CAPES

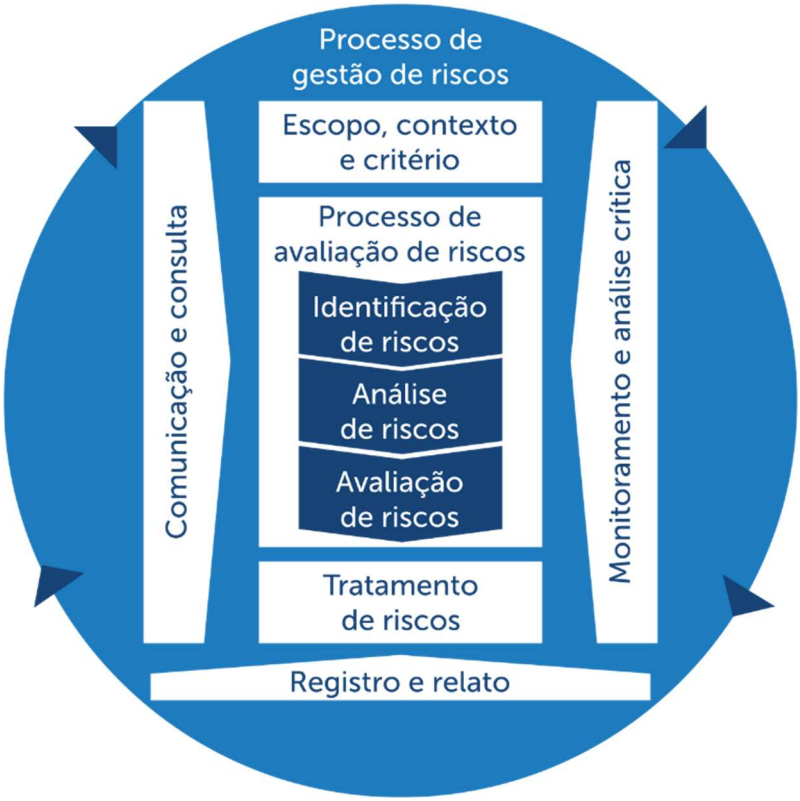
Anexo 10
Gerenciamento de Riscos das Ações do PDTIC 25-28

GERENCIAMENTO DE RISCOS DAS AÇÕES DO PDTIC 25-28

Seguem abaixo diretrizes operacionais para o gerenciamento de riscos das ações do PDTIC 2025-2028:

1. Macroprocesso de Gestão de Riscos

1.1. As etapas que envolvem operacionalização da gestão de riscos na CAPES foram estabelecidas com base nas etapas mínimas previstas no art. 5º da Portaria CAPES nº 301/2022 que versa sobre a Política de Gestão de Riscos da CAPES:



1.2. 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. Identificação e Descrição do Risco (Sintaxe)

SINTAXE:

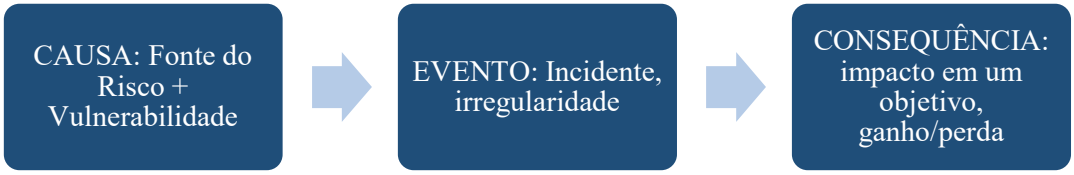
2.1. A sintaxe adotada será:

Devido a <CAUSAS>, poderá acontecer <EVENTO DE RISCO>, o que poderá levar a <CONSEQUÊNCIA> .

Exemplo 1: Devido à <falta de manutenção no sistema de informática> poderá ocorrer <uma falha no sistema de pagamento>, o que poderá levar a <atraso no pagamento das bolsas>.

Exemplo 2: Devido à <desorganização da equipe na gestão da execução contratual>, poderá acontecer <o atraso ou a não realização tempestiva dos pagamentos contratuais>, o que poderá levar ao <pagamento de encargos de mora e a um dispêndio adicional de recursos públicos pelo órgão>.

