METODOLOGIA DE GESTÃO DE RISCOS

IFCE

2024

MISSÃO

Produzir, disseminar e aplicar os conhecimentos científicos e tecnológicos na busca de participar integralmente da formação do cidadão, tornando-a mais completa, visando a sua total inserção social, política, cultural e ética.

VISÃO

Ser referência no ensino, pesquisa, extensão e inovação, visando à transformação social e ao desenvolvimento regional.

VALORES

Valorizar o compromisso ético com responsabilidade social, respeito, transparência, excelência e determinação em suas ações, em consonância com os preceitos básicos de cidadania e humanismo, com liberdade de expressão, com os sentimentos de solidariedade, com a cultura da inovação e com ideias fixas na sustentabilidade ambiental.

GESTÃO SUPERIOR

José Wally Mendonça Menezes

Reitor do IFCE

Cristiane Borges Braga

Pró-Reitora de Ensino

Joélia Marques de Carvalho

Pró-Reitora de Pesquisa, Pós-Graduação e Inovação

Ana Cláudia Uchôa Araújo

Pró-Reitora de Extensão

Reuber Saraiva de Santiago

Pró-Reitor de Administração e Planejamento

Marcel Ribeiro Mendonça

Pró-Reitor de Gestão de Pessoas

Danilo Reis de Vasconcelos

Diretor de Gestão de Tecnologia da Informação

Ana Caroline Cabral Cristino

Diretora de Assistência Estudantil

EQUIPE TÉCNICA

Vládia de Sousa Ferreira

Coordenadora de Governança

Stênio Wagner Pereira de Queiroz

Diretor de Desenvolvimento Institucional

Cláudio Ferreira Oliveira

Chefe do Departamento de Governança de Tecnologia da Informação

Milena Mendes da Costa

Chefe da Auditoria Interna

José Cláudio Karam de Oliveira

Assistente da Auditoria Interna

Felipe Sousa Almeida

Auditor Interno

Dirlândia de Oliveira Marques

Auditora Interna

Lista de Siglas e Abreviaturas

CGU - Controladoria Geral da União

COSO - Committee of Sponsoring Organizations of the Treadway Commission

GR - Gestão de Riscos

IIA - Institute of Internal Auditors

IFCE - Instituto Federal de Educação do Ceará

IGG - Índice de Governança e Gestão

IN – Instrução Normativa

TCU - Tribunal de Contas da União

Lista de Quadros

Lista de Figuras

Sumário

01. INTRODUÇÃO

A Instrução Normativa nº 01/2016 do então Ministério do Planejamento em conjunto com a Controladoria Geral da União estabeleceu que os órgãos e entidades do Poder Executivo Federal deveriam adotar medidas para a sistematização de práticas relacionadas à gestão de riscos, aos controles internos e à governança.

Essa IN foi o marco inicial para os órgãos poder executivo federal começarem a se apropriar e estabelecer um processo de gerenciamento de riscos condizente com sua estrutura e complexidade.

Seguindo a IN, foi publicado o Decreto 9.203/2017 que dispõe sobre a política de governança da administração pública federal direta, autárquica e fundacional. Esse decreto fortaleceu a IN 16 à medida que ratificou a necessidade de as organizações gerenciarem riscos e estabelecerem controles internos.

O Tribunal de Contas da União vem avaliando as organizações públicas por meio do Índice de Governança e Gestão – IGG (atualmente denominada IESGO) no qual uma das perspectivas avaliada é a governança e gestão de riscos.

O processo de gerenciamento de riscos vem sendo difundido e cobrado cada vez mais pelos órgãos estratégicos bem como pelas instâncias de controle interno e externo em um processo de alinhamento internacional de práticas de governança que zelam pela eficiente aplicação de recursos, pessoas e processos. O Institute of Internal Auditors (IIA) é uma organização internacional demasiadamente referenciada nos documentos de orientação da CGU e do TCU, constituindo, dessa forma, uma importante fonte de pesquisa no que se refere ao gerenciamento de riscos.

O processo de gerenciamento de riscos no IFCE se integra com o planejamento estratégico

Nessa perspectiva, o IFCE, no comprometimento com as boas práticas de governança, apresenta a primeira versão de sua metodologia de gestão de riscos que será utilizada como um guia para a aplicação efetiva de um processo de gestão de riscos críticos que atentem contra o alcance dos objetivos institucionais.

02. FUNDAMENTOS E CONCEITOS

Esta metodologia está fundamentada, de acordo com a Política de Gestão de Riscos do IFCE, nas seguintes normas nacionais e internacionais:

- Instrução Normativa Conjunta CGU/MP nº 01, de 10/5/2016;
- ABNT NBR ISO 31.000: 2018, Gestão de Riscos - Princípios e Diretrizes;
- COSO Report. Internal Control: Integrated Framework. 1992;
- Declaração de Posicionamento do IIA - Instituto dos Auditores Internos: As Três Linhas de Defesa no Gerenciamento Eficaz de Riscos e Controles.

As normas mencionadas orientam e servem de diretrizes para que o Instituto Federal do Ceará construísse um guia para ser utilizado no processo de gerenciamento de riscos, de modo que em que pese esse processo seja personalizado às características e nível de complexidade do IFCE, as macro diretrizes estão pautadas em regulamentações postas pelo poder executivo federal.

Para iniciar, o processo de gerenciamento de riscos do IFCE convém definir alguns conceitos básicos.

Risco

Risco é o efeito da incerteza nos objetivos. Um efeito é um desvio em relação ao esperado. Pode ser positivo, negativo ou ambos, e pode abordar, criar ou resultar em oportunidades e ameaças.1 (ISO 31000/2018)

Risco é a possibilidade de um evento afete negativamente o alcance dos objetivos. 2(Manual de Gestão de Riscos do TCU 2ed 2020)

Gerenciamento de Risco

Gerenciamento de riscos corporativos não e uma função nem um departamento. É a cultura, as competências e as práticas que as organizações integram à definição e à execução da estratégia, com o objetivo de gerenciar o risco na criação, na preservação e na realização de valor. 3 (COSO ERM 2017 Sumário Executivo)

