do dia a dia [2].
Integrados	Devem fazer parte dos planos, ações, políticas e sistemas da Escola, envolvendo o esforço de todos [2].
Sistematicamente avaliados	Devem ser checados e revisados sempre que necessário para garantir que continuem funcionando bem e sendo úteis [2].

Referências:

[1] Art. 5º da Portaria ESP/CE nº 33/2024.
[2] Art. 7º da Portaria ESP/CE nº 33/2024.

4. Princípios da Gestão de Riscos na ESP/CE

A gestão de riscos na ESP/CE é guiada pelos seguintes princípios:

Gráfico 1: Os 12 Princípios da Gestão de Riscos na ESP/CE

12 PRINCÍPIOS

da Política de Gestão de Riscos

1. Agrega e protege valor
2. É apoiada e gerenciada pela alta gestão e por todos da organização
3. É parte integrante dos processos organizacionais
4. Subsidia a tomada de decisões
5. Considera ameaças e oportunidades
6. É estruturada e processada de forma personalizada e proporcional aos contextos internos e externos
7. É baseada nas informações disponíveis, oportunas e claras para as partes interessadas
8. Considera fatores humanos e culturais
9. É sistemática, estruturada, abrangente e oportuna
10. É transparente e inclusiva
11. É dinâmica, iterativa e capaz de reagir a mudança
12. Fomenta a melhoria contínua da organização.

5. Estrutura de Governança e Responsabilidades

Conforme previsto no Capítulo V – Das Competências, Art.9º da Política de Gestão de Riscos da ESP/CE (Portaria Nº 33/2024), a governança da gestão de riscos, em sua estrutura formal, é composta por:

Quadro 3: Estrutura de Governança e Responsabilidades – Comitê de Governança

Nível Estratégico

Área de atuação estratégica: **Comitê de Governança**

	Papel na Gestão de Riscos
1	**Aprovar os processos** organizacionais selecionados para o gerenciamento de riscos;
2	**Definir as estratégias** de implementação do gerenciamento de riscos, considerando os contextos externo e interno;
3	**Avaliar a eficácia** dos controles internos existentes em relação aos objetivos dos processos organizacionais selecionados para o gerenciamento de riscos;
4	**Definir os níveis de apetite a riscos** dos processos organizacionais da ESP/CE, caso sejam diferentes dos propostos na Metodologia de Gerenciamento de Riscos do Poder Executivo Estadual;
5	**Aprovar a periodicidade** máxima do ciclo do processo de gerenciamento de riscos para cada um dos processos organizacionais da ESP/CE;
6	**Aprovar os indicadores** de desempenho para a gestão de riscos da ESP/CE, alinhados com os indicadores de desempenho da ESP/CE;
7	**Aprovar as respostas aos riscos** e as medidas de tratamento e controle a serem implementadas nos processos organizacionais selecionados (Plano de Tratamento);
8	**Avaliar e validar o resultado** do processo de gerenciamento de riscos de cada processo organizacional selecionado;
9	**Avaliar a efetividade das medidas** de tratamento e controle implementadas nos processos organizacionais da ESP/CE;
10	**Avaliar o desempenho do processo** de gerenciamento de riscos e fortalecer a aderência dos processos organizacionais da ESP/CE à conformidade normativa;
11	**Aprovar o plano de comunicação** e consulta de gerenciamento de riscos;
12	**Supervisionar a atuação** das áreas quanto à gestão de riscos.