2.2. A referida sintaxe está representada graficamente abaixo:



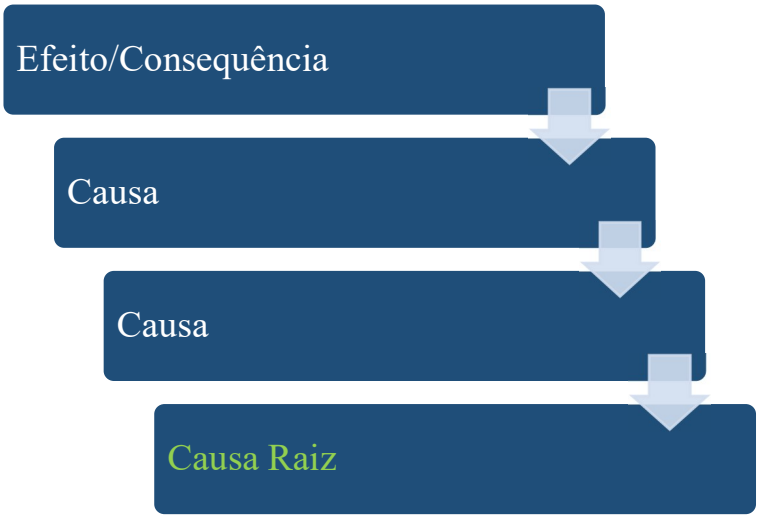
2.2.1. **CAUSAS:** São as condições que possibilitam a ocorrência de um evento. Podem ter origem tanto no ambiente interno quanto externo. É composta pela **fonte** + **vulnerabilidade**.

2.2.2. **EVENTO DE RISCO:** Possibilidade de ocorrência de um evento que possa impactar o cumprimento do objetivo do objeto.

2.2.3. **CONSEQUÊNCIA:** É o resultado decorrente de um evento de risco sobre os objetivos do objeto.

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

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



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

3. Categorias do Risco (tipologias)

3.1. As categorias de riscos decorrem da experiência adquirida pela DTI no monitoramento de suas ações internas e do PDTIC 2020 – 2024, 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 não conformidade com recomendações de controle interno e externo.
2	Risco Contratual	Risco decorrente de falhas na formalização, execução, fiscalização ou gestão de contratos, ou que impactem obrigações contratuais.
3	Risco Orçamentário/Financeiro	Risco relacionado à insuficiência, contingenciamento, atraso ou má alocação de recursos orçamentários e financeiros.
4	Risco de Câmbio	Risco de impacto negativo na execução das ações em razão de flutuações de câmbio, especialmente em contratos ou aquisições internacionais.
5	Risco de Descontinuidade	Risco de paralisação definitiva ou prolongada de soluções, sistemas ou serviços de TI, afetando a continuidade operacional.
6	Risco de Indisponibilidade	Risco de indisponibilidade total ou parcial temporária de sistemas, serviços ou informações, comprometendo a operação.
7	Risco de Informação	Risco relacionado ao acesso não autorizado, à alteração indevida, à perda de integridade, à violação da confidencialidade, à proteção de dados pessoais e à segurança da informação.
8	Risco de Capacidade de TIC	Risco decorrente da insuficiência ou indisponibilidade de recursos necessários à execução das ações de TIC, incluindo pessoas, competências, orçamento, infraestrutura ou tempo.
9	Risco de Escopo	Risco associado à definição inadequada, incompleta, desatualizada ou mal controlada do escopo das ações, projetos ou iniciativas.
10	Risco de Gestão	Risco decorrente de falhas nos processos de gestão organizacional e na gestão de projetos, incluindo planejamento, coordenação, monitoramento e tomada de decisão.
11	Risco de Prazo	Risco de atraso parcial ou integral na execução de ações, projetos, resultados ou objetivos planejados.

