CEARÁ
GOVERNO DO ESTADO
SECRETARIA DA INFRAESTRUTURA

Manual de procedimentos para avaliação dos controles internos

Maria Izolda Cela de Arruda Coelho
Governadora do Estado do Ceará

Lucio Ferreira Gomes
Secretário da Infraestrutura

José André Pierre Pessoa
Secretário executivo de logística Intermodal e obras

Adão Linhares Muniz
Secretário Executivo de Energia e Telecomunicações

Paulo César Moreira de Sousa
Secretário Executivo de Planejamento e Gestão Interna

COMISSÃO DE ELABORAÇÃO

Paula Dannyelly Alves Fidelis *(presidente)*
Assessoria de Controle Interno

Alexsidiney Fontenele Carneiro
Coordenadoria Administrativo-Financeira

Bruno Facundo Braga
Coordenadoria de Planejamento

Lucas Souza dos Santos,
Coordenadoria de Planejamento

Francisco Carlos Nobre Junior
Coordenadoria de Transportes e Obras

Luciana Alves Lemos Marques
Coordenadoria de Energia e Telecomunicações

Marília Kelvia Mota Costa
Ouvidoria

Soraia Azevedo Olímpio
Assessoria Jurídica

José Mário de Lima Chaves
Revisão

V 1.0 – 1ª. EDIÇÃO – Fortaleza, outubro de 2022

SUMÁRIO

1. INTRODUÇÃO

A Secretaria da Infraestrutura do Estado do Ceará, com a elaboração e disseminação do Manual de Controle Interno, tem como objetivo principal nortear a Assessoria de Controle Interno e as áreas a serem controladas e auditadas, bem como atender à Prestação de Contas Anual do Tribunal de Contas do Estado do Ceará – TCE, como evidência de Procedimentos de Controle, em seu item 3.1, que refere-se às políticas e ações de natureza preventiva ou de detecção, para diminuir os riscos e alcançar os objetivos, através de sua formalização e ampla disseminação nos diversos níveis da organização.

O tema destaca-se devido ao fato que a Assessoria de Controle Interno, por meio de seus processos e atividades de controle, consiste em ferramenta gerencial para a administração, visando propiciar efetividade à gestão e assegurar a transparência das ações emanadas pelo Poder Público e dos valores despendidos para custear tais ações. Por fim, salienta-se que o Tribunal de Contas do Estado do Ceará – TCE orienta, de acordo com a Instrução Normativa 003/2015, que, na Prestação de Contas Anual, seja apresentado o Manual de Controle Interno como evidência de Procedimentos de Controle.

O presente Manual auxiliará e orientará a atuação dos integrantes da Assessoria de Controle Interno desta SEINFRA, servindo como um instrumento em busca de planejamento, gerenciamento e padronização das atividades desenvolvidas, visando atingir padrões de qualidade e aprimoramento das atividades inerentes à Administração Pública, bem como proporcionar maior transparência das ações ao TCE e aos demais órgãos de controle, almejando-se, por fim, ajustes, ao longo do tempo, promovendo uma importante evolução da gestão desta SEINFRA.

Este Manual está dividido em 5 (cinco) itens, onde, na Introdução, serão apresentados os objetivos do referido documento, seguido de explanação quanto ao Controle Interno, no item 02, e a definição do conceito de Risco adotado pela SEINFRA, no item seguinte.

No item 04, será apresentada a metodologia do Gerenciamento de Riscos, que segue as diretrizes do COSO (Committee of Sponsoring

Organizations of the Treadway Commission), bem como o Decreto nº 33.805, de 9 de novembro de 2020, que institui a Política de Gestão de Riscos – PGR, do Poder Executivo do Estado do Ceará, e a Portaria 05/2021/CGE, que institui a metodologia de gerenciamento de riscos do Poder Executivo do Estado do Ceará.

