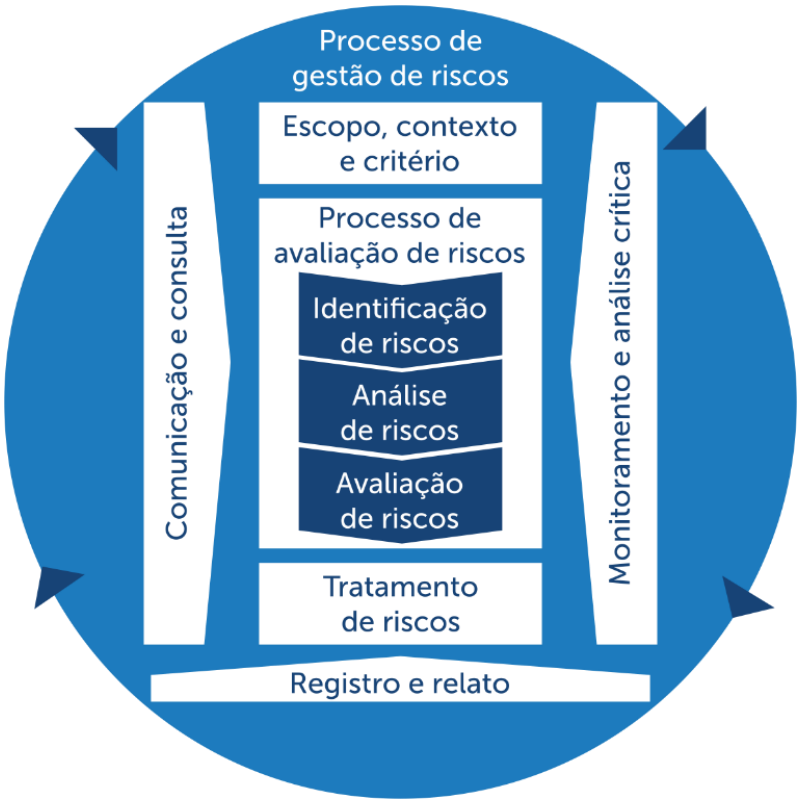
Anexo 10
Gerenciamento de Riscos das Ações

GERENCIAMENTO DE RISCOS DE EXECUÇÃO DOS RESULTADOS-CHAVESDO PDTIC

Seguem abaixo diretrizes para o gerenciamento de riscos dos resultados-chaves do PDTIC 2025-2028:

1. Macroprocesso de Gestão de Riscos



Para realizar a gestão de riscos, as seguintes etapas devem ser seguidas:

a) **estabelecimento do contexto**: Consiste em compreender o ambiente externo e interno no qual o objeto de gestão de riscos se encontra inserido e em identificar parâmetros e critérios a serem considerados no processo de gestão de riscos;
b) **identificação dos riscos**: Compreende o reconhecimento e a descrição dos riscos relacionados aos objetivos/resultados de um objeto de gestão de riscos, envolvendo a identificação de possíveis fontes de riscos;
c) **análise dos riscos**: É o desenvolvimento da compreensão sobre o risco e à determinação do nível do risco;

d) **avaliação dos riscos**: A avaliação do risco envolve a comparação do seu nível com o limite de exposição a riscos, a fim de determinar se o risco é aceitável;
e) **tratamento dos riscos**: Compreende o planejamento e a realização de ações para modificar o nível do risco;
f) **comunicação e consulta com partes interessadas**: Refere-se à identificação das partes interessadas e ao compartilhamento de informações relativas à gestão de riscos sobre determinado objeto, observada a classificação da informação quanto ao sigilo;
g) **monitoramento**: Compreende o acompanhamento e a verificação do desempenho ou da situação de elementos da gestão de riscos, podendo abranger a política, as atividades, os riscos, os planos de tratamento de riscos, os controles e outros assuntos de interesse; e
h) **melhoria contínua**: Compreende o aperfeiçoamento ou ajuste de aspectos da gestão de riscos avaliados no monitoramento.