12	Risco Estratégico	Risco relacionado ao desalinhamento entre as ações de TIC e os objetivos estratégicos institucionais, incluindo falhas de governança corporativa, digital, de TIC, de dados ou de contratações.
13	Risco de Priorização	Risco de ausência de priorização, ou incorreção na priorização.
14	Risco Negocial	Risco decorrente da ausência, inadequação ou inconsistência na priorização de demandas, ações, projetos ou investimentos de TIC.
15	Riscos Externos	Risco decorrente de fatores externos à organização, incluindo mudanças nos cenários político, econômico, social e tecnológico.
16	Risco Reputacional ou de Imagem	Risco de danos à imagem institucional ou da área de TI perante a sociedade, órgãos de controle, parceiros ou usuários.
17	Risco Técnico	Risco relacionado a falhas técnicas operacionais, erros de configuração, manutenção inadequada ou limitações técnicas das soluções.
18	Risco Tecnológico	Risco associado à obsolescência tecnológica, adoção inadequada de tecnologias, dependência de fornecedores ou incompatibilidade tecnológica.

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

4. Probabilidade (de acontecer)

ESCALA DE PROBABILIDADE:

Probabilidade	Descrição
Muito baixa	Improvável. O evento poderá ocorrer em situações excepcionais, mas não há histórico disponível de sua ocorrência ou são raros os casos práticos onde se percebe a ocorrência deste tipo de evento. *Chance de acontecer ou frequência observada menor que 10%.*
Baixa	Pouco provável. O evento poderá ocorrer de forma inesperada ou casual, pois o histórico conhecido aponta para baixa frequência de ocorrência deste tipo de evento. *Chance de acontecer ou frequência observada entre 10% e 30%.*
Média	Possível. O evento pode ocorrer em algum momento, pois o histórico de ocorrência conhecido indica moderadamente essa possibilidade. *Chance de acontecer ou frequência observada entre 30% e 60%.*
Alta	Provável. O evento é esperado, provavelmente ocorrerá na maioria das circunstâncias, pois o histórico conhecido indica fortemente essa possibilidade. *Chance de acontecer ou frequência observada entre 60% e 80%.*
Muito alta	Praticamente certa. O evento é frequente, ocorre repetidamente, e seu histórico indica claramente essa possibilidade. *Chance de acontecer ou frequência observada entre 80% e 100%.*

5. Impacto (dano)

ESCALA DE IMPACTO:

Impacto	Descrição
Muito baixo	Impacto mínimo. Não altera o alcance dos objetivos do projeto ou a alteração é insignificante.
Baixo	Impacto pequeno. Compromete muito pouco o alcance dos objetivos do projeto e é de fácil reparação ou recuperação.
Médio	Impacto moderado. Compromete razoavelmente o alcance dos objetivos, porém é possível a reparação ou recuperação.
Alto	Impacto significativo. Compromete a maior parte do atingimento dos objetivos do projeto, sendo de difícil reparação ou recuperação.
Muito alto	Impacto catastrófico. Compromete totalmente ou quase totalmente, de forma irreversível, os objetivos do projeto, sem possibilidade de reparação.

6. Nível de Risco

6.1. Considerando o item 3.1.5.3 da Metodologia de Gestão de Riscos da CAPES, que diz: *"Nos riscos gerenciados pela Diretoria de Tecnologia da Informação (DTI), deve-se considerar o impacto como a dimensão mais relevante da Matriz"*, optou-se por utilizar a matriz de Impacto x Probabilidade baseada no Manual de Gestão de Riscos do Tribunal de Contas da União (TCU), pelos motivos a seguir expostos:

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.

6.2. 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).

Matriz de Probabilidade e Impacto

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: Baseada no Manual de Riscos do TCU
e na Metodologia de Gestão de Riscos da CAPES

CLASSIFICAÇÃO DO NÍVEL DE RISCO:

a) Risco Baixo: 1 a 5;
b) Risco Moderado: 6 a 11;
c) Risco Alto: 12 a 19; e
d) Risco Extremo: 20 a 25.

LIMITES DE EXPOSIÇÃO AO RISCO:

Classificação do nível de risco	Ações
Risco baixo	Dentro do apetite a risco. Não é necessário implementar novo controle. Podem existir oportunidades de diminuir os controles.
Risco moderado	Dentro do apetite a risco. É necessário monitorar a efetividade dos controles existentes. Podem ser implementados outros controles que tenham custo-benefício adequado.

Risco alto	Acima do apetite a risco. É necessário adotar alguma medida de controle em um período determinado.
Risco extremo	Muito acima do apetite a risco. É necessário adotar uma medida de controle imediata.

6.3. 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.