Finalizando o Manual, serão descritas ,no item 05, as técnicas de auditoria prioritárias a serem utilizadas, seguidas dos Procedimentos de Avaliação a serem realizados pela Assessoria de Controle Interno (Acint), conforme disposto no Plano Anual de Auditoria, apresentados no item 06.

2. CONTROLES INTERNOS

Os Controles Internos podem ser adequadamente compreendidos por meio da Teoria da Agência. A satisfação do titular depende da atuação do agente, portanto, o titular deve se assegurar de que a atuação do agente será aquela que satisfaça seu objetivo. Porém, os interesses do agente nem sempre estão alinhados aos do titular. Nesse caso, tem-se, como resultado, um conflito de agência ou conflito agente-titular e, para minimizar tais problemas, torna-se necessária a criação dos instrumentos de controle, pois dificilmente o titular terá condições de fiscalizar 100% dos atos praticados pelo agente. Esse conjunto de mecanismos de controles adotados para selecionar e monitorar os atos praticados pelos agentes denomina-se “Controles Internos”.

Os Controles Internos devem ser operados por pessoas em todos os níveis da organização, desde os mais altos (conselhos e diretorias) até o quadro de pessoal em geral.

Como uma das principais referências no assunto, temos o Committee of Sponsoring Organizations of the Treadway Commission (COSO), uma organização americana que reúne cinco patrocinadores, que atuam para o desenvolvimento de estruturas e orientações sobre gerenciamento de riscos corporativos, controle interno e controle de fraudes.

O COSO define os controles internos da seguinte forma:

> “Controle interno é um processo conduzido pela estrutura de governança, administração e outros profissionais da entidade, e desenvolvido para proporcionar segurança razoável com respeito à realização dos objetivos relacionados a operações, divulgação e conformidade.”

Com o COSO I, o papel dos controles internos foi ampliado e reconhecido como ferramenta de gestão e monitoramento de riscos em relação ao alcance dos objetivos da organização.

O Controle Interno, na área pública, tem o objetivo de ser um mecanismo de auxílio ao administrador público e um instrumento de proteção e defesa do cidadão. Os controles contribuem para que os objetivos da organização pública sejam alcançados e as ações conduzidas de forma econômica, eficiente e eficaz, resultando na salvaguarda dos recursos públicos contra o desperdício, o abuso, os erros, as fraudes e as irregularidades.

3. RISCOS

Toda entidade, pública ou privada, ao desempenhar suas atividades, está sujeita a eventos, ou seja, incidentes e ocorrências oriundos de fontes internas ou externas, que podem afetar, positiva ou negativamente, a realização de seus objetivos. Quando um evento qualquer impacta positivamente a entidade, ou seus objetivos, tem-se a oportunidade, quando impacta negativamente tem-se o risco.

Segundo o TCU (2018, p. 08), “Risco é o efeito da incerteza sobre objetivos estabelecidos. É a possibilidade de ocorrência de eventos que afetem a realização ou alcance dos objetivos, combinada com o impacto dessa ocorrência sobre os resultados pretendidos”.

Já o PMBOK (2013) define risco como uma condição ou evento incerto, que, caso se concretize, causará efeitos negativos ou positivos sobre pelo menos um dos objetivos do projeto, como escopo, tempo, custo ou qualidade.

Para a CGE (2020, p. 01) é “possibilidade de ocorrência de um evento que tenha impacto no atingimento dos objetivos da organização”.

De outra parte, o Committee of Sponsoring Organizations of the Treadway Commission (Comitê das Organizações Patrocinadoras da Comissão Treadway) definiu que incertezas representam riscos e oportunidades, com potencial para destruir ou agregar valor às organizações, as quais só existem para gerar valor para os *stakeholders* (partes interessadas).

Nota-se, portanto, que risco é todo evento que pode causar impactos, tanto positivos como negativos, na consecução de objetivos preestabelecidos.