Gestão de Risco

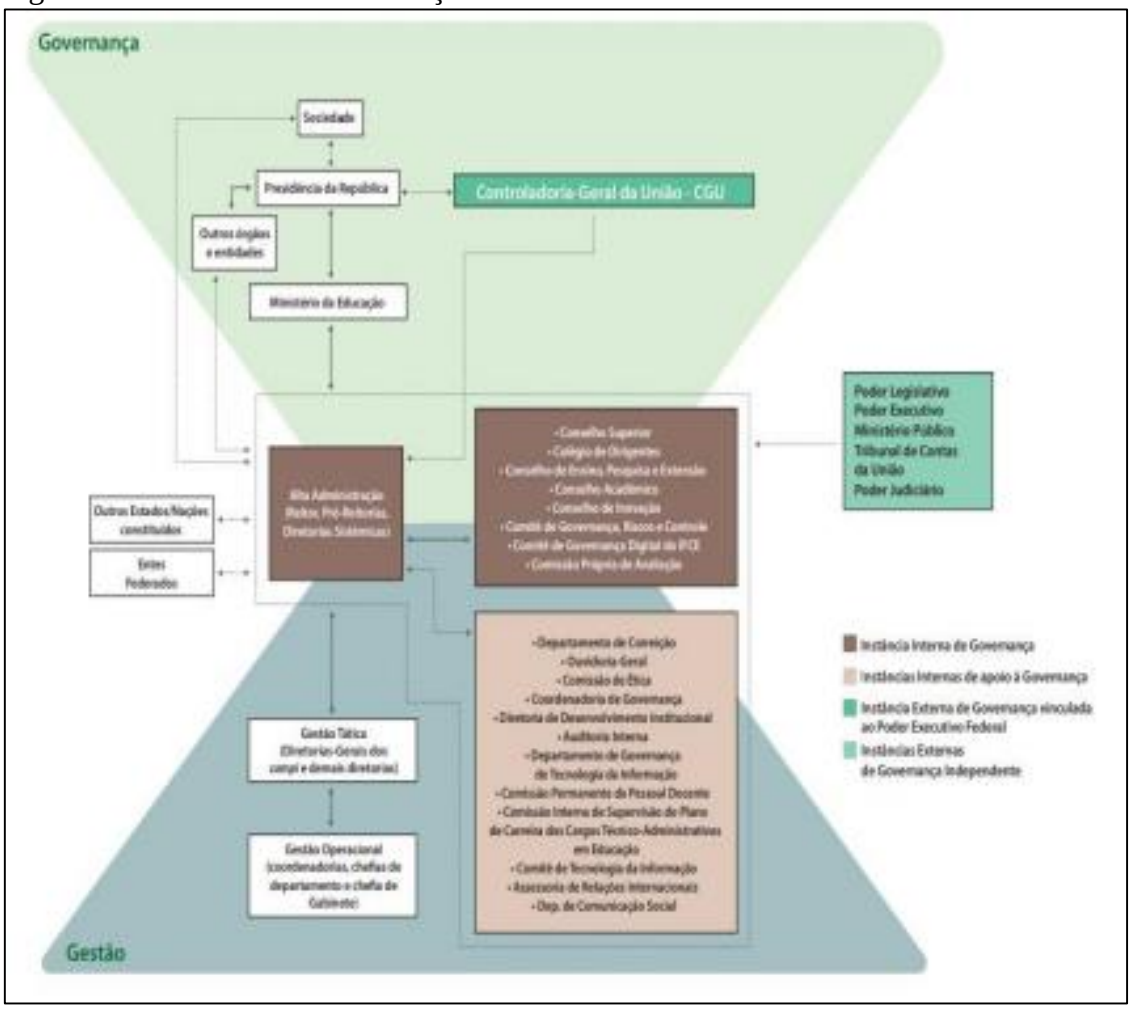
Gestão de riscos é o conjunto de ações direcionadas ao desenvolvimento, disseminação e implementação de metodologias de gerenciamento de riscos institucionais, objetivando apoiar a melhoria contínua de processos de trabalho, projetos e a alocação e utilização eficaz dos recursos disponíveis, contribuindo para o cumprimento dos objetivos da instituição.4 (Política de Gestão de Riscos do IFCE)

A alta administração da organização tem a responsabilidade de gerenciar os riscos da organização com vistas ao alcance dos objetivos e à entrega de valor. Nesse sentido, a alta administração deve patrocinar e assegurar a implementação de uma cultura organizacional voltada à gestão de riscos. Assim orienta a ISO 31000/2018:

> *Convém que a Alta Direção e os órgãos de supervisão, onde aplicável, assegurem que a gestão de riscos esteja integrada em todas as atividades da organização, e convém que demonstrem liderança e comprometimento por: personalizar e implementar todos os componentes da estrutura; emitir uma declaração ou política que estabeleça uma abordagem, plano ou curso de ação da gestão de riscos; assegurar que os recursos necessários sejam alocados para gerenciar riscos; atribuir autoridades, responsabilidades e responsabilização nos níveis apropriados dentro da organização.*

Em conformidade com a Política de Gestão de Riscos do IFCE, todos os servidores da instituição fazem parte, em alguma medida, do processo de gestão de riscos. Em primeira análise, é relevante conhecer e apropriar-se do mosaico da governança do IFCE (Figura 1).