2. Quantidade de Riscos

Preferencialmente, os demandantes devem elencar, pelo menos, 3 (três) riscos, por resultado-chave.

3. Categorias do Risco

As categorias de riscos decorrem da experiência adquirida pela DTI no monitoramento de suas ações internas e do PDTIC 2020 – 2023, ao longo do seu período de vigência, além de considerar a Política de Gestão de Riscos e Controles Internos da Fundação Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - CAPES – Portaria nº 301, de 22 de dezembro de 2022.

A lista inicial de categorias de risco é:

ID	CATEGORIA	DEFINIÇÃO
1	Risco Conformidade	Risco relacionado à legislação e recomendações de controle.
2	Risco Contratual	Risco decorrente de contratos ou que impactam contratos.
3	Risco de Cadastro	Risco de cadastro incorreto da ação no PDTIC.
4	Risco de Capacidade	Risco de ausência de recursos necessários (capacidade de execução).
5	Risco de Confidencialidade	Risco de pessoas não-autorizadas (não legitimamente autorizados pelo proprietário das informações) acessarem a informação.
8	Risco de Descontinuidade	Risco de descontinuidade da solução ou serviço.

9	Risco de Escopo	Risco relacionado à definição incorreta, à desatualização ou incompletude do escopo.
6	Risco de Falta de Integridade	Risco de as características da mensagem original serem alteradas, ou seja, de os dados serem indevidamente alterados.
11	Risco de Flutuação de Câmbio	Risco de as flutuações de câmbio afetarem a execução da ação.
12	Risco de Gestão	Risco de problemas relacionados às atividades de gestão da organização ou da área.
13	Risco de Gestão de Projetos	Risco de problemas relacionados à atividade de gestão de projetos.
14	Risco de Governança	Risco de problemas relacionados à governança corporativa, digital, de TIC, de contratações ou de dados.
7	Risco de Indisponibilidade (solução/infra)	Risco de indisponibilidade das informações ou da solução.
15	Risco de Prazo	Risco de atraso.
16	Risco de Priorização	Risco de ausência de priorização, ou incorreção na priorização.
17	Risco de Proteção de Dados	Risco relacionado à proteção de dados.
20	Risco de SIC	Risco relacionado à segurança das informações.
21	Risco Estratégico	Risco relacionado ao alinhamento estratégico com os objetivos da organização ou de TIC (plano estratégico, tático ou outros).
22	Risco Negocial	Risco relacionado negócio da organização.
23	Risco Orçamentário/Financeiro	Risco relacionado à recursos orçamentários ou financeiros.
24	Risco Político	Risco relacionado às mudanças do cenário político.
25	Risco Reputacional ou de Imagem	Riscos relacionado à imagem organizacional ou da área de TIC.
26	Risco Técnico	Risco relacionado às questões técnicas operacionais.
27	Risco Tecnológico	Risco relacionado à questões tecnológicas.

Esta lista poderá ser alterada durante a execução do PDTIC, para melhor alinhamento do gerenciamento de riscos com a realidade fática encontrada.

4. Descrição do Risco (Sintaxe)

SINTAXE:

A sintaxe adotada será:

> **Devido a <CAUSAS/FONTES>, poderá acontecer <DESCRIÇÃO DA INCERTEZA>, o que poderá levar a <DESCRIÇÃO DO IMPACTO/CONSEQUÊNCIA/EFEITO> impactando no/na <DIMENSÃO DE OBJETIVO IMPACTADA>**

Exemplo 1: **Devido a** <desorganização da equipe, os pagamentos referentes à execução contratual> **poderão <**não ocorrer tempestivamente>, **o que poderá levar ao** <pagamento de encargos de mora> **implicando em** <um dispêndio excedente de recursos do órgão>.

Exemplo 2: **Devido a** <erro no registro de período de férias dos servidores>, **poderá acontecer o** <não pagamento de vantagens devidas>, **o que poderá levar ao** <enriquecimento ilícito do erário> **impactando na** <folha de pagamento de pessoal>.