Quadro 4: Estrutura de Governança e Responsabilidades - Assessoria de Controle Interno e Ouvidoria (Ascoi)

Nível Tático

Área de atuação tática: **Assessoria de Controle Interno e Ouvidoria (Ascoi)**

	Papel na Gestão de Riscos
1	**Auxiliar na identificação dos objetivos** da ESP/CE e na compreensão dos contextos externo e interno a serem considerados no gerenciamento de riscos;
2	**Auxiliar na identificação, análise e avaliação dos riscos** dos processos organizacionais selecionados para a implementação do gerenciamento de riscos;
3	**Auxiliar na definição das respostas aos riscos** e das medidas de tratamento e controle a serem implementadas nos processos organizacionais (Plano de Tratamento);
4	**Auxiliar na definição dos indicadores** de desempenho para a gestão de riscos, alinhados com os indicadores de desempenho da ESP/CE;
5	**Propor o plano de comunicação** e consulta de gerenciamento de riscos;
6	**Propor a atualização das estratégias** de gerenciamento de riscos, considerando os contextos externo e interno;
7	**Propor a periodicidade** máxima do ciclo do processo de gerenciamento de riscos para cada um dos processos organizacionais da ESP/CE;
8	**Realizar o monitoramento e a análise crítica** dos níveis de riscos e da efetividade das medidas de tratamento e controle implementadas nos processos organizacionais;
9	**Auxiliar na definição dos níveis de apetite a riscos** dos processos organizacionais caso sejam diferentes dos propostos na Metodologia de Gerenciamento de Riscos do Poder Executivo Estadual;
10	**Auxiliar na identificação dos responsáveis** pelo gerenciamento de riscos dos processos organizacionais;
11	**Avaliar os indicadores de desempenho** para a gestão de riscos objetivando melhoria contínua;
12	**Requisitar** aos responsáveis pelo gerenciamento de riscos dos processos organizacionais as informações necessárias para a consolidação dos dados e a elaboração dos relatórios gerenciais;
13	**Acompanhar** o desempenho do processo de gerenciamento de riscos e estimular o fortalecimento da aderência dos processos organizacionais à conformidade normativa;
14	**Documentar** e informar as outras áreas de atuação cada etapa do processo de gerenciamento de riscos.

Quadro 5: Estrutura de Governança e Responsabilidades - Unidades Operacionais

Nível Operacional

Área de atuação Operacional: **Unidades Operacionais**
(responsáveis por processos organizacionais e demais colaboradores)

	Papel na Gestão de Riscos
1	**Identificar os objetivos da ESP/CE** e compreender os contextos externo e interno a serem considerados na gestão de riscos;
2	**Identificar, analisar e avaliar os riscos** dos processos organizacionais selecionados para a implementação do gerenciamento de riscos;
3	**Propor as respostas aos riscos e as medidas de tratamento e controle** a serem implementadas nos processos organizacionais (Plano de Tratamento);
4	**Monitorar os níveis de riscos e a efetividade das medidas** de tratamento e controle implementadas nos processos organizacionais sob sua responsabilidade;
5	**Informar à área de atuação tática** sobre mudanças significativas nos processos organizacionais sob sua responsabilidade;
6	**Propor os indicadores** de desempenho para a gestão de riscos, alinhados com os indicadores de desempenho da ESP/CE;
7	**Responder às requisições** da área de atuação tática;
8	**Disponibilizar as informações** quanto ao gerenciamento de riscos dos processos sob sua responsabilidade a todos os níveis da ESP/CE e demais partes interessadas;
9	**Realizar outras atividades de gerenciamento de riscos** dos processos sob sua responsabilidade, em conformidade com a Política de Gestão de Riscos instituída pelo Decreto Estadual nº 33.805/2020 e com a Metodologia de Gerenciamento de Riscos instituída pela Portaria CGE nº 05/2021.

Matriz de Responsabilidade

Segundo a Portaria CGE nº 05/2021, a "Matriz de Responsabilidade - RACI (Responsável, Autoridade, Consultado, Informado) define as atribuições das áreas e atores dentro do processo de gerenciamento de riscos na organização¨. Veja as atribuições de cada um destes atores:

- **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.