7. Papéis

7.1. A Metodologia de Gestão de Riscos da CAPES adota o modelo das Três Linhas de Defesa, estabelecendo de forma clara os papéis e responsabilidades no âmbito institucional, a saber:

a) 1ª Linha: composta pelos gestores de riscos das unidades organizacionais, responsáveis pela gestão direta dos riscos associados aos processos, projetos e ações sob sua responsabilidade;
b) 2ª Linha: atua no nível tático da gestão e é composta pela Coordenação-Geral de Governança e Planejamento (CGGOV) e pela Unidade de Gestão da Integridade, responsáveis pelo apoio metodológico, supervisão e monitoramento da gestão de riscos;
c) 3ª Linha: exercida pela Auditoria Interna, responsável pela prestação de serviços independentes e objetivos de avaliação e consultoria, com fundamento nos princípios de autonomia técnica e objetividade.

7.2. Nos termos do art. 7º da Portaria CAPES nº 301, de 2022, a Presidência da Fundação é a instância máxima responsável pelo estabelecimento da estratégia institucional e pela definição da estrutura de gerenciamento de riscos, incluindo a manutenção, o monitoramento e o aprimoramento dos controles internos de gestão.

7.3. O nível operacional, representado pelos gestores de riscos nas diretorias, poderá acionar o nível tático, representado pela CGGOV, tanto para solicitar orientações quanto para reportar novos riscos identificados no âmbito de seus processos ou projetos. Compete, ainda, ao nível operacional responder às demandas do nível tático, relativas ao monitoramento das ações previstas nos planos de ação e às atividades de gestão de riscos de forma geral.

7.4. No exercício de suas atribuições, a CGGOV, no nível tático, poderá acionar o nível operacional durante o monitoramento das ações de gestão de riscos, sendo também

responsável por consolidar e reportar ao Comitê Gerencial de Governança (CGG) o progresso das ações definidas no modelo institucional de gestão de riscos.

7.5. As diretorias da CAPES são responsáveis por designar formalmente os gestores de riscos dos processos e projetos organizacionais sob sua responsabilidade, conforme disposto no art. 9º da Portaria CAPES nº 301, de 2022, assegurando a efetiva implementação da política de gestão de riscos em suas respectivas áreas.

7.6. Todos os servidores e colaboradores da CAPES tem por competência:

a) o monitoramento da evolução dos níveis de riscos corporativos e da efetividade das medidas de controles internos implementadas nos processos e projetos organizacionais em que estiverem envolvidos ou que tiverem conhecimento; e
b) Caso sejam identificadas mudanças ou fragilidades nos processos ou projetos organizacionais, o colaborador deverá reportar imediatamente o fato ao gestor de riscos do processo ou projeto em questão.

7.7. A Metodologia de Gestão de Riscos da CAPES estabelece papéis e responsabilidades específicos para a gestão de riscos nos níveis estratégico, tático e operacional. No que se refere, em especial, aos riscos associados às ações do Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC), observam-se, em princípio, as seguintes atribuições:

a) Nível operacional – Diretorias: Compete às Diretorias designar formalmente os gestores de riscos dos processos e projetos sob sua responsabilidade, bem como assegurar a efetiva implementação da Política de Gestão de Riscos em suas respectivas áreas de atuação. Salvo designação em contrário, o gestor de riscos das iniciativas (projetos) de TI corresponderá ao titular da área responsável por sua execução no âmbito do PDTIC;

b) Nível operacional – Gestores de Riscos (Processos e Projetos de TI): Cabe aos gestores de riscos implementar a Política de Gestão de Riscos e Controles Internos; identificar, analisar e avaliar os riscos de TI; propor respostas aos riscos e as correspondentes medidas de controle; implementar e monitorar os controles internos; acompanhar a evolução dos níveis de risco; e reportar à Coordenação-Geral de Governança e Planejamento (CGGOV), bem como às instâncias superiores competentes, eventuais mudanças significativas e os resultados do monitoramento. Recomenda-se que a análise e a avaliação de cada risco identificado sejam atualizadas, no mínimo, a cada ciclo mensal de monitoramento das iniciativas de TI; e

c) Atuação transversal – Servidores e Colaboradores: Todos os servidores e colaboradores devem acompanhar os riscos e controles relacionados aos processos e projetos em que atuem ou dos quais tenham conhecimento, reportando imediatamente ao gestor de riscos responsável quaisquer fragilidades, falhas ou alterações relevantes identificadas. Considerando a quantidade de iniciativas estabelecidas no PDTIC, recomenda-se, ainda, que os gestores de riscos possam solicitar o apoio de gerentes ou executores dos projetos (iniciativas) para o monitoramento e a análise operacional dos riscos, sem prejuízo de sua responsabilidade formal.