Exemplo 3: **Devido a** <falta de padronização de requisitos para contratações com objetos semelhantes>, **poderá acontecer de o** <termo de referência conter requisitos inadequados>, **o que poderá levar a** <dificuldade em escolher a proposta mais vantajosa; desperdício de recursos públicos> **impactando no** <processo de contratações públicas>.

Exemplo 4: **Devido a** <falha no cálculo e especificação de vigas de sustentação>, **poderá acontecer a** <queda de parte da estrutura da obra>, **o que poderá levar ao** <atraso no cronograma da obra; dano físico irreparável em trabalhadores> **impactando na** <construção do prédio>.

INCERTEZA:

Risco é a incerteza envolvida na obtenção de um resultado ou um objetivo. A **incerteza** surge da possibilidade de se obter um resultado inesperado ou indesejado. Risco está relacionado à imprevisibilidade dos resultados desejáveis, ou seja, o risco não é necessariamente uma certeza, é **algo que pode acontecer ou não** e **pode gerar um dano ou não**.

Incerteza é a falta de informação ou de conhecimento sobre o resultado de uma ação, decisão ou evento. A **incerteza** existe sempre que não se sabe precisar o que vai ocorrer no futuro. O risco é a **incerteza** que possui potencial para afetar o **alcance de um objetivo, a execução de um planejamento** e até mesmo a saúde e a integridade física das pessoas.

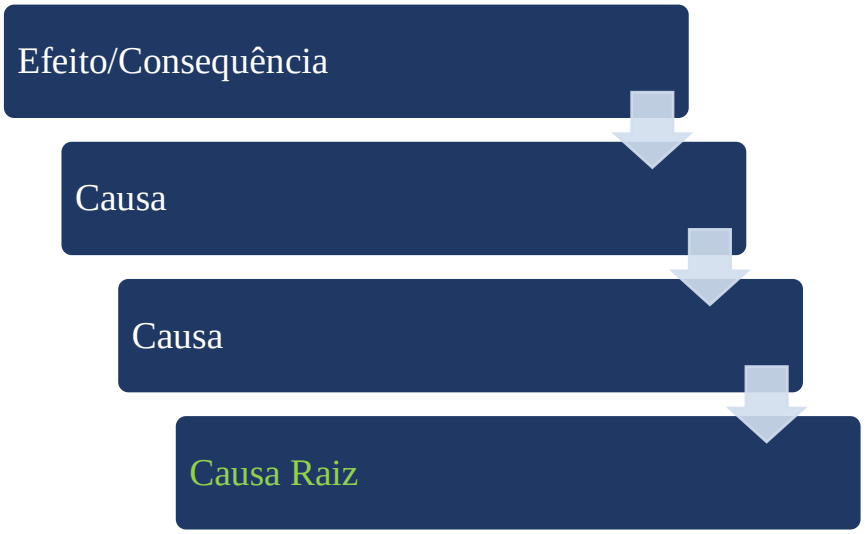
CAUSA:

Deve-se evitar a confusão entre os eventos de risco com suas causas e consequências. Para descrever o risco, é necessário estabelecer, de forma clara, a relação entre **causa** e **consequência**, que são:

a) **Causa:** Situações ou motivos que podem promover a ocorrência do risco; e
b) **Consequência**: Resultados do risco que afetam os objetivos de TIC ou objetivos estratégicos da CAPES (descritos no PEI).

Pode existir mais de uma **causa** para um mesmo evento de risco.

Para identificar a **causa**, é necessário chegar na **causa raiz** do risco, que muitas vezes pode ser a "causa da causa":



A **causa** é composta da **fonte do risco** e da **vulnerabilidade** ou **fragilidade** – que precisam ser identificadas.

Exemplo: O evento de risco “má elaboração do termo de referência” pode ter como fonte “pessoas” e como vulnerabilidade “sem capacitação adequada”. Portanto, a causa do risco seria: “pessoas sem capacitação adequada”.

CONSEQUÊNCIAS:

As **consequências, impactos ou efeitos** de um evento de risco serão determinadas após a sua identificação e podem ser verificadas em maior número que o próprio evento. Elas influenciarão diretamente a análise de **impact**o.

OBJETIVO:

Identificar o **objetivo estratégico (PEI) ou de TIC (PDTIC)** que pode ser impactado pelo risco.

5. Probabilidade (de acontecer)

MENSURAÇÃO QUANTITATIVA:

PROBABILIDADE	DESCRIÇÃO	ESCALA
Muito alto	acima de 90%	**5**
Alto	de 50,1% a 90%;	**4**
Médio	de 30,1% a 50%	**3**
Baixo	de 5,1% a 30%	**2**
Muito baixo	até 5%.	**1**

MENSURAÇÃO QUALITATIVA 1:

PROBABILIDADE	DESCRIÇÃO	ESCALA
Muito alta	Pode ser que ocorra semanalmente;	**5**
Alta	Pode ser que ocorra mensalmente;	**4**
Média	Pode ser que ocorra mais de uma vez dentro de um ano;	**3**
Baixa	Pode ser que ocorra uma vez dentro de um ano; e	**2**
Muito baixa	Não é provável que aconteça.	**1**

MENSURAÇÃO QUALITATIVA 2:

PROBABILIDADE	DESCRIÇÃO	ESCALA
Muito alto	Muito Provável. Certamente ocorrerá na maioria das circunstâncias	**5**
Alto	Provável. Provavelmente ocorrerá na maioria das circunstâncias	**4**
Médio	Possível. Pode ocorrer em algum momento	**3**
Baixo	Improvável. Poderia ocorrer em circunstâncias excepcionais	**2**
Muito baixo	Muito improvável. Poderia ocorrer em circunstâncias extremamente excepcionais	**1**

6. Impacto (dano)

MENSURAÇÃO CRITÉRIO 1:

IMPACTO	DESCRIÇÃO	ESCALA
Muito alto	Eventos que causem danos extremamente complexos, de elevado custo e de difícil reparação; ou com repercussão negativa em nível nacional e internacional; ou acarretem inconformidade legal ou perante órgãos reguladores/de controle; ou que acarretem alto risco de indenizações decorrentes de ação judicial ou de controle; ou ainda que causem indisponibilidade de serviços ou soluções negociais ou de TIC	5
Alto	Eventos que causem danos complexos, de elevado custo e com razoável dificuldade de reparação; ou com repercussão negativa em nível nacional; ou que acarretem razoável risco de indenizações decorrentes de ação judicial ou de controle; ou ainda que causem paralisação parcial de serviços ou soluções negociais ou de TIC.	4
Médio	Eventos que causem danos de moderada dificuldade de reparação; ou com repercussão negativa em nível organizacional (CAPES); ou ainda que causem intermitência em serviços ou soluções negociais ou de TIC	3
Baixo	Eventos que causem danos de fácil reparação; ou com repercussão negativa em apenas algumas unidades	2

	organizacionais; ou ainda que causem dificuldade na utilização dos serviços ou soluções negociais ou de TIC.	
Muito baixo	Eventos que causem danos de muito fácil reparação.	1

MENSURAÇÃO CRITÉRIO 2:

IMPACTO	DESCRIÇÃO	ESCALA
Muito alto	Catastrófico. Impacto máximo nos objetivos, sem possibilidade de reparação/recuperação.	5
Alto	Maior. Impacto significante nos objetivos, com possibilidade remota de reparação/recuperação.	4
Médio	Moderado. Impacto moderado nos objetivos, com possibilidade de reparação/recuperação.	3
Baixo	Menor. Impacto mínimo nos objetivos, com possibilidade de fácil de reparação/recuperação.	2
Muito baixo	Insignificante. Impacto insignificante nos objetivos, dispensadas medidas de reparação/recuperação.	1

7. Nível de Risco

A avaliação dos riscos fornece subsídios para a tomada de decisão, não se constituindo em fator determinante para eventual tratamento do risco. Ou seja, cabe ao gestor, diante da lista de riscos ordenados por nível de risco, decidir quais merecerão ações mitigadoras.

Matriz de Impacto x Probabilidade:

Impacto						
	Muito Alto	15	19	22	24	25
	Alto	10	14	18	21	23
	Médio	6	9	13	17	20
	Baixo	3	5	8	12	16
	Muito Baixo	1	2	4	7	11
		Muito Baixa	Baixa	Média	Alta	Muito Alta
		Probabilidade				

Fonte: Manual de Riscos do TCU

O **nível do risco** é dado pelo **número inscrito em cada célula** da matriz, **não é obtido por qualquer fórmula matemática**. São 25 possíveis níveis de risco, em que cada nível está associado a uma estimativa de probabilidade e de impacto. A matriz ordena os possíveis níveis de risco, desde o mais baixo, ao qual é atribuído o nível 1 (evento muito raro, de impacto muito

baixo), até o mais elevado, ao qual se atribui o nível 25 (evento praticamente certo e de impacto muito alto).

Considerações importantes sobre o uso da matriz de Impacto x Probabilidade:

a) O **impacto é a dimensão mais importante**: um evento de impacto muito alto e de probabilidade de ocorrência muito baixa deve preocupar o gestor muito mais do que o oposto, um evento de probabilidade muito alta e impacto muito baixo – **se o impacto é mínimo, para que se preocupar?**

   Relaciona-se com a teoria do **risco cisne negro**, ou seja, um risco com impacto extremamente elevado (consequência catastrófica) e baixíssima probabilidade, considerado **difícil de ser previsto ou prevenido**, demandando atenção dos gestores, que devem tratar do assunto com a alta administração. Exemplo: Pandemia Covid-19; e

b) Atribuição de valores arbitrários: **Não foi utilizada** uma matrize que "calcula" o nível do risco pela soma ou multiplicação desses valores, dado o risco de distorção trazido por matrizes simétricas, que consideraram como do mesmo nível os riscos. Na matriz acima apresentada, um risco com probabilidade rara e impacto muito alto é classificado como de nível 15, enquanto outro risco de probabilidade praticamente certa e impacto muito baixo é considerado de nível 11, ou seja, é menos prioritário para a ação do gestor do que o de nível 15.

LIMITES DE EXPOSIÇÃO AO RISCO:

Considerar as seguintes faixas de limites a exposição ao risco:

a) Riscos acima do limite de exposição (nível 20 a 25): **faixa vermelha**;
b) Riscos com necessidade de monitoramento (nível 7 a 19): **faixa amarela**; e
c) Riscos que podem ser aceitos (nível 1 a 6): **faixa verde.**

A avaliação dos riscos fornece subsídios para a tomada de decisão, não se constituindo em fator determinante para eventual tratamento do risco. Ou seja, cabe ao gestor, diante da lista de riscos ordenados por nível de risco, decidir quais merecerão ações mitigadoras.

8. Resposta ao Risco

Tipos de resposta aos riscos (não se trata aqui de eventuais oportunidades, positivas):

a) **Aceitar**: Esta técnica indica que a equipe envolvida na ação decidiu não trocar o plano original para negociar com um risco ou não é possível fazer algo para identificar alguma outra estratégia de resposta apropriada. A aceitação ativa pode incluir desenvolver um plano de contingência para executar quando ocorrer um risco. A aceitação passiva não requer ação, deixando a equipe de projeto fazer um arranjo quando o risco ocorrer;

b) **Evitar:** Evitar o risco é mudar o plano da ação para eliminar o risco ou a condição ou para proteger os objetivos da ação ou do PDTIC destes impactos. Embora a equipe envolvida não possa eliminar todos os eventos de risco, alguns riscos específicos podem ser evitados. Alguns eventos de risco que surgem cedo podem ser evitados com esclarecimentos, obtendo-se informações, melhorando a comunicação ou consultando especialistas. Reduzindo escopo para evitar atividades de alto risco, acrescentando recursos ou tempo, adotando uma abordagem familiar em vez de uma inovação, ou evitando um fornecedor desconhecido podem ser exemplos de evitar o risco;

c) **Mitigar**: A mitigação procura reduzir a probabilidade e/ou consequências de um evento de risco adverso para um aceitável. Tomar ações cedo para reduzir a probabilidade de uma ocorrência ou impacto na ação é mais eficaz que tentar reparar as consequências depois de ocorrido. A mitigação de custos deve ser apropriada, dando a provável probabilidade do risco e suas consequências. Onde não é possível reduzir a probabilidade, a mitigação da resposta pode abarcar o impacto do risco para determinar a severidade. Por exemplo, desenhando redundâncias no subsistema pode reduzir o impacto que resultem de falhas de um componente original;

d) **Remover a fonte:** O objetivo dessa resposta é remover a fonte que dá origem ao risco. As principais fontes de risco são: equipamentos, regulamentos, pessoas e ambiente; ou

e) **Transferir**: Transferir o risco é procurar mudar a consequência de um risco para um terceiro junto com a responsabilidade da resposta. Transferindo o risco, daremos a outro a responsabilidade para gerenciar isso, mas o risco não é eliminado. Transferir risco quase sempre envolve pagamentos de um valor para que o terceiro assuma este risco. Inclui, por exemplo, o uso de seguro, bônus de desempenho, garantias e comprovação.

9. Ações

Depois de definida a resposta ao risco, caberá aos proprietários de riscos elencar as ações de tratamento que pretendem implementar. O tratamento é o processo de modificar um risco. Envolve a seleção de uma ou mais opções para modificar a probabilidade ou a consequência dos riscos.

Podem ser avaliados:

a) o custo-benefício de cada ação proposta;
b) o efeito de cada ação sobre a probabilidade e o impacto; e
c) os riscos cujo tratamento não é economicamente justificável.

Para cada risco identificado, deverão ser identificadas **ações** de prevenção e/ou contingência, conforme o caso, com os respectivos **responsáveis**, conforme definição a seguir:

a) **Prevenção:** É uma estratégia que envolve um trabalho preventivo de se antecipar a possíveis situações que possam impedir que o risco ocorra ou modificar a probabilidade ou o impacto; e
b) **Contingência:** Ações que devem ser executadas quando o risco ocorre. As ações de contingência são definidas de forma organizacional e devem ser alteradas sempre que necessário. Desenvolvendo um plano de contingência antecipadamente pode-se reduzir enormemente o custo de uma ação quando ocorrer o risco

A ação que se pretende realizar deverá ser descrita de forma sucinta; caberá ao proprietário de riscos definir o responsável pela execução da ação, bem como uma data-alvo para a execução.

Caso o proprietário verifique que a ação de tratamento proposta esteja além das atribuições e responsabilidades originárias de sua unidade, caberá a ele comunicar tal situação àqueles que detenham competência para atuar no tratamento do risco, consultando-os sobre a viabilidade.

10. *Status* dos Riscos

a) **Finalizado**: Quando o risco já ocorreu e não tem mais chance de ocorrer ou já foi completamente tratado;
b) **Identificado**: Imediatamente após a identificação do risco;
c) **Monitorado**: Quando o risco ainda não ocorreu, mas necessita ser monitorado. Ações de prevenção podem ser adotadas para reduzir a sua probabilidade ou o seu impacto; e
d) **Ocorrido**: Quando o risco já ocorreu, e será realizada uma ou mais ações de contingência para reduzir o impacto do risco.

11. Análise do Risco

Os riscos de execução dos resultados-chave ações serão monitorados ao longo do ciclo de vida do PDTIC. Recomenda-se às áreas demandantes e as áreas responsáveis pelos resultados-chaves que, nos monitoramentos mensais e trimestrais, os riscos sejam avaliados, para fins de ajustes que eventualmente sejam necessários, conforme fluxo abaixo:


Identificar os riscos
Avaliar a probabilidade dos riscos acontecerem e o impacto de cada um
Definir o nível de cada risco (importância de resolução)
Determinar as respostas aos riscos
Estabelecer as medidas preventivas e as contingências e indicar os responsáveis
Acompanhar as estratégias e rever os planos com frequência