4. GERENCIAMENTO DE RISCOS

A gestão de riscos exige o equilíbrio e a integração de uma série de elementos, que interagem uns com os outros. A escolha do método de gerenciamento de riscos deve considerar a realidade, o nível de criticidade dos processos e a capacidade técnica e operacional dos atores envolvidos.

O gerenciamento de riscos compreende o processo para identificar, analisar, avaliar, tratar e controlar potenciais eventos ou situações, a fim de fornecer razoável certeza quanto ao alcance dos objetivos. Neste sentido, o processo completo de gerenciamento de riscos é composto pelas seguintes etapas:

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

II – Identificação de riscos: elaboração de abrangente lista de riscos com base nos eventos que possam criar, aumentar, evitar, reduzir, acelerar ou atrasar a realização dos objetivos associados aos processos organizacionais;

III – Análise de riscos: identificação das possíveis causas, consequências e probabilidade de ocorrência dos riscos;

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

V – 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;

VI – Comunicação e consulta: realização de atividades a fim de assegurar que os responsáveis pela implementação do processo de gerenciamento 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; e

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 do gerenciamento de riscos.

O documento COSO I discorre que controle interno é um processo constituído de cinco componentes que se interrelacionam: Ambiente de Controle, Avaliação de Risco, Procedimentos de Controle, Informação e Comunicação e Monitoramento, conforme demonstrado na figura abaixo.

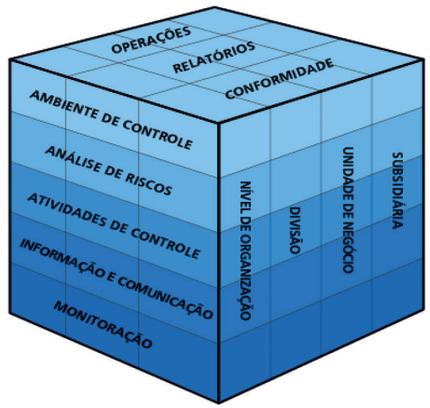


Figura Coso I (adaptado)

Esta figura representa a estrutura do cubo do Coso I, contemplando três dimensões. A dimensão superior do cubo representa os objetivos; a dimensão frontal indica os componentes do gerenciamento de riscos e a dimensão lateral representa os níveis da organização pelos quais perpassa a gestão de riscos.

Em 2004, o COSO publicou o Enterprise Risk Management – integrated framework (Gerenciamento de Risco Corporativo – estrutura integrada), COSO-ERM ou COSO II, documento que ainda hoje é tido como referência para o tema gestão de riscos corporativos, apresentando algumas alterações de sua versão anterior.