Desta forma, a Matriz RACI na Gestão de Riscos da ESP/CE foi assim definida:

Quadro 6: Matriz de Responsabilidade (RACI)

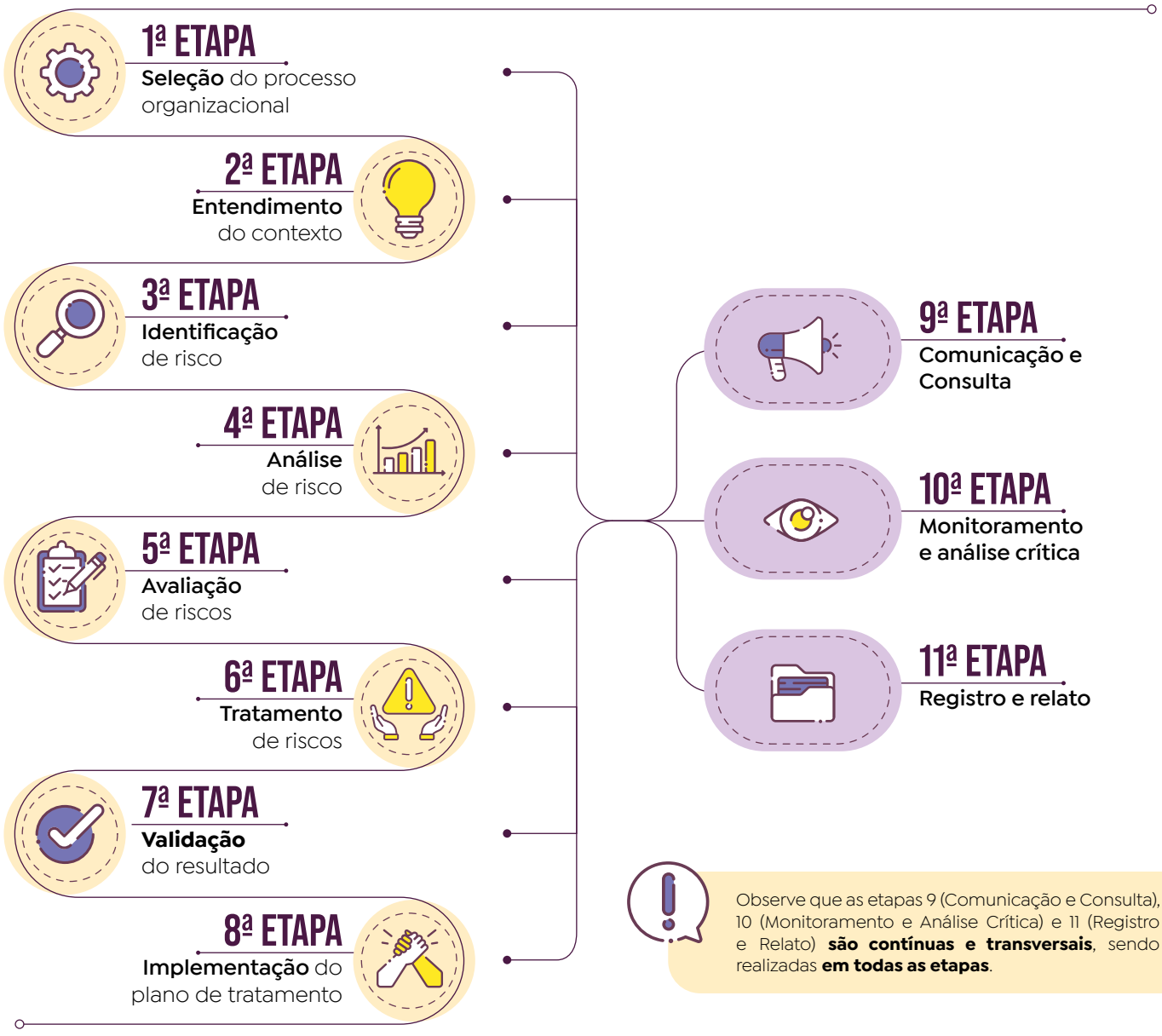
Atividade	Área de atuação estratégica	Área de atuação tática	Área de atuação operacional	Gestor da área	Responsável pelo gerenciamento de riscos	Colaboradores do órgão ou entidade
Selecionar processos organizacionais	A	I	C	R	C	I
Identificar os responsáveis pelos processos organizacionais	I	I	C	R	C	I
Definir os níveis de Apetite a Riscos dos processos organizacionais selecionados caso sejam diferentes dos sugeridos	A	C	R	C	C	I
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 o 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	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 controle a serem implementadas)	A	C	R	C	C	I
Implementar o plano de tratamento	I	I	R	C	C	I
Realizar monitoramento	I	R	R	R	R	I
Realizar a 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	I	R	C	C	C	I