Figura 1 – Estrutura de Governança do Instituto Federal do Ceará

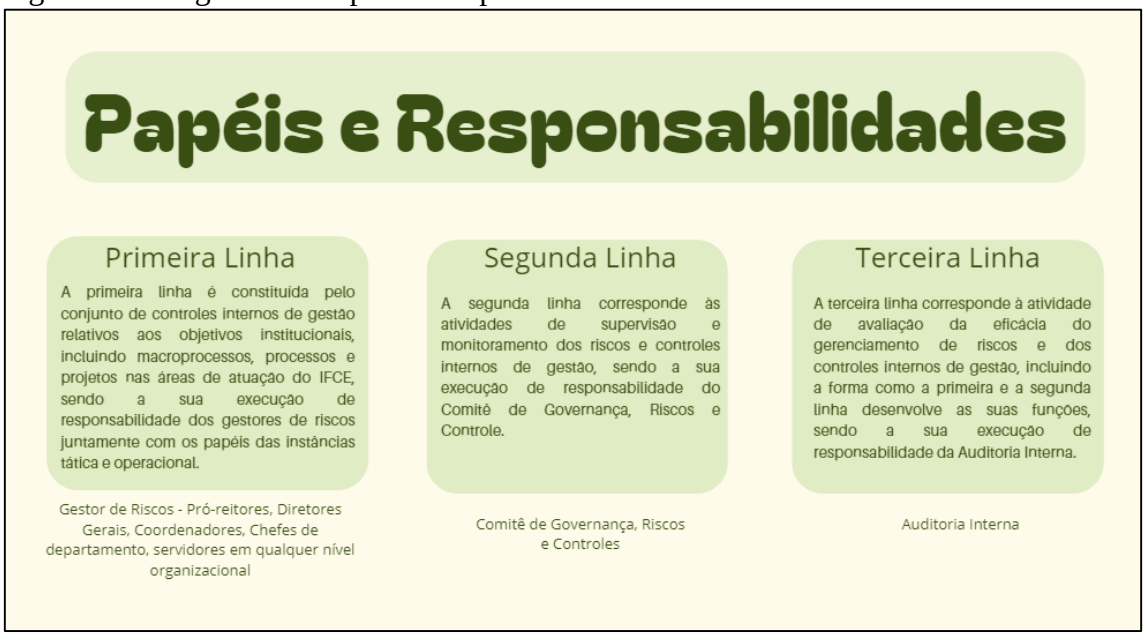


Fonte: Relatório de Gestão 2024

Em segunda análise, é relevante destacar, de acordo com a política de gestão de riscos do IFCE, os atores do processo de gestão de riscos no IFCE. A definição dos atores está de acordo com o modelo de três linhas do IIA.

Todos os servidores em todos os níveis da organização participarão do processo de gestão de riscos no desenvolvimento de um ou mais componentes do processo de gestão de riscos. É importante ressaltar que a participação dos servidores não está relacionada à ocupação ou não de função gratificada, mas à participação deles no objeto (macroprocesso, processo, projeto etc.) que está sendo analisado. (Figura 2).

Figura 2 – Infográfico – Papéis e Responsabilidades na Gestão de Riscos do IFCE



Fonte: Elaboração própria

Todo risco mapeado estará associado a um gestor de risco formalmente identificado. Esse gestor terá autonomia para orientar e acompanhar as ações necessárias para mapear, avaliar e reduzir a ação do risco.

Todos os trabalhos executados no contexto do gerenciamento de risco terão seus registros arquivados e periodicamente acompanhados pela Coordenadoria de Gestão de Riscos (CGR).

03. DECLARAÇÃO DE APETITE A RISCO

A IN nº 01/2016 define apetite a risco como o nível de risco que uma organização está disposta a aceitar.

O COSO ERM 2017 Sumário Executivo estabeleceu que "Cada estratégia tem um perfil de risco próprio - essas são as implicações que emanam da estratégia. O conselho e a administração precisam determinar se a estratégia funciona levando em conta o apetite a risco da organização e como ela direcionará a organização a definir objetivos e alocar recursos com eficiência. Os riscos são priorizados com base no grau de severidade, no contexto do apetite a risco. "

Nesse contexto, o IFCE elaborou essa declaração para definir os critérios a serem considerados na definição do apetite a que o IFCE estará disposto a aceitar frente aos riscos identificados e analisados.

Os riscos serão avaliados e classificados mediante pontuação na matriz de riscos. O apetite do IFCE será em aceitar apenas os riscos classificados como Baixo. Contudo, os riscos mapeados terão, antes de ser tratado, uma matriz de priorização que poderá considerar alguns critérios relevantes (fonte do risco, macroprocesso, entre outros) que devem ser eleitos quando da priorização dos riscos na fase de avaliação. Não havendo critérios relevantes que devam priorizar alguns riscos em detrimento de outros que pela Matriz de Riscos estejam com pontuação maior, a coordenadoria de gestão de riscos deverá considerar a priorização da matriz de riscos.

04. METODOLOGIA

A Metodologia para a execução do processo de gestão de riscos utilizada pelo IFCE observará os componentes da ISO 31000/2018, conforme figura 3.

Figura 3 – Ciclo da metodologia de GR do IFCE

Fonte: ISO 31000/2018

4.1 ESTABELECIMENTO DO CONTEXTO, ESCOPO E CRITÉRIO

O estabelecimento do escopo, contexto (interno e externo) e critérios tem como propósito personalizar o processo de gestão de riscos, permitindo um processo de avaliação de riscos eficaz e um tratamento de riscos apropriado.

O escopo, no âmbito do processo de gestão de riscos, deve ser definido tendo em vista os diferentes e variados níveis e atividades executadas no órgão. Nesse sentido, quando se inicia a aplicação da gestão de riscos, a equipe designada tem de, em primeira análise, definir o escopo que será trabalhado, o que será chamado de agora em diante de objeto da gestão de riscos (OGR). Esse objeto pode ser um objetivo, programa, processo, projeto, atividade ou outro mecanismo que ocorra dentro da instituição e tenha relação com o alcance de seus objetivos.

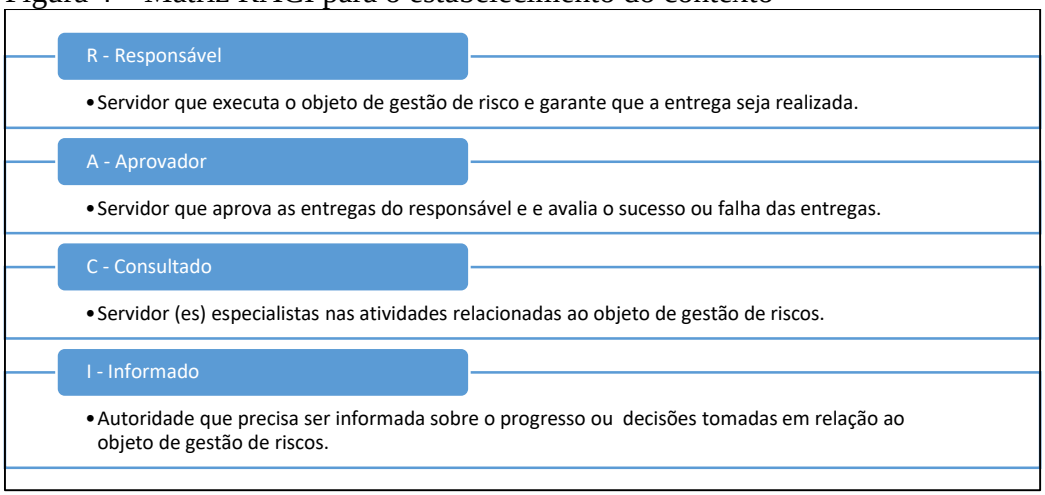
Nesse momento, serão levantadas informações acerca dos contextos externos e internos que devem ser compreendidos a partir do ambiente organizacional, dos cenários econômicos, dos objetivos institucionais. No IFCE, o estabelecimento do contexto dependerá do objeto da gestão de risco que será analisado.

O processo de estabelecimento do contexto deve respeitar todas as diretrizes da política de gestão de riscos, e deve considerar diversas variáveis: todos os atores do macroprocesso, processo ou projeto; a legislação correlacionada; os clientes; os principais problemas recorrentes; os sistemas informatizados utilizados; as partes interessadas; o ambiente externo e outras variáveis que os participantes julguem relevantes. É nessa fase que se processa o entendimento da organização no nível do objeto.

Essa etapa deve ser realizada com bastante atenção, deve envolver todos os servidores relacionados com o objeto analisado seja ele um processo, um projeto, um programa, uma atividade ou um fator que deva ser considerado no alcance da estratégia.

Para identificar os responsáveis que atuarão na fase 4.1 será utilizada uma matriz RACI para estabelecer as responsabilidades dos agentes que participarão dessa fase.

Figura 4 – Matriz RACI para o estabelecimento do contexto



Fonte: Elaboração própria

Esse processo pode se dar por meio de técnicas a exemplo do Brainstorming e do método SWOT devidamente registrados e documentados.

Figura 5 – Análise SWOT

Fonte: Elaboração própria

As informações levantadas por meio desse processo devem ser documentadas nos templates dos quadros 1 e 2.

Quadro 1 – Ficha de definição do escopo

Definição do Escopo	
Tipo de objeto de gestão de risco (*)	Processo
Descrição do objeto	Promoção de ingresso em cursos técnicos
Principais objetivos do objeto	Promover o aumento de matrículas em cursos técnicos, a permanência e conclusão.
Setor(s) ou unidade(s) organizacional a que está vinculado	PROEN – Departamento de Ensino Básico
Macroprocesso da cadeia de valor associado	Macroprocesso Finalístico 1 – Gestão da educação básica e profissional
Tema estratégico associado	Tema T1 – Publicar editais de seleção simplificados para facilitar o entendimento dos estudantes.
Objetivo estratégico associado	0E-10 Elevar a taxa de ocupação das vagas ofertadas, maximizando a utilização dos recursos disponíveis e atraindo um número maior de candidatos nos processos seletivos.
Indicador associado	Matrículas em cursos técnicos
Meta associada	No mínimo 50% das vagas ofertadas em cursos técnicos
(*) Processo, Projeto, Atividade, Outros.	

Fonte: Adaptado do Manual de Gestão de Riscos do TCU 2ed 2020

Quadro 2 – Ficha de definição do contexto interno e externo

CONTEXTO INTERNO	CONTEXTO EXTERNO
Pessoas chaves	Principais stakeholders e seus interesses
Processos de trabalho	Recursos externos
Atividades que mais agregam valor	Relevância das entregas
Problemas do passado	Entidades parceiras
Principais objetivos	Cenário político, social, econômico
Leis e normas relacionadas	
Registrar em tópicos as informações importantes para a compreensão do contexto interno e externo da Unidade. Pode-se ampliar os critérios desta ficha a depender do OGR.	

Fonte: Adaptado do Manual de Gestão de Riscos do TCU 2ed 2020

Em conformidade com o art. 23 da política de gestão de riscos do IFCE, o gerenciamento de riscos deverá ser implementado de forma gradual em todas as áreas da instituição, sendo priorizados os processos organizacionais que impactam diretamente nos resultados esperados dos macroprocessos definidos na cadeia de valor do IFCE.

Diante do exposto no parágrafo anterior e considerando que em virtude da limitação de recursos é preciso priorizar processos. A instituição, por meio do CGRC e da CGR, deve mapear processos prioritários entre os processos disponíveis para gerenciamento de riscos. A priorização de processos deve envolver pessoas com visão sistêmica da organização e ser baseada nas melhores informações disponíveis.

Na priorização de processos será utilizada a orientação do Referencial Básico de Gestão de Riscos do TCU.

Os fatores a serem considerados na priorização de processos são: a) Relevância estratégica; b) Materialidade; c) Maturidade.

O ordenamento dos processos deve ser feito com base em um índice numérico, a exemplo deste: P = RE * Mat/M

Onde: P é a prioridade do processo;
RE é a relevância estratégica do processo;
Mat é a materialidade do processo;
M é a maturidade do processo.

Quadro 3 – Escalas para medição das variáveis consideradas para a priorização de processos.

FATORES	PONTOS DE ESCALA			
	1	2	3	4
RELEVÂNCIA ESTRATÉGICA DO PROCESSO	O processo tem pouca relevância para a realização dos objetivos-chave da organização (macro produtos, macro objetivos	O processo tem média relevância para a realização dos objetivos-chave da organização.	O processo tem alta relevância para a realização dos objetivos-chave da organização.	O processo tem relevância muito alta para a realização dos objetivos-chave da organização.

	ou resultados finalísticos).			
MATERIALIDADE	Menos de 2,0% do orçamento anual.	De 2,0% a 10,0% do orçamento anual.	De 10,0% a 20,0% do orçamento anual.	Mais de 20,0 % do orçamento anual.
MATURIDADE DO PROCESSO	O processo não foi modelado ou sua modelagem não é utilizada para seu gerenciamento. Os resultados acontecem graças a iniciativas individuais. Padrões de entrega de produtos e serviços não existem ou são ignorados. Prática de "apagar incêndios".	O processo foi modelado e sua modelagem é de conhecimento dos servidores que executam o processo. Produtos e serviços costumam atender aos padrões de entrega, mas falhas significativas ainda acontecem.	A gestão do processo é feita com base em modelagem e em indicadores avaliados periodicamente. Métodos e tecnologias de gestão concentrados no nível gerencial. Produtos e serviços atendem aos padrões de entrega na grande maioria das vezes.	A gestão do processo é feita com base em modelagem e com medição de desempenho plenamente incorporada. Métodos e tecnologias de gestão amplamente utilizados pelos servidores da área. Muito raro algum produto ou serviço não atender aos padrões de entrega.

Fonte: Adaptado do Referencial Básico de Gestão de Riscos do TCU - 2018.

Quadro 4 – Objetos de gestão de risco

OBJETO DE GESTÃO DE RISCO (*)	NÍVEL DE PRIORIDADE
Processo de gestão de almoxarifado	
Programa pé de meia	
Processo de pagamento de auxílio-transporte	
(*) Processo, Projeto, Atividade, Outros.	

Fonte: Elaboração própria

Ao final do levantamento de todas as informações relativas ao escopo e contexto, estas devem ser levadas à planilha documentadora Mapa de Riscos que consignará as informações relacionadas ao contexto da organização.

