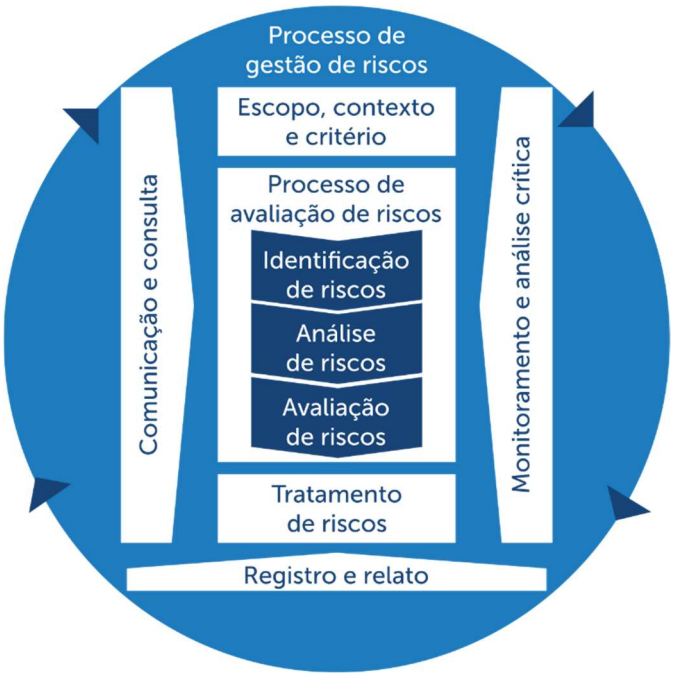
GERENCIAMENTO DE RISCOS DE EXECUÇÃO DAS AÇÕES DO PDTIC

Seguem abaixo diretrizes para o gerenciamento de riscos das ações do PDTIC 2020-2024:

1. Macroprocesso de Gestão de Riscos



2. Quantidade de Riscos

Preferencialmente, os demandantes e responsáveis pelas ações devem elencar, no máximo, **3 (três) riscos**, por ação, no cadastro da ação (formulário) ou a cada mês de monitoramento.

3. Categorias do Risco

As categorias de riscos decorrem da experiência adquirida pela DTI no monitoramento de suas ações internas e do PDTIC ao longo de 2022, 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.
6	Risco de Falta de Integridade	Risco de as características da mensagem original serem alteradas, ou seja, de os dados serem indevidamente alterados.
7	Risco de Indisponibilidade	Risco de indisponibilidade das informações ou da solução.
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.
10	Risco de Flutuação de Câmbio	Risco de as flutuações de câmbio afetarem a execução da ação.
11	Risco de Gestão	Risco de problemas relacionados às atividades de gestão da organização ou da área.
12	Risco de Gestão de Projetos	Risco de problemas relacionados à atividade de gestão de projetos.
13	Risco de Governança	Risco de problemas relacionados à governança corporativa, digital, de TIC, de contratações ou de dados.
14	Risco de Prazo	Risco de atraso.
15	Risco de Priorização	Risco de ausência de priorização, ou incorreção na priorização.
16	Risco de Proteção de Dados	Risco relacionado à proteção de dados.
17	Risco de Recursos Humanos	Risco relacionado à quantidade ou à qualidade dos recursos humanos (necessidade de alocação ou capacitação).
18	Risco de Shadow IT	Risco de soluções implementadas sem o conhecimento, acompanhamento ou homologação da área de TIC da organização.
19	Risco de SIC	Risco relacionado à segurança das informações.
20	Risco Estratégico	Risco relacionado ao alinhamento estratégico com os objetivos da organização ou de TIC (plano estratégico, tático ou outros).
21	Risco Negocial	Risco relacionado negócio da organização.
22	Risco Orçamentário/Financeiro	Risco relacionado à recursos orçamentários ou financeiros.
23	Risco Político	Risco relacionado às mudanças do cenário político.
24	Risco Reputacional ou de Imagem	Riscos relacionado à imagem organizacional ou da área de TIC.
25	Risco Técnico	Risco relacionado às questões técnicas operacionais.
26	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)

Deve-se evitar a confusão entre os eventos de risco com suas causas e consequências.

Portanto, a sintaxe adotada será:

> **"Devido à <CAUSA (fonte + vulnerabilidade)>, poderá acontecer <DESCRIÇÃO DA INCERTEZA>, o que levaria <DESCRIÇÃO DO IMPACTO, CONSEQUÊNCIA, EFEITO> impactando no/na <DIMENSÃO DO OBJETIVO IMPACTADA>".**

Pode existir mais de uma **causa** para um mesmo evento de risco. Exemplo: o evento de risco "má elaboração do termo de referência" tem como fonte "pessoas" e como vulnerabilidade "sem capacitação adequada". Causa do risco: "pessoas sem capacitação adequada".

As **consequências** 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 impacto.

Exemplo: "Devido a "pessoas" "sem capacitação adequada", poderá acontecer "má elaboração do termo de referência", o que levaria a termo de referência ou projeto básico cujo conteúdo não permite selecionar a proposta mais vantajosa para a Administração ou a contrato sem mecanismos adequados para a gestão contratual, impactando na utilização dos recursos públicos empregados, de forma inadequada.

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 organizacionais; ou ainda que causem dificuldade na utilização dos serviços ou soluções negociais ou de TIC.	2
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

Probabilidade						
	Muito Alta (5)	5	10	15	20	25
	Alta (4)	4	8	12	16	20
	Média (3)	3	6	9	12	15
	Baixa (2)	2	4	6	8	10
	Muito Baixa (1)	1	2	3	4	5
		Muito Baixo (1)	Baixo (2)	Médio (3)	Alto (4)	Muito Alto (5)
		Impacto				

1 a 3	Muto Baixo
4 a 6	Baixo
7 a 9	Médio
10 a 12	Alto
13 a 25	Muito Alto

8. Resposta ao Risco

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

- **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;

- **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;

- **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;

- **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. Aonde 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; ou

- **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.

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:

- o custo-benefício de cada ação proposta;
- o efeito de cada ação sobre a probabilidade e o impacto; e
- 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:

- **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

- **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

- **Identificado**: Imediatamente após a identificação do risco.
- **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.
- **Ocorrido**: Quando o risco já ocorreu, e será realizada uma ou mais ações de contingência para reduzir o impacto do risco.
- **Finalizado**: Quando o risco já ocorreu e não tem mais chance de ocorrer ou já foi completamente tratado.

11. Análise do Risco

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