6. Metodologia de Gerenciamento de Riscos

AS 11 ETAPAS

A ESP/CE adota a metodologia de Gerenciamento de Riscos do Poder Executivo do Estado do Ceará, conforme a Portaria CGE nº 05/2021. O processo é orientado a processos organizacionais e é dividido em 11 etapas:

Gráfico 2: As 11 Etapas da Metodologia de Gerenciamento de Riscos



Observe que as etapas 9 (Comunicação e Consulta), 10 (Monitoramento e Análise Crítica) e 11 (Registro e Relato) **são contínuas e transversais**, sendo realizadas **em todas as etapas**.

Para que este manual seja autoexplicativo, detalhamos cada uma das 11 etapas a seguir:

Etapa 1:
Seleção do Processo Organizacional

O que é:

Escolher qual processo de trabalho será analisado.

Para que serve:

Identificar os processos mais importantes ou que impactam diretamente os objetivos principais da instituição.

Como fazer:

O gestor da área, com o apoio da Assessoria de Controle Interno e Ouvidoria (ASCOI), deve selecionar o processo e identificar o responsável por gerenciá-lo. Para ajudar na escolha, podem ser usados critérios de priorização, que avaliam a importância e a criticidade de cada processo.

Esses critérios podem ser de dois tipos:

- **Critérios Qualitativos**: São baseados em percepções e análises subjetivas, mas muito importantes. Por exemplo:

  Impacto social e ambiental: O quanto o processo afeta a comunidade e o meio ambiente?

  Satisfação dos usuários: O processo está ligado diretamente à satisfação do público que atendemos?

  Qualidade da execução: A falha neste processo compromete a qualidade final do nosso trabalho?

- **Critérios Quantitativos**: São baseados em dados e números que podemos medir. Por exemplo:

  Volume de reclamações: Quantas queixas ou ouvidorias o processo gera?

  Valores financeiros envolvidos: O processo movimenta um grande volume de recursos?

  Quantidade de servidores: Quantas pessoas estão envolvidas na execução do processo?

É recomendado combinar os dois tipos de critérios para ter uma visão mais completa e selecionar os processos que são realmente críticos para a ESP/CE.

O que é um processo crítico?

Um processo é considerado crítico quando ele é essencial para o sucesso da instituição. Geralmente, são os processos finalísticos (a atividade principal da Escola), mas também podem ser processos de apoio que, se falharem, causam um grande impacto nos resultados.

Para identificar um processo como crítico, faça as seguintes perguntas:

- Ele envolve valores financeiros altos?
- A entrega de seus produtos ou serviços é complexa ou difícil?
- Ele costuma gerar muitas reclamações ou problemas?
- Uma falha neste processo poderia prejudicar a imagem da ESP/CE na mídia?
- Ele recebe muitas recomendações de órgãos de controle?

Ao responder a essas perguntas, você terá mais clareza para selecionar os processos que mais precisam de atenção e, assim, garantir que a gestão de riscos seja aplicada onde ela é mais necessária.

Lembre-se: O responsável pelo processo organizacional também será o responsável por gerenciar seus riscos e implementar as ações de melhoria.

Etapa 2:
Entendimento do Contexto

O que é:

Conhecer em detalhes o processo de trabalho que foi escolhido.

Para que serve:

Entender como o processo funciona, quem são os envolvidos, quais os seus objetivos e o que pode influenciá-lo, tanto positiva quanto negativamente.

Como fazer:

A a área de atuação operacional, auxiliada pela área de atuação tática, deve reunir informações importantes, como:

- Descrição resumida do processo organizacional;
- Área responsável;
- Ciclo médio (em dias);
- Sistemas tecnológicos;

- Partes interessadas (internas ou externas);
- Fluxo (mapa) do processo organizacional;
- Objetivos do processo organizacional;
- Relação de objetivos estratégicos da organização alcançados pelo processo;
- Justificativa para o gerenciamento de riscos;
- Leis e regulamentos relacionados ao processo organizacional;
- Informações sobre o contexto externo do processo organizacional;
- Informações sobre o contexto interno do processo organizacional;
- Periodicidade máxima do ciclo do processo de gerenciamento de riscos (ver 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).
- Apetite a risco da área para o processo organizacional, caso seja diferente do proposto neste documento (quadro 12).

Além disso, a equipe responsável pelo processo também será responsável pela implementação das respostas aos riscos e das medidas de tratamento compatíveis com o processo organizacional correspondente. Caso seja necessário envolver mais de uma área, o responsável pelo processo de gerenciamento de riscos deverá alinhar com a(s) áreas adicionais como se dará a participação.

Modelo: Consulte o link no tópico 8 deste documento para acessar o "MODELO ESP - Diagrama de Escopo e Interface do Processo", para padronizar o preenchimento e garantir a conformidade com a metodologia.

Etapa 3: Identificação de Riscos

O que é:

Listar tudo o que pode atrapalhar o bom funcionamento do processo de trabalho.

Para que serve:

Antecipar os problemas para evitar que eles aconteçam ou para diminuir seus efeitos negativos.

Como fazer:

A equipe deve pensar em tudo o que pode impedir, atrasar ou prejudicar o alcance dos objetivos do processo. Uma boa pergunta a se fazer é: "O que pode dar errado

nesta etapa do trabalho?".

- 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?

Modelo: Consulte o link no tópico 8 no final deste documento para acessar o "Modelo de planilha para registro das informações produzidas nas etapas de Identificação e Análise de Riscos", para padronizar o preenchimento e garantir a conformidade com a metodologia.

Etapa 4: Análise de Riscos

O que é:

Entender por que um risco pode acontecer e quais seriam as suas consequências.

Para que serve:

Compreender a origem e o impacto de cada risco para criar formas mais eficientes de proteção.

Como fazer:

Para cada risco identificado, a equipe deve descrever suas possíveis **causas** e **consequências**. Também é preciso listar o que já é feito para evitar que o risco aconteça (controles preventivos) e o que é feito para diminuir o prejuízo caso ele ocorra (controles de atenuação).

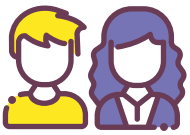
Para que essa atividade seja realizada, a área de atuação operacional, com auxílio da área de atuação tática, deve indicar:

- Etapa e objetivo impactados pelo risco;
- Categoria do risco:

Operacional: eventos que podem comprometer as atividades do órgão ou entidade;

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;



Integridade: eventos relacionados à corrupção, fraudes, irregularidades e/ou desvios éticos e de conduta que podem comprometer os valores e padrões preconizados e a realização dos 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;
- Controles de atenuação e recuperação: controles existentes executados após a ocorrência do risco com o intuito de diminuir o impacto de suas consequências.

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.

Modelo: Consulte o link no final deste documento para acessar o "Modelo de planilha para registro das informações produzidas nas etapas de Identificação e Análise de Riscos", para padronizar o preenchimento e garantir a conformidade com a metodologia.

Etapa 5: Avaliação de Riscos

Esta etapa serve para medir o tamanho de cada risco e decidir quais são mais graves e precisam de mais atenção.

Modelo: Consulte o link no tópico 8 deste documento para acessar o "Modelo de Planilha para Registro das Informações Produzidas nas Etapas de Identificação e Análise De Riscos", para padronizar o preenchimento e garantir a conformidade com a metodologia.