4.2 PROCESSO DE AVALIAÇÃO DE RISCOS

O processo de avaliação dos riscos compreende as etapas de identificação, análise e avaliação dos riscos considerados potenciais para impedir o alcance dos objetivos.

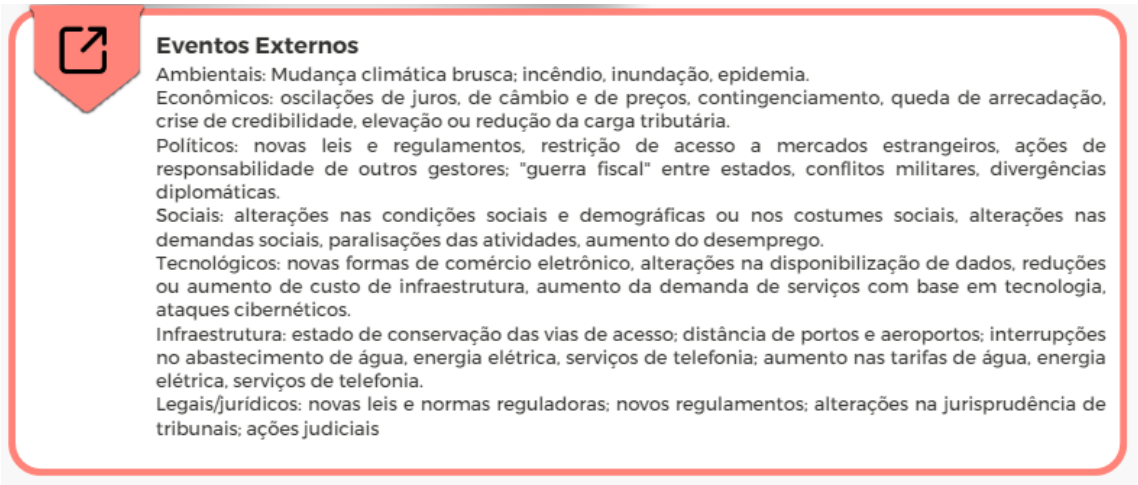
4.2.1 IDENTIFICAÇÃO DOS RISCOS

Com o objeto de gestão de riscos definido, cabe agora a identificação dos riscos relacionados aos seus objetivos/resultados. O propósito da identificação de riscos é encontrar, reconhecer e descrever riscos que possam ajudar ou impedir que uma organização alcance seus objetivos.

De acordo com a ISO 31000, a identificação de riscos é o processo da busca, reconhecimento e descrição dos riscos; envolvendo a identificação das fontes de risco, eventos, causas e consequências potenciais. A identificação dos riscos deve ser realizada em oficinas de trabalho ou, dependendo do objeto, pelo próprio gestor do risco.

As fontes de riscos podem ser exemplificadas como na figura 6:

Figura 6: Definições e exemplos de fontes de riscos e vulnerabilidades



Fonte: Adaptado do Manual de Orientações Técnicas da CGU/2017.

No processo de identificação de riscos, deve-se buscar a participação de pessoas que conheçam bem o objeto de gestão de riscos, executores do objeto, pessoas em níveis estratégico e tático e outros consultados. Deve-se considerar a mesma matriz RACI utilizada no estabelecimento do contexto para essa fase.

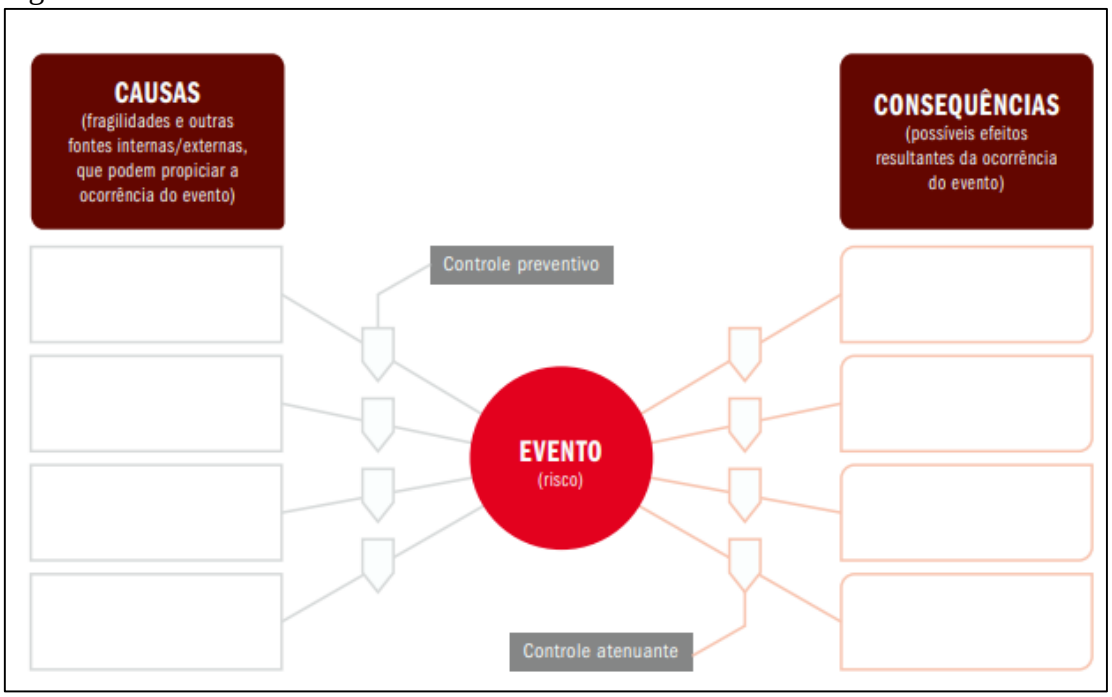
Figura 7: Definições e exemplos de categorias de riscos

Fonte: Guia Prático para a implementação da Gestão de Riscos no Poder Executivo Estadual do Ceará/2024.

A organização pode usar uma variedade de técnicas para identificar incertezas que podem afetar um ou mais objetivos, e que permitam a coleta do maior número de riscos, tais como: brainstorming, brainwriting, entrevistas, visitas técnicas, pesquisas etc.

Na identificação do evento de risco pode-se utilizar como técnica a análise BOW TIE.

Figura 8 – Análise Bow Tie



Fonte: RBG TCU - 2018

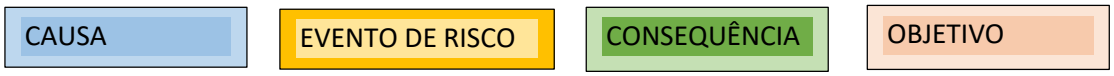
Como forma complementar de orientação, Rodrigo Fontenele traz a seguinte sintaxe em seu curso:

Figura 9 – Sintaxe da Identificação de risco

Devido à <CAUSA>, poderá acontecer <RISCO>, o que poderá levar à <CONSEQUÊNCIA> impactando no/na <OBJETIVO>.

Fonte: Curso de Gestão de Riscos – Da teoria à prática. Rodrigo Fontenelle, 2024.

Exemplo (Rodrigo Fontenelle): Devido ao **[contato direto dos empregados da área de licitações com fornecedores**], poderá acontecer o **[oferecimento ou solicitação de pagamento indevido]**, o que poderá levar à **[corrupção dos empregados**] impactando na **[entrega de bens à população]**.



Quadro 5 - Ficha de Identificação de Riscos

Objeto de gestão de risco (processo, projeto, programa, etc)	Participantes do processo de identificação do risco	Objetivos/resultado do objeto de gestão de risco	Fonte de Risco	Risco	Causas	Consequências (impactos nos objetivos)	Categoria do Risco

Fonte: Adaptado do Manual gestão de Riscos - TCU 2Ed 2020 e (ISO 31000:2018) (Referencial Básico de Gestão de Riscos – TCU)

As informações dessa fase deverão ser consignadas na planilha documentadora Mapa de Riscos.

4.2.2 ANÁLISE DOS RISCOS

Conforme a ISO 31000/2018: O propósito da análise de riscos é compreender a natureza do risco e suas características, incluindo o nível de risco, onde apropriado. A análise de riscos envolve a consideração detalhada de incertezas, fontes de risco, consequências, probabilidade, eventos, cenários, controles e sua eficácia. Um evento pode ter múltiplas causas e consequências e pode afetar múltiplos objetivos.

Para o TCU, o risco é uma função tanto da probabilidade como das medidas das consequências.

Risco = *f*(Probabilidade e Impacto)

Diante dos conceitos apresentados, o IFCE irá, a partir dos riscos já mapeados na etapa de identificação de riscos, analisá-los e classifica-los em uma matriz de riscos.

A análise dos riscos pelos responsáveis considerará a probabilidade, o impacto e o efeito dos controles existentes e classificará os riscos quanto ao nível de criticidade.
Os quadros 6 e 7 apresentam as escalas de probabilidade e impacto que serão consideradas na análise de cada risco.

Quadro 6 – Escala de probabilidade

Classificação	Descrição da probabilidade, desconsiderando os controles	Peso
Muito baixo	Improvável. Em situações excepcionais, o evento poderá até ocorrer, mas nada nas circunstâncias indica essa possibilidade.	1
Baixo	Rara. De forma inesperada ou casual, o evento poderá ocorrer, pois as circunstâncias pouco indicam essa possibilidade.	2
Médio	Possível. De alguma forma, o evento poderá ocorrer, pois as circunstâncias indicam moderadamente essa possibilidade.	5
Alto	Provável. De forma até esperada, o evento poderá ocorrer, pois as circunstâncias indicam fortemente essa possibilidade.	8
Muito Alto	Praticamente certa. De forma inequívoca, o evento ocorrerá, as circunstâncias indicam claramente essa possibilidade.	10

Fonte: Adaptado do RBG/TCU

Quadro 7 – Escala de impacto

Classificação	Descrição do impacto nos objetivos, caso o evento ocorra	Peso
Muito baixo	Mínimo impacto nos objetivos (estratégicos, operacionais, de informação/comunicação/divulgação ou de conformidade).	1
Baixo	Pequeno impacto nos objetivos (idem).	2
Médio	Moderado impacto nos objetivos (idem), porém recuperável.	5
Alto	Significativo impacto nos objetivos (idem), de difícil reversão.	8
Muito Alto	Catastrófico impacto nos objetivos (idem), de forma irreversível.	10

Fonte: Adaptado do RBG/TCU

A escala de classificação após a pontuação de cada risco seguirá o disposto no Quadro 8

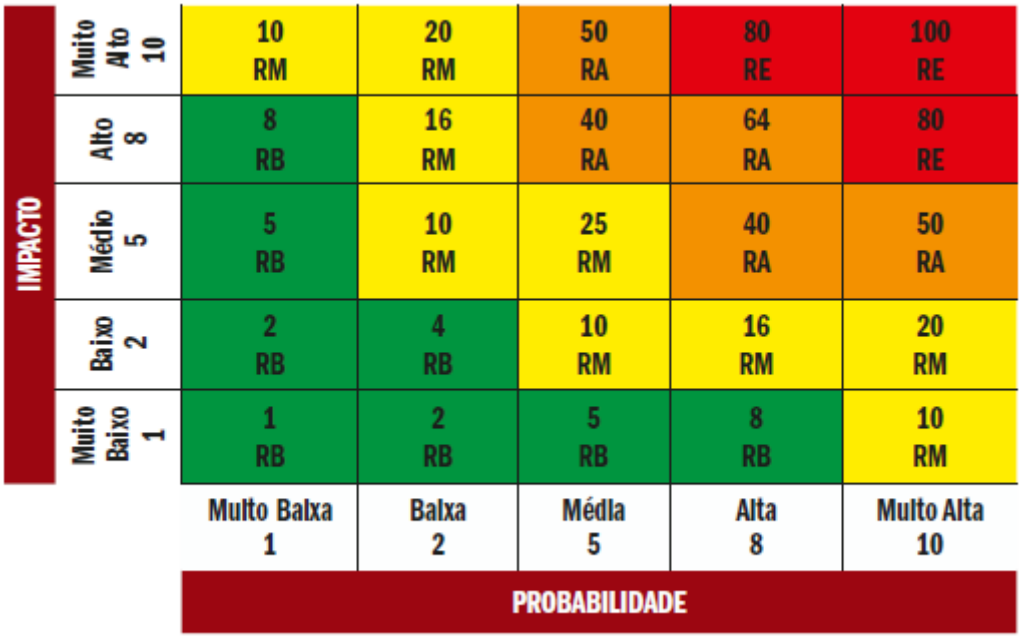
Quadro 8 – Escala de classificação de risco

RB (Risco Baixo)	RM (Risco Médio)	RA (Risco Alto)	RE (Risco Extremo)
0 – 9,99	**10 – 39,99**	**40 – 79,99**	**80 - 100**

Fonte: Adaptado do RBG/TCU

Os resultados das combinações possíveis de riscos deverão estar expressos em uma matriz de riscos

MATRIZ DE RISCOS



Nessa fase, a CGR deverá reunir os responsáveis pelo objeto de gestão de risco que está sendo analisado para, de forma qualitativa, estabelecerem a pontuação em termos de probabilidade e impacto de cada risco identificado. Devem ser utilizadas técnicas para levantamento dessas informações, uma vez que a pontuação será aplicada com base na percepção das pessoas.

A CGR deverá documentar essa fase preenchendo a ficha de análise de riscos inerentes da tabela 1.

Tabela 1 – Ficha de análise de riscos inerentes

Riscos Identificados	Probabilidade	Impacto	Nível de Risco Inerente (NRI)
Risco 1 – Descrição do risco 1	8	10	**80**
Risco 2 – Descrição do risco 2	5	8	**40**
Risco 3 – Descrição do risco 3	2	5	**10**
Risco n – Descrição do risco n	1	5	**5**

Fonte: Adaptado do RBG/TCU

Se necessário, deve-se voltar para a fase de identificação e observar as causas e consequências do risco, a fim de se aproximar o máximo possível de informações fidedignas.

Os riscos serão classificados nos níveis baixo, médio, alto e extremo.

Nessa fase o risco que está sendo analisado é denominado de risco inerente (RI). O nível de risco inerente (NRI) é o nível de risco antes da consideração das respostas que a Administração adota para reduzir a probabilidade do evento ou os seus impactos nos objetivos, incluindo controles internos.

Após a classificação quanto ao nível de criticidade considerando a probabilidade e o impacto, será considerado o efeito dos controles existentes, que pode ensejar a revisão da classificação e das medidas e controles a serem adotados, conforme tabelas 2 e 3.

Trata-se do cálculo do Nível de Risco Residual, ou seja, a magnitude do risco após a implementação dos controles internos que a gestão adota para responder ao risco. Esse cálculo deve ser feito aplicando-se um fato multiplicador aos resultados da tabela 1.

Nível de risco residual = Nível de risco inerente x Risco de controle

Quadro 9 – Ficha de descrição dos controles internos existentes

Riscos Identificados	Descrição dos controles aplicados pela gestão (Descreva 1 ou mais controles)
Risco 1	
Risco 2	
Risco 3	
Risco n	

Fonte: Elaboração própria

Tabela 2: Escala de definição do fator efeito dos controles internos

NÍVEL DE CONFIANÇA (NC)	AVALIAÇÃO DO DESENHO E IMPLEMENTAÇÃO DOS CONTROLES (ATRIBUTOS DO CONTROLE)	RISCO DE CONTROLE (RC)
Inexistente NC = 0% (0,0)	Controles inexistentes, mal desenhados ou mal implementados, isto é, não funcionais.	Muito Alto **1,0**
Fraco NC = 20% (0,2)	Controles têm abordagens ad hoc, tendem a ser aplicados caso a caso, a responsabilidade é individual, havendo elevado grau de confiança no conhecimento das pessoas.	Alto **0,8**
Mediano NC = 40% (0,4)	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.	Médio **0,6**
Satisfatório NC = 60% (0,6)	Controles implementados e sustentados por ferramentas adequadas e, embora passíveis de aperfeiçoamento, mitigam o risco satisfatoriamente.	Baixo **0,4**
Forte NC = 80% (0,8)	Controles implementados podem ser considerados a "melhor prática", mitigando todos os aspectos relevantes do risco.	Muito Baixo **0,2**

Fonte: RBG TCU, 2018.

Tabela 3: Ficha de análises de riscos residuais

Riscos Identificados	P	I	Nível de Risco Inerente (NRI)	Eficácia do Controle	Risco de Controle (RC)	Nível de Risco Residual (NRR)
Risco 1	8	10	**80**	**Inexistente**	**1,0**	**80**
Risco 2	5	8	**40**	**Mediano**	**0,6**	**24**
Risco 3	2	5	**10**	**Fraco**	**0,8**	**8**
Risco 4	8	9	**72**	**Satisfatório**	**0,4**	**29**
Risco n	1	5	**5**	**Forte**	**0,2**	**1**

Fonte: Adaptado do RBG/TCU

As percepções da equipe quando da pontuação do nível de confiança dos controles existentes deve ser documentada em ata.

As informações dessa fase deverão ser consignadas na planilha documentadora Mapa de Riscos.

4.2.3 AVALIAÇÃO DOS RISCOS

Conforme a ISO 31000/2018, "A avaliação de riscos envolve a comparação dos resultados da análise de riscos com os critérios de risco estabelecidos para determinar onde é necessária ação adicional. "

Para o TCU, "A finalidade da avaliação de riscos é auxiliar na tomada de decisões, com base nos resultados da análise de riscos, sobre **quais riscos necessitam de tratamento** e a prioridade para a implementação do tratamento".

Nessa fase, de posse dos riscos residuais calculados quando da fase de análise de riscos, o Comitê de Governança deverá decidir frente à declaração de apetite a risco já estabelecida, quais os riscos serão tratados e quais estarão dentro do apetite de modo que estes não demandarão esforços excessivos posto que estão sob controle da organização.

Desse modo, é imprescindível a análise da declaração do apetite a risco para a definição dos riscos que serão levados para a próxima fase: tratamento. Além disso, dentre os riscos que serão tratados, deverão ser definidos, nesta fase, critérios de priorização.

Quadro 10 – Critérios de priorização de riscos

Riscos Identificados	NRR	Está dentro do Apetite a risco?
Risco 1	BAIXO	SIM
Risco 2	MÉDIO	SIM
Risco 3	ALTO	NÃO
Risco n	EXTREMO	NÃO

Fonte: Elaboração própria

A ordem de priorização dos riscos deverá ser documentada na Planilha de Riscos.

4.2.4 TRATAMENTO DOS RISCOS

O tratamento de riscos envolve a seleção de uma ou mais opções para modificar o nível de cada risco e a elaboração de planos de tratamento que, uma vez implementados, implicarão em novos controles ou modificação dos existentes. (RBG/TCU)

Conhecido o nível de risco residual, verifique qual estratégia a ser adotada para responder ao evento de risco. A escolha da estratégia dependerá do nível de exposição a riscos previamente estabelecido pela organização em confronto com a avaliação que se fez do risco.

O tratamento dos riscos deve seguir os seguintes passos (TCU, 2018): Identificar medidas de resposta ao risco. Avaliar a viabilidade da implantação dessas medidas (custo

benefício, viabilidade técnica, etc.). Decidir quais serão implementadas. Elaborar plano de implementação das medidas para inclusão nos planos institucionais.

As opções de tratamento do risco incluem: Evitar, Mitigar, Transferir ou Aceitar.

Quadro 11 – Opções de tratamento de riscos

Evitar	Mitigar	Transferir	Aceitar
É a decisão de não iniciar ou de descontinuar a atividade, ou ainda desfazer-se do objeto sujeito ao risco.	Consiste em adotar medidas para reduzir a probabilidade ou a consequência dos riscos ou até mesmo ambos.	É o caso especial de se mitigar a consequência ou probabilidade de ocorrência do risco por meio da transferência ou compartilhamento de uma parte do risco, mediante contratação de seguros ou terceirização de atividades nas quais a organização não tem suficiente domínio.	É não tomar, deliberadamente, nenhuma medida para alterar a probabilidade ou a consequência do risco. Ocorre quando o risco está dentro do nível de tolerância da organização capacidade para fazer qualquer coisa sobre o risco é limitada ou, ainda, o custo de tomar qualquer medida é desproporcional em relação ao benefício potencial

Fonte: RBR/TCU

É importante refletir, quando da decisão de qual resposta será dada ao risco, os seguintes fatores: As ações de mitigação devem ter um custo benefício positivo e um eventual plano de ação deve ser eficaz na redução do risco. A transferência de risco não elimina uma ameaça, simplesmente faz com que a outra parte seja responsável pelas perdas econômicas/físicas conectadas. As organizações transferem para terceiros (companhias de seguros, mercados de derivativos etc.), principalmente, quando o custo de transferência é menor ou igual a perda esperada.

De acordo com o **Quadro 10 do item 4.2.3**, deverão ser implementados controles internos para os riscos cujo nível de risco residual esteja entre Médio e Extremo. Para isso, deve ser estabelecido um plano de tratamento com definição dos controles que serão implementados (O que?); a área responsável pela implementação (Onde?); os responsáveis pela implementação (Quem?); de que forma (por meio de) os controles serão implementados (Como?); em qual período de tempo os controles deverão ser implementados ou o tempo de resposta que esse controle deve fornecer para a gestão (Quando?).

Essas variáveis devem ser definidas em conjunto por pessoas relacionadas com o risco identificado e devem ser realizadas consultas às áreas detentoras de informações chaves como orçamento disponível, legalidade do controle e outras informações que sejam necessárias para a tomada de decisão na definição do controle. Informações relevantes

devem ser registradas em ata ou documentadas de forma que essa informação seja rastreável para possíveis revisões de controles.

Essa fase também deverá ser levada à Planilha de Riscos.

5. MONITORAMENTO E ANÁLISE CRÍTICA

Segundo a ISO, o propósito do monitoramento e análise crítica é assegurar e melhorar a qualidade e eficácia da concepção, implementação e resultados do processo. Convém que o monitoramento contínuo e a análise crítica periódica do processo de gestão de riscos e seus resultados sejam uma parte planejada do processo de gestão de riscos, com responsabilidades claramente estabelecidas.
A norma técnica ISO também ressalta que o monitoramento deve ocorrer em todas as fases do processo.

No processo de gerenciamento de riscos no IFCE, serão consideradas as ações, os responsáveis e os prazos para a fase de monitoramento que deverão estar consignadas na plataforma designada para o gerenciamento de riscos.

O QUE?	QUEM?	QUANDO?
Avaliar os controles internos e acompanhar o sucesso das medidas mitigadoras estabelecidas, propondo, se necessário alterações nos controles, nos responsáveis, no período.	Os gestores do risco	No mínimo semestralmente

6. COMUNICAÇÃO E CONSULTA

De acordo com a ISO, a comunicação busca promover a conscientização e o entendimento do risco, enquanto a consulta envolve obter retorno e informação para auxiliar a tomada de decisão.
A comunicação entre todos os integrantes do processo de gestão de riscos deve estar clara e consignada em um fluxo padronizado a ser obedecido rigorosamente pelas partes.

7. REGISTRO E RELATO

A fase de registro e relato do processo de gerenciamento de riscos constitui uma importante e imprescindível etapa.
Nessa fase, a coordenadoria de gestão de riscos deverá consolidar, pelo menos a cada dois anos, os resultados alcançados na perspectiva dos riscos mitigados, dos controles implementados e do cenário atualizado do mapa de riscos.
Essa consolidação que deverá ser consignada em um relatório de gestão de riscos só será possível se cada gestor de risco implementar os controles estabelecidos e monitorar os riscos de seus objetos.
Esse relatório deverá ser publicado e divulgado para toda a instituição com a finalidade de promover a transparência e a prestação de contas das principais entregas do órgão.

8. REFERÊNCIAS BIBLIOGRÁFICAS

BRASIL. Tribunal de Contas da União. Referencial Básico de Gestão de Riscos, 2018. Disponível em: https://portal.tcu.gov.br/referencial-basico-de-gestao-de-riscos.htm.

Prefeitura Municipal de Fortaleza. Gestão de Riscos – Teoria e Metodologia, 2022. Disponível em: https://transparencia.fortaleza.ce.gov.br/index.php/legislacao/controle_interno/outros.

Controladoria e Ouvidoria Geral do Poder Executivo do Estado do Ceará. Guia Prático para a Implementação da Gestão de Riscos no Poder Executivo Estadual do Ceará, 2024. Disponível em: https://www.cge.ce.gov.br/wp-content/uploads/sites/20/2024/07/Guia-Pratico-para-a-Implementacao-da-Gestao-de-Riscos-no-Poder-Executivo-Estadual-do-Ceara-2024_v4.pdf.

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

Manual de Gestão de Riscos da Universidade Federal do Amazonas, 1ª edição, 2023. Disponível em: https://proplan.ufam.edu.br/index.php/gestao-de-riscos?id=282.

Declaração de Posicionamento do IIA - Instituto dos Auditores Internos: As Três Linhas de Defesa no Gerenciamento Eficaz de Riscos e Controles.

Committee of Sponsoring Organizations of the Treadway Commission (COSO). Gerenciamento de Riscos Corporativos – Integrado com Estratégia e Performance. Sumário Executivo, 2017. Disponível em: https://repositorio.cgu.gov.br/bitstream/1/74040/1/Coso_portugues_versao_2017.pdf