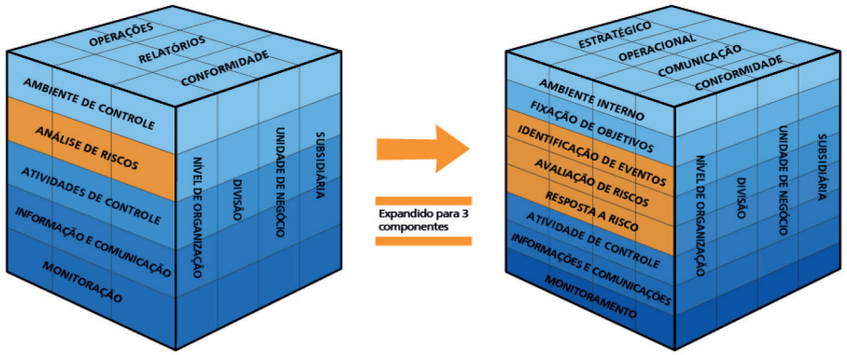
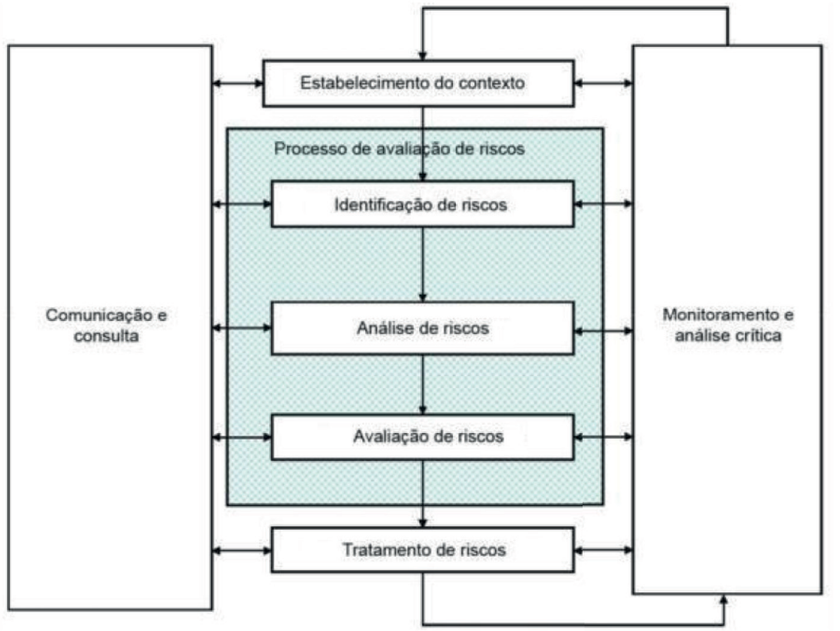


Figura Coso II (adaptado)

Temos, ainda, a norma ISO 31000 para a gestão de riscos, que foi proposta em 2009, sendo traduzida, no Brasil, pela Associação Brasileira de Normas Técnicas (ABNT). Ela fornece princípios e diretrizes para gerenciar qualquer tipo de risco no todo ou em parte de qualquer organização. Constitui uma norma geral, independentemente de indústria, setor ou área, e não concorre com outras normas sobre gestão de riscos em áreas específicas (ABNT, 2009).

A ISO 31000:2009 visa harmonizar os processos de gestão de riscos, fornecendo uma abordagem comum, que pode ser aplicada a uma ampla gama de atividades, incluindo estratégias, decisões, operações, processos, funções, projetos, produtos, serviços e ativos (ABNT, 2009). Contempla sete dimensões, conforme a figura abaixo.



Fonte: ABNT

Com base na ISO 31000:2009, a operacionalização do gerenciamento de riscos deve contemplar os seguintes componentes: a) estabelecimento do contexto; b) identificação de riscos; c) análise de riscos; d) avaliação de riscos; e) tratamento de riscos; f) comunicação e consulta; e g) monitoramento e análise crítica.

No âmbito do Estado do Ceará, existem dois documentos que regem a política de gestão de riscos e a metodologia para aplicação da mesma, estando em perfeita harmonia com o que já foi apresentado neste Manual:

I – o Decreto nº 33.805, de 9 de novembro de 2020, que institui a Política de Gestão de Riscos – PGR do Poder Executivo do Estado do Ceará; e

II – a Portaria 05/2021/CGE, que institui a metodologia de gerenciamento de riscos do Poder Executivo do Estado do Ceará.

Assim, neste Manual de Controle Interno, passaremos a utilizar a metodologia abordada na referida Portaria, conforme demonstrado nos itens a seguir.

4.1 AMBIENTE DE CONTROLE

O Ambiente de Controle refere-se a um conjunto de normas, processos e estrutura que servem de base para a condução do controle interno no âmbito da organização como um todo. Trata-se da atitude geral do órgão, ou seja, o envolvimento, a conscientização e o comportamento da entidade a respeito da importância dos controles.

4.2 AVALIAÇÃO DE RISCOS

Identificação de quais riscos necessitam de tratamento e qual a prioridade para a implementação do tratamento.

Nesta etapa, obteremos informações primordiais para o processo de gerenciamento de riscos. A área de Controle Interno, com o apoio operacional da área de Negócio, deverá:

- 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:
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 a seguir trazem, respectivamente, as escalas de probabilidade e de impacto:

Quadro 1: Escala de Probabilidade desconsiderando os controles

PROBABILIDADE	DESCRIÇÃO	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

Fonte: CGE

Quadro 2: Escala de Impacto

PROBABILIDADE	DESCRIÇÃO	PESO
Muito Baixo	Mínimo impacto nos objetivos do processo organizacional.	1
Baixo	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

Fonte: CGE

4.2.1 Metodologia de 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 2, 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 x NI

Em que:

RI = nível do risco inerente
NP = nível de probabilidade do risco
NI = nível de impacto do risco

Exemplo:

Um risco qualquer da área financeira foi classificado com Probabilidade Média (Peso 5) e Impacto Alto (Peso 8). O valor do Risco Inerente seria:

RI = 5 x 8
RI = 40

4.2.2 Classificação do Risco Inerente

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

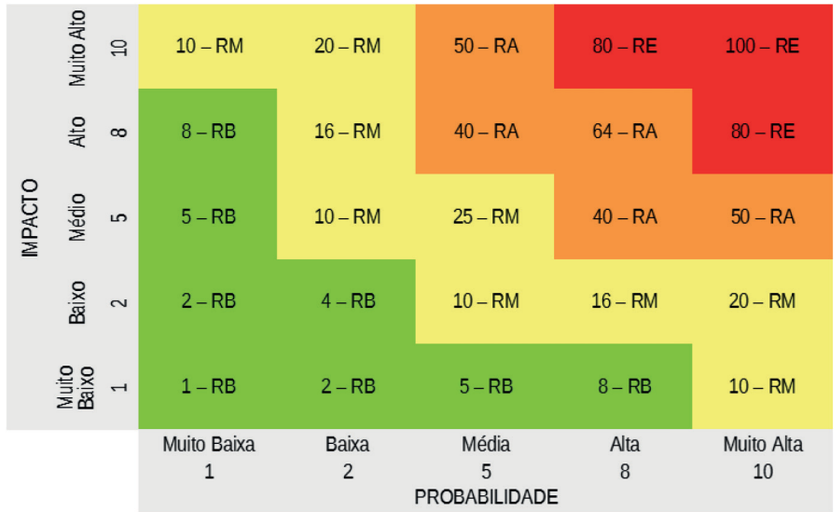
Quadro 3: Classificação do Risco

CLASSIFICAÇÃO	FAIXA
Risco Baixo – RB	0 a 9,99
Risco Médio – RM	10 a 39,99
Risco Alto – RA	40 a 79,99
Risco Extremo – RE	80 a 100

Fonte: CGE

- No caso do exemplo apresentado, a área financeira teria um risco classificado como Alto. Visualmente, temos a matriz probabilidade *x* impacto, que apresenta os possíveis resultados da combinação NP x NI.

Quadro 4: Matriz Probabilidade *x* Impacto



Fonte: CGE (Modificado)

4.2.3 Avaliação da eficácia dos controles existentes

Após a classificação do risco, 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 anterior) têm auxiliado no tratamento adequado desses riscos.

O Quadro 5 mostra os níveis de avaliação da eficácia dos controles existentes:

Quadro 5: Níveis da Avaliação dos Controles Internos Existentes

NÍVEL DE EFICÁCIA DOS CONTROLES EXISTENTES	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 sendo 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 que, embora passíveis de aperfeiçoamento, mitigam o risco satisfatoriamente.	0,4
Forte	Controles implementados podem ser considerados a "melhor prática", mitigando todos os aspectos de risco relevantes.	0,2

Fonte: CGE

4.2.4 Metodologia de Cálculo do Risco Residual

Após a avaliação dos controles existentes (Tópico 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.

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.

RR = RI x 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.

Exemplo:

Voltemos ao caso do risco classificado pela área financeira. Lá, o Risco Inerente ficou com o valor final de 40 (Risco Alto).

No entanto, a área adota algumas medidas de controles existentes, as quais foram classificadas com eficácia mediana (fator de avaliação 0,8), conforme Quadro 5.

Assim, o valor do Risco Residual será:

RR = 40 x 0,8
RR = 32

Note que o risco agora está enquadrado na faixa de Risco Médio, conforme Quadro 3.

4.3 TRATAMENTO DE RISCOS

O Tratamento de Riscos é a 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.

4.3.1 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.

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, para 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 neste 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 neste 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.

Fonte: CGE

NOTA: Sobre o Apetite a Risco do Processo Organizacional

Segundo o inciso XIII, do art. 3º, do Decreto nº 33.805, de 9 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:

1. 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;
2. 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.

4.3.2 Definição de Respostas aos Riscos

Esta etapa objetiva definir as opções de tratamento para os riscos priorizados na etapa anterior. 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

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 haja 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.

Fonte: CGE

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").

4.3.3 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 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: 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.

4.4 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.

4.5 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.

4.6 COMUNICAÇÃO DE CONSULTA

Segundo a ISO 31000:2018, durante todas as etapas do processo de gerenciamento de riscos, é importante a comunicação entre as partes interessadas.

O Decreto nº 33.805, de 9 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 ESTRAT.	ÁREA TÁTICA	ÁREA OPERAC.	GESTOR ÁREA	RESP. PELO GEREN. RISCOS	COLAB. DO ÓRGÃO
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 nesta metodologia	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 e 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 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 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 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

Fonte: CGE

4.7 MONITORAMENTO

O monitoramento é a verificação e supervisão crítica contínua, visando identificar mudanças no desempenho requerido ou esperado para determinar adequação, suficiência e eficácia da gestão de riscos.

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 9 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. Essas incluem planejamento, coleta e análise de dados e informações, registro de resultados e fornecimento de retorno (*feedback*).

4.8 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 na organização como um todo;
- 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.

4.8.1 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:

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

4.8.2 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 a tomada de decisão.

5. TÉCNICAS DE AUDITORIA

As Técnicas de Auditoria prioritárias, que poderão ser utilizadas na avaliação dos controles internos administrativos, são:

- **Inspeção:** verificação de registros, documentos e ativos tangíveis;
- **Indagação oral:** uso de entrevistas junto aos membros da unidade auditada para obtenção de dados e informações. A entrevista é um método de coleta de informações que consiste em conversas individuais ou em grupo com pessoas selecionadas cuidadosamente e cujo grau de pertinência, validade e confiabilidade auxilie na coleta de informações. As entrevistas poderão ser reduzidas a termo, se o auditor considerar necessário. A indagação oral poderá ter auxílio de instrumentos, tais como:
  - fluxogramas;
  - narrativas.
- **Observação das atividades e condições:** tem a finalidade de avaliar se o levantamento do processo foi efetivo, de acordo com as normas legais vigentes ou fluxograma que porventura esteja formalizado. Pode ser chamada de teste de percurso, que é efetuado por meio da análise de todas as fases do processo sobre uma amostra limitada de transações. Ela deverá comprovar que o sistema de controle interno funciona de forma coerente, eficaz e continuada. Os elementos da observação são:
  - identificação da atividade específica a ser observada;
  - observação de sua execução;
  - comparação do comportamento observado com os padrões estabelecidos;
  - avaliação e conclusão.

6. PROCEDIMENTOS DE AVALIAÇÃO

A avaliação dos controles internos será realizada pela Assessoria de Controle Interno (Acint), conforme disposto no Plano Anual de Auditoria. Tal avaliação consistirá em uma nota atribuída de acordo com o Quadro de Avaliação dos Controles Internos (QACI), que consiste num conjunto de afirmativas visando auxiliar a avaliação dos controles instituídos para mitigar os riscos inerentes ao processo auditado.

Dividido em cinco componentes (ambiente de controle, avaliação de risco, procedimentos de controle, informação e comunicação e monitoramento), o QACI adotado segue um modelo baseado na Instrução Normativa nº 03/2015, do Tribunal de Contas do Estado do Ceará, conforme detalhamento a seguir:

Quadro 9: Quadro de Avaliação dos Controles Internos

N	AFIRMATIVAS	EVIDÊNCIAS
1	Ambiente de Controle	
1.1	O planejamento estratégico está formalizado por meio de objetivos e metas.	Planejamento Estratégico com objetivo e metas definidas.
1.2	Existe(m) código(s) formal(is) de conduta e outras políticas que explicitam os referenciais éticos da instituição a todos.	Código de Ética ou documento similar.

N	AFIRMATIVAS	EVIDÊNCIAS
1.3	A estrutura organizacional atualizada está formalmente estabelecida.	Organograma ou normativo que detalhe a estrutura do órgão.
1.4	As delegações de autoridade e competência são acompanhadas de definições claras das responsabilidades.	Documento descrevendo as funções e suas respectivas competências.
1.5	Os deveres e responsabilidades essenciais são divididos ou segregados entre diferentes pessoas para reduzir o risco de ocorrerem erros, desperdícios ou fraudes.	Documentação que comprove a definição de controles-chave e como um controle supervisionará o outro, demonstrando a segregação de funções.
1.6	A alta direção monitora a implementação das recomendações e determinações da auditoria interna dos controles interno e externo.	Documento de acompanhamento das determinações/recomendações.
1.7	Existe programa de educação continuada efetivamente executado com ações de capacitação orientadas para melhorar o desempenho dos servidores.	Programação periódica de treinamento.
1.8	Durante o processo de contratação de colaboradores e preenchimentos de cargos comissionados existem regras e controles para evitar privilégios.	Políticas de realização dos processos seletivos ou documento similar.
1.9	Os resultados das avaliações de desempenho são considerados para tomada de decisão por parte das chefias e são comunicados ao servidor mediante *feedback*.	Política de avaliação de desempenho ou documento similar.
2	Avaliação de Risco	
2.1	É prática da unidade o diagnóstico dos riscos (de origem interna ou externa) envolvidos nos seus processos estratégicos, bem como a identificação da probabilidade de ocorrência e impacto desses riscos, sua classificação e a consequente resposta ao risco.	Política de gestão de riscos ou documento similar.
2.2	Durante o processo de tomada de decisão gerencial é considerado o diagnóstico de riscos, já comentado no item 2.1 desse questionário.	Política de gestão de riscos ou documento similar.
2.3	Existe histórico, nos últimos cinco anos, de fraudes e perdas decorrentes de fragilidades nos processos internos da unidade.	Documentos comprobatórios da(s) situação(ões) irregular(es).
2.4	Na ocorrência de indícios de fraudes e desvios é prática da unidade instaurar sindicância para apurar responsabilidades e exigir eventuais ressarcimentos.	Processos de apuração da(s) situação(ões) irregular(es).
3	Procedimentos de Controle	
3.1	As políticas e ações de natureza preventiva ou de detecção para diminuir os riscos e alcançar os objetivos da unidade estão formalizadas (normas e manuais) e são amplamente disseminados nos diversos níveis da organização.	Manual de Controles Internos ou documento similar.
3.2	Há política de segurança de informação formalmente definida.	Política de Segurança de Informação ou documento similar.
3.3	Os ativos, recursos e registros vulneráveis são protegidos e salvaguardados por acesso restrito e controles físicos.	Item da Política de Segurança de Informação que trata do assunto ou documento similar.
3.4	É realizado periodicamente inventário de bens e valores de responsabilidade da entidade, observando inclusive a sua adequada mensuração nos registros contábeis.	Inventários.
3.5	Existe plano periódico de atividades de auditorias internas aprovado pela alta direção e efetivamente executado.	Plano de Auditoria ou documento similar.
4	Informação e Comunicação	
4.1	As informações consideradas relevantes para o Órgão são devidamente identificadas, documentadas e armazenadas.	Item da Política de Segurança de Informação que trata do assunto ou documento similar.
4.2	O fluxo das informações e das comunicações está devidamente documentado, atende aos objetivos do órgão de forma tempestiva e perpassa todos os níveis hierárquicos.	Mapeamento de Processos ou documento similar.
5	Monitoramento	
5.1	A estrutura de controle interno do órgão/entidade é periodicamente monitorada, para avaliar sua validade e qualidade ao longo do tempo.	Atas das reuniões periódicas de monitoramento ou documento similar.
5.2	Quando necessário, os gestores determinam ações corretivas com vistas ao aperfeiçoamento da estrutura de controle interno do Órgão.	Resumo das ações corretivas adotadas ou documento similar.
5.3	Existem padrões para medir periodicamente o desempenho da organização em relação a todos os seus objetivos e metas.	Indicadores de desempenho ou documento similar.
5.4	Quando necessário, os gestores determinam ações corretivas com vistas ao alcance de metas.	Resumo das ações corretivas adotadas ou documento similar.

Fonte: TCE.

A pontuação adotada foi baseada numa combinação entre os procedimentos adotados no Manual de Procedimentos para Avaliação dos Controles Internos do Departamento Nacional de Infraestrutura de Transportes (DNIT) e na Metodologia de Gerenciamento de Riscos no Poder Executivo do Estado do Ceará, da Controladoria e Ouvidoria Geral do Estado (CGE).

Assim, cada afirmativa será avaliada de acordo com a escala a seguir:

Quadro 10: Quadro de Avaliação das Afirmativas

Nível	Descrição	Pontuação
Não se aplica	Não há como afirmar a proporção de aplicação do fundamento descrito na afirmativa no contexto da unidade no período de análise.	–
Totalmente inobservada	O fundamento descrito na afirmativa é, integralmente, não aplicado no contexto da unidade.	0
Parcialmente inválida	O fundamento descrito na afirmativa é parcialmente aplicado no contexto da unidade, porém, em sua minoria.	25
Parcial	O fundamento descrito na afirmativa é parcialmente observado, nem em sua minoria, nem em sua maioria, e sim exatamente em sua mediana.	50
Parcialmente válida	O fundamento descrito na afirmativa é parcialmente aplicado no contexto da unidade, porém, em sua maioria.	75
Totalmente válida	O fundamento descrito na afirmativa é integralmente aplicado no contexto da unidade.	100

Fonte: DNIT.

Logo, quando uma afirmativa for avaliada como “não se aplica”, não fará parte da base para calcular a nota média do componente.

Na sequência, será calculada a média aritmética simples das notas individuais de cada um dos cinco componentes avaliados (ambiente de controle, avaliação de risco, procedimentos de controle, informação e comunicação e monitoramento), para que, então, seja auferida a Nota de Avaliação dos Controles Internos (NACI), obtida pela média aritmética simples das notas dos componentes.

A qualificação da NACI se dará da seguinte forma:

- De 0,0 a 20,0: Precário;
- De 20,1 a 40,0: Deficiente;
- De 40,1 a 60,0: Regular;
- De 60,1 a 80,0: Bom;
- De 80,1 a 100,0: Ótimo.

Após a aferição da NACI e a fim de promover a melhoria contínua dos controles internos, a Acint, sob supervisão da alta gestão e em conjunto com as demais partes interessadas, promoverá a avaliação das afirmativas para as quais não se tenha atribuído avaliação “Totalmente válida”, as quais deverão observar os procedimentos descritos na Seção 4 deste Manual (Gerenciamento de Riscos).

CEARÁ

GOVERNO DO ESTADO

SECRETARIA DA **INFRAESTRUTURA**