Os quadros 7 e 8 trazem as escalas de probabilidade e impacto, respectivamente:

Quadro 7: 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 ocorrerá pois, as circunstâncias indicam claramente essa possibilidade).	10

Quadro 8: Escala de Impacto

Probabilidade		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
Média		Moderado impacto nos objetivos do processo organizacional, porém recuperável.	5
Alta		Significativo impacto nos objetivos do processo organizacional, de difícil reversão.	8
Muito Alta		Catastrófico impacto nos objetivos do processo organizacional, de forma irreversível.	10

5.1 Cálculo do Risco Inerente

O que é:

Medir o risco puro, sem considerar nenhuma proteção existente.

Como fazer:

A equipe multiplica a **Probabilidade** (chance de o risco acontecer) pelo **Impacto** (o tamanho do prejuízo se ele acontecer).

$$RI = NP \times NI$$

Onde:

RI = nível do risco inerente

NP = nível de probabilidade do risco

NI = nível de impacto do risco

5.2 Classificação do Risco

O que é:

Dar uma nota para o risco com base no cálculo anterior.

Como fazer:

O risco é classificado como Baixo, Médio, Alto ou Extremo.

A partir do resultado do cálculo feito no tópico 5.1, o risco pode ser classificado dentro das seguintes faixas:

Quadro 9: Classificação do Risco

Classificação	Peso
Risco Baixo (RB)	0 - 9,99
Risco Médio (RM)	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 10: Matriz de Riscos

Matriz de Risco		Probabilidade				
		Muito baixa (x 1)	Baixa (x 2)	Média (x 5)	Alta (x 8)	Muito alta (x 10)
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 RM	8 RM	10 RM

5.3 Avaliação dos Controles

O que é:

Verificar se as proteções que já existem para controlar os riscos estão funcionando bem.

Como fazer:

O Comitê de Governança avalia se os controles atuais são Fortes, Satisfatórios, Medianos, Fracos ou Inexistentes.

O quadro 11 mostra os níveis de avaliação da eficácia dos controles existentes:

Quadro 11: 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

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

5.4 Cálculo do Risco Residual

O que é:

Medir o risco que sobra mesmo depois de aplicar as proteções existentes.

Como fazer:

A equipe multiplica o Risco Inerente pelo fator de avaliação dos controles. O resultado mostra o nível real do risco no dia a dia.

$$RR = RI \times FC$$

Onde:

RR = nível do risco residual

RI = nível do risco inerente

FC = fator de avaliação dos controles existentes

Etapa 6: Tratamento de Riscos

Esta etapa serve para criar um plano de ação para lidar com os riscos que foram identificados e avaliados como mais importantes.

6.1 Cálculo do Risco Residual

O que é:

Decidir quais riscos serão tratados primeiro.

Para que serve:

A equipe usa o Risco Residual para focar nos riscos mais altos e urgentes.

Modelo: Consulte o link no tópico 8 deste documento para acessar o "Modelo de Planilha para Registro das Informações Produzidas na Etapas de Tratamento dos Eventos de Risco", para padronizar o preenchimento e garantir a conformidade com a metodologia.

Quadro 12: 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 responsável pelo processo.	Caso o risco não seja priorizado para implementação de medidas de tratamento, a não priorização deve ser justificada pelo responsável 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.

6.2 Definição de respostas aos riscos

O que é:

Definir a melhor estratégia para cada risco priorizado.

Para que serve:

A equipe pode escolher uma das quatro opções:

EVITAR (Risco Extremo): Mudar o processo de trabalho para que o risco não exista mais.

COMPARTILHAR (Risco Alto): Dividir a responsabilidade pelo risco com outra área ou contratar um seguro.

MITIGAR (Risco Médio): Criar novas ações para diminuir a chance ou o impacto do risco.

ACEITAR (Risco Baixo): Não fazer nada de novo, pois o risco é baixo e o custo para tratá-lo não compensa.

Quadro 13: Ações de acordo com o Nível de Risco

Probabilidade x impacto (p x i)	Opção de Tratamento	Descrição (o que fazer)	Quando usar
Extremo	**Evitar**	Decidir não iniciar ou interromper a atividade que gera o risco.	Para Riscos Extremos, quando não há como reduzir.
Alto	**Compartilhar**	Transferir parte do risco para terceiros (ex: contratar seguro, fazer convênios, terceirizar).	Quando o custo de reduzir é muito alto.
Médio	**Mitigar**	Implementar novos controles ou melhorar os existentes para diminuir a Probabilidade e/ou o Impacto.	Para a maioria dos Riscos Médios e Altos.
Baixo	**Aceitar**	Não tomar nenhuma ação, apenas monitorar.	Para Riscos Baixos, onde o custo do tratamento é maior que o benefício.

6.3 Elaboração do Plano de Tratamento

O que é:

Criar um documento com as ações práticas para tratar os riscos.

Para que serve:

O plano deve dizer o que será feito, quem será o responsável, qual o prazo e quais os resultados esperados, levando em conta:

1) Responsabilidade compartilhada na execução dos planos de tratamento de riscos.
2) Plano de Tratamento deve ser aprovado pela área de atuação estratégica (Comitê de Governança).

Importante: 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.

Modelo: Consulte o link no tópico 8 deste documento para acessar o "Plano de Tratamento de Eventos de Risco - ESP/CE", para padronizar o preenchimento e garantir a conformidade com a metodologia.

Etapa 7:
Validação do Resultado

O que é:

Apresentar todo o trabalho de gerenciamento de riscos para aprovação.

Para que serve:

Garantir que a análise foi bem feita e que o plano de tratamento é adequado antes de colocá-lo em prática.

Como fazer:

A equipe responsável pelo processo apresenta os resultados para a área estratégica (Comitê de Governança), que irá validar o trabalho, em seguida:

- A área estratégica deve encaminhar o resultado às áreas internas para conhecimento;
- O plano de tratamento deve ser incluído nas metas e atividades das áreas responsáveis;
- O plano aprovado deve também ser encaminhado às áreas corresponsáveis para execução.

Etapa 8:
Implementação do Plano de Tratamento

O que é:

Colocar em prática as ações definidas no Plano de Tratamento.

Para que serve:

Executar as melhorias e os novos controles para proteger o processo contra os riscos.

Como fazer:

O servidor indicado como responsável no plano deve garantir que as ações sejam executadas no prazo, envolvendo outras áreas se necessário, e acompanhar o progresso.

Etapa 9:
Comunicação e Consulta

O que é:

Manter todos os envolvidos e interessados informados sobre a gestão de riscos.

Para que serve:

Garantir que a informação certa chegue às pessoas certas, promovendo a transparência e a colaboração.

Como fazer:

A equipe deve comunicar as decisões e os resultados em todas as etapas do processo, consultando as áreas e pessoas que podem contribuir ou que serão impactadas pelas ações.

- A comunicação deve seguir o fluxo definido na Matriz de Responsabilidade – RACI (ver: Tópico 4 - Estrutura de Governança e Responsabilidade, Quadro 5: Matriz RACI).

Importante: Convém que a Comunicação e Consulta ocorra em todas as etapas do processo de gerenciamento de riscos.

Etapa 10:
Monitoramento e Análise Crítica

O que é:

Acompanhar de perto se os controles estão funcionando e se os riscos estão diminuindo.

Para que serve:

Verificar se o plano de tratamento está sendo eficaz e identificar novos riscos que possam surgir.

Como fazer:

A equipe responsável pelo processo, em conjunto com a área de atuação tática, deve observar continuamente os resultados, analisar se os riscos estão de fato sob controle e fazer ajustes no plano sempre que necessário.

- 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.

Importante: Convém que o Monitoramento e a Análise Crítica ocorra 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).

Importante: 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.

Etapa 11: Registro e Relato

Esta etapa serve para documentar e comunicar todo o processo de gestão de riscos.

11.1 Registro

O que é:

Guardar de forma organizada todas as informações e decisões do processo.

Como fazer:

A equipe deve documentar cada etapa, incluindo a análise de contexto, os riscos identificados, os planos de tratamento e os responsáveis.

11.1 Relato

O que é:

Produzir relatórios sobre a gestão de riscos para as áreas interessadas.

Como fazer:

A equipe cria relatórios claros e objetivos para a diretoria e outras áreas, ajudando na tomada de decisão e mostrando os resultados do trabalho.

Importante: Convém que o Registro e Relato ocorra em todas as etapas do processo de gerenciamento de riscos.

7. Referências

Este manual foi elaborado com base nos seguintes documentos, que fornecem as diretrizes e o contexto legal para a Gestão de Riscos na ESP/CE, entre outros documentos de referências nacionais e internacionais relacionados a Boas Práticas da Gestão de Risco:

Quadro 14: Referências

Documento	Descrição da finalidade
Decreto Estadual nº 33.805/2020 Clique e acesse	Institui a Política de Gestão de Riscos (PGR) do Poder Executivo do Estado do Ceará. É a base legal para todo o processo.
Portaria CGE nº 05/2021 Clique e acesse	Institui a Metodologia de Gerenciamento de Riscos do Poder Executivo Estadual, detalhando as 9 etapas que adotamos neste Manual.
Lei Estadual nº 16.717/2018 Clique e acesse	Institui o Programa de Integridade do Poder Executivo do Estado do Ceará, no qual a Gestão de Riscos é um dos eixos centrais.
Portaria ESP/CE nº 33/2024 Clique e acesse	Política de Gestão de Riscos da ESP/CE. É o ato normativo interno que formaliza a adoção da política na Escola.
Guia Prático para Implementação da Gestão de Riscos no Poder Executivo Estadual do Ceará (CGE/2024) Clique e acesse	Documento orientativo da CGE que detalha a aplicação da metodologia e serve como referência técnica para a elaboração deste Manual.
Cartilha "Como Usar Linguagem Simples" (CGE/Lab ÍRIS) Clique e acesse	Guia prático para a redação de documentos públicos com clareza e acessibilidade, garantindo o direito do cidadão de entender a informação.
ABNT NBR ISO 31000:2018 Clique e acesse	Norma internacional que fornece diretrizes e princípios para a gestão de riscos, servindo como base para as boas práticas metodológicas.

Documento	Descrição da finalidade
Referencial Básico de Governança (TCU) Clique e acesse	Documento do Tribunal de Contas da União que estabelece as diretrizes e boas práticas de governança e gestão de riscos para o setor público federal e estadual.
Manual de Gestão de Riscos e Controles Internos Fundação Universidade Estadual do Ceará (Funece) Clique e acesse	Documento de referência de outra instituição, usado para análise comparativa de boas práticas e modelos de estruturação.
Planos de Ação da Implantação da Gestão de Riscos na ESP/CE	Planilha de trabalho que detalha as ações e cronograma para a implementação e fortalecimento da Gestão de Riscos na ESP/CE.
Plano de Comunicação da Gestão de Risco da ESP/CE Clique e acesse	Acompanhe neste documento os processos de trabalho relacionados à divulgação das ações, capacitações e outras ações de comunicação.

8. Planilhas, formulários e modelos editáveis

Acesse os links abaixo para fazer download de modelos de documentos que devem ser considerados na realização das etapas correspondentes para garantir a manutenção dos padrões da metodologia.

Quadro 15: Modelos editáveis

Descrição do arquivo
Modelo de Diagrama de Escopo e Interface do Processo (DEIP)
Modelo de Planilha para Registro das Informações Produzidas - Etapas Identificação, Análise, Avaliação, Priorização e Definição de Respostas aos Riscos - ESP/CE
Modelo de Plano de Tratamento de Eventos de Risco - ESP/CE

Clique e acesse os documentos editáveis

CEARÁ

GOVERNO DO ESTADO

SECRETARIA DA **SAÚDE**

ESCOLA DE SAÚDE PÚBLICA DO CEARÁ