8. Resposta ao Risco

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

a) **Aceitar**: Aceitar o risco significa que não são necessárias medidas adicionais para alterar os níveis de risco, pois estes já estão dentro do apetite a riscos. No entanto, devem ser monitorados;

b) **Compartilhar**: Compartilhar o risco pode ser realizado por meio de terceirização ou contratação de seguros, visando reduzir tanto o impacto quanto a probabilidade do risco. Essa abordagem normalmente ocorre quando o risco é classificado fora do apetite ao risco, buscando trazê-lo para dentro desse limite;

c) **Evitar:** Evitar o risco significa não iniciar ou descontinuar a atividade que gera o risco, especialmente quando o custo-benefício da implementação dos controles é elevado e não é possível compartilhar o risco; e

d) **Mitigar**: Mitigar o risco significa implementar controles com o objetivo de reduzir a probabilidade ou o impacto dos riscos, atuando nas suas causas ou consequências. Esse processo normalmente ocorre quando o risco está classificado fora do apetite ao risco, buscando trazê-lo para dentro desse limite. É importante avaliar se o custo-benefício da implementação do controle é adequado.

9. Ações

9.1. Após a definição da resposta ao risco, caberá aos Gestores de Riscos, ou aqueles por eles autorizados, definir e elencar as ações de tratamento a serem implementadas. O tratamento do risco consiste no processo de sua modificação, envolvendo a seleção de uma ou mais opções destinadas a alterar a probabilidade de ocorrência e/ou as consequências dos riscos identificados.

9.2. No processo de definição das ações de tratamento, poderão ser considerados, entre outros aspectos:

a) a relação custo-benefício de cada ação proposta;
b) o efeito esperado de cada ação sobre a probabilidade de ocorrência e o impacto do risco; e
c) a identificação de riscos cujo tratamento não seja economicamente justificável.

9.3. Para cada risco identificado, deverão ser definidas ações de prevenção e/ou contingência, conforme aplicável, com a indicação dos respectivos responsáveis, observadas as seguintes definições:

a) **Ações Preventivas:** Compõe a estratégia voltada à atuação antecipada, com o objetivo de evitar a ocorrência do risco ou de reduzir sua probabilidade e/ou impacto. São controles preventivos que atuam nas causas do risco, com o objetivo de diminuir a probabilidade de ocorrência, ou seja, prevenir. Nessa categoria também podem ser cadastradas as ações que atuam na detecção da materialização de um risco (controles detectivos); e

b) **Ações de Contingência:** São o conjunto de ações a serem executadas caso o risco se materialize. São controles corretivos que objetivam diminuir o impacto. As ações de contingência devem ser definidas de forma organizada, revisadas sempre que necessário e formalizadas em um plano específico, de modo a reduzir custos, impactos e tempo de resposta quando da ocorrência do risco.

9.4. Monitoramento

9.4.1. A ação que se pretende realizar deverá ser descrita de forma sucinta. Caberá aos Gestores de Riscos, ou aqueles por eles autorizados, definir o responsável pela execução da ação, bem como uma data-alvo para a execução.

9.4.2. Caso o Gestor do Risco, 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) **Identificado**: Imediatamente após a identificação do risco;

b) **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;
c) **Ocorrido**: Quando o risco já ocorreu, e será realizada uma ou mais ações de contingência para reduzir o impacto do risco; e
d) **Finalizado**: Quando o risco já ocorreu e não tem mais chance de ocorrer ou já foi completamente tratado.

11. Análise do Risco

11.1. Os riscos das iniciativas de TI serão monitorados ao longo do ciclo de vida do PDTIC. Recomenda-se às áreas demandantes e às áreas responsáveis pelos resultados-chaves que, nos monitoramentos mensais e bimestrais, os riscos sejam avaliados, para fins de ajustes que eventualmente sejam necessários, conforme fluxo abaixo: