



Plano de Gestão de Riscos de TIC 2025-2026

Abril/2025

1. Introdução

A sistematização da gestão de riscos em nível institucional constitui estratégia que aumenta a capacidade da organização para lidar com incertezas, estimula a transparência, contribui para o uso eficiente de recursos públicos e melhora a entrega de serviços ao cidadão (TCU, 2018). As organizações não podem ser avessas ao risco e ter sucesso, pois o risco é inerente a tudo o que fazemos para oferecer serviços de alta qualidade.

Este documento visa orientar as atividades a serem conduzidas de forma coletiva em reuniões de planejamento da área de Tecnologia da Informação (TI), de forma a prever eventos ou situações que possam comprometer a execução dos objetivos estratégicos definidos no Plano Diretor de TI (2025-2026). Com isso, espera-se aumentar a probabilidade e o impacto dos eventos positivos, reduzir a probabilidade e o impacto dos eventos negativos, e orientar a equipe de TI sobre como os riscos devem ser gerenciados.

Sendo assim, o Plano de Gestão de Riscos de Tecnologia da Informação do TRE-PR contribui para a identificação de possíveis ameaças que poderão afetar o dia a dia organizacional, possibilitando agir proativamente, o que reduzirá os impactos negativos na missão e nos objetivos estratégicos de TI.

1.1. Objetivo

O Plano de Gestão de Riscos em Tecnologia da Informação tem o objetivo de ser parte integrante da tomada de decisão informada desde o início da política ou do projeto, passando pela implementação até a entrega diária de serviços de Tecnologia da Informação. Este documento fornece uma abordagem para a gestão de riscos relacionados à Tecnologia da Informação por meio de um conjunto de atividades e tarefas que permitem identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos.

Este documento estabelece um plano de ação contendo o processo de gestão de riscos para a área de TI de forma a orientar a identificação, a análise, a avaliação, o tratamento, a priorização, o monitoramento e a comunicação dos riscos inerentes aos recursos, serviços e sistemas informatizados do TRE-PR.

Para que o objetivo geral seja alcançado, foram definidos os seguintes objetivos específicos:

- a) Definir as atividades e tarefas que compõem o processo de gestão de riscos;
- b) Definir as técnicas e ferramentas para identificação, análise, avaliação, tratamento, monitoramento e comunicação de riscos para a área de TI do TRE-PR;
- c) Definir os papéis e responsabilidades de cada envolvido na gestão de riscos.

1.2. Escopo e Abrangência

O Plano de Gestão de Riscos em Tecnologia da Informação proposto neste documento permeia todo o ciclo de vida das iniciativas para desenvolvimento, implementação e gestão de soluções que envolvem as áreas de Tecnologia da Informação do TRE-PR. Abrange as áreas de infraestrutura de TI, manutenção de equipamentos de TI, suporte operacional, desenvolvimento de sistemas, governança e gestão de TI, redes e segurança da informação.

1.3. Referências

As referências para a construção do Plano de Gestão de Riscos em Tecnologia da Informação são:

1. [Manual de Gestão de Riscos do TRE-PR](#).
2. Política de Gestão de Riscos do TRE-PR ([Portaria TRE-PR/PRESID nº 423/2021](#)).
3. Norma Técnica ABNT NBR ISO 31000: 2018 Risk management: guidelines, provides principles, framework and a process for managing risk.
4. Norma Técnica ABNT 31010:2019. Risk Management: Risk assessment techniques.

1.4. Vigência

O atual Plano de Gestão de Riscos de Tecnologia da Informação terá validade de 2 (dois) anos e está alinhado ao PDTIC da Secretaria de Tecnologia da Informação.

2. Metodologia

A metodologia para construção deste Plano baseia-se nas ferramentas de gestão conhecidas por *Ciclo de Deming*, para melhoria contínua de processos e produtos (PDCA), e a ferramenta para construção de plano de ação *5W2H*.

O quadro a seguir apresenta as fases da metodologia utilizada para a construção deste documento.

Fase	Atividades
Planejamento	Planejar o processo de gestão de riscos com suas atividades, tarefas, ferramentas e técnicas.
Desenvolvimento	Definir papéis e responsabilidades bem como as atividades e tarefas a serem executadas por cada papel.
Checagem	Definir como será o monitoramento e o controle do plano de ação a ser seguido.
Ação	Comunicar o cronograma para a execução do plano.

3. Processo de Gerenciamento de Riscos

De acordo com os princípios e diretrizes dispostos na Política de Gestão de Riscos do TRE-PR, a gestão de riscos deve ser parte integrante dos processos organizacionais, de forma sistemática, estruturada e oportuna, visando, sobretudo, subsidiar a tomada de decisão e a elaboração do planejamento estratégico, assim como promover a melhoria contínua dos processos organizacionais. A gestão de riscos deve ser utilizada ainda como instrumento para promover a simplificação de procedimentos associados à prestação de serviços públicos, de modo a assegurar que somente sejam utilizados os controles

indispensáveis, de acordo com os limites de exposição a riscos institucionalmente definidos, e que sejam eliminados controles desnecessários ou economicamente desvantajosos. A partir das orientações e determinações constantes na normativa, a operacionalização da gestão de riscos deve seguir as etapas da figura abaixo. Observe-se que essas etapas não são obrigatoriamente sequenciais.

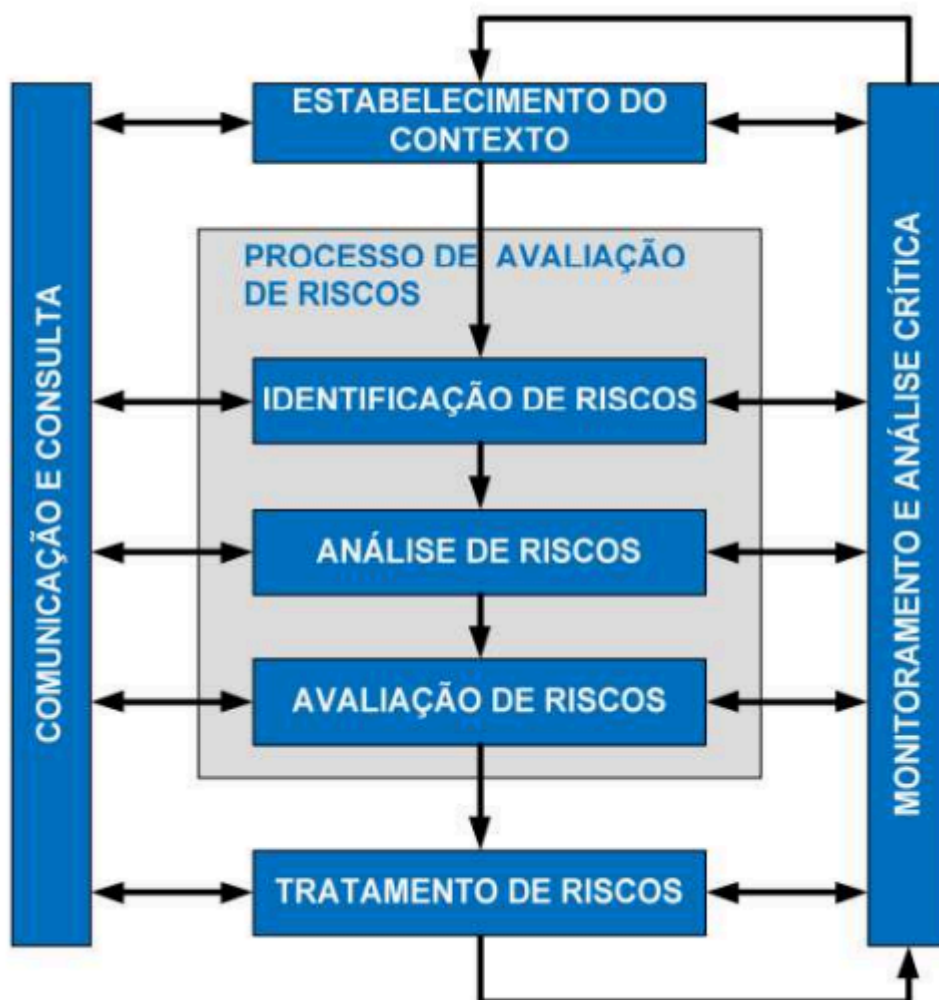


Figura 1 – Processo de Gestão de riscos de TI

A Figura 1 apresenta as atividades executadas para a realização da gestão de riscos relacionados aos projetos de TI. São elas: estabelecimento do contexto, processo de avaliação de riscos (identificação de riscos, análise de riscos e avaliação de riscos), tratamento de riscos, monitoramento e análise crítica, e comunicação e consulta com as partes interessadas. Todos os passos para o gerenciamento de Riscos da SECTI estão dispostos no Manual do Processo de Gestão de Riscos de TI.

4. Papéis e Responsabilidades

4.1) Quem são os Gestores de Riscos de TI

Os Gestores de Riscos são:

- Secretários
- Coordenadores
- Assessores
- Chefes de Seção;
- Responsáveis pelos Núcleos, Comissões e Grupos de Trabalho
- Gerentes de projeto
- Gestores de contratações

4.2) Responsabilidades dos Gestores de Riscos

- I. Priorizar os processos de trabalho que devam ter os riscos gerenciados, à vista da dimensão do impacto que possam causar à missão institucional;
- II. Identificar, analisar, avaliar, tratar e monitorar os riscos, em alinhamento aos objetivos estratégicos do Tribunal;
- III. Elaborar os Planos e as Ações de Tratamento a serem implementados, bem como definir o responsável, o prazo de execução e de avaliação dos resultados obtidos;
- IV. Implementar controles internos em sua área de atuação, decorrentes da gestão de riscos;
- V. Estruturar a gestão de riscos sob sua responsabilidade, assegurando o tratamento por meio de ações de caráter imediato, de curto, médio ou longo prazo, ou de aperfeiçoamento contínuo;
- VI. Realizar o monitoramento e a análise crítica do processo de gestão de riscos;
- VII. Reportar as conclusões e eventos relevantes às instâncias competentes e ao Comitê de Gestão Estratégica e Riscos, conforme o caso.

Papel (Responsável)	Responsabilidade
Comitê de Gestão da TI (CGTI)	Monitoramento de riscos estratégicos de TI.
Comitê de Gestão de Segurança da Informação de Proteção de Dados Pessoais (CGSIPDP)	Monitoramento de riscos de segurança da informação e proteção de dados pessoais.
Comitê de Gestão Estratégica e Riscos (CGER)	Monitoramento de riscos estratégicos.
Comitê Executivo de TI (CETI)	Monitoramento de riscos operacionais e de processos de gestão de TI.
Equipes de projeto	Monitoramento de riscos de projeto.

Papel (Responsável)	Responsabilidade
Equipes de contratação, Assistência às Contratações de TI (ACTI) e Secretaria de Administração (SECAD)	Monitoramento de riscos nas contratações de TI.
Secretário de Tecnologia da Informação	<ul style="list-style-type: none"> • Associar um agente responsável por cada risco identificado e avaliado nos projetos ou planos de contingência e resposta a riscos. • Assegurar que o risco seja gerenciado de acordo com as diretrizes estabelecidas neste documento. • Garantir que as informações adequadas sobre o risco estejam disponíveis e atualizadas. • Gerenciar e reportar informações adequadas sobre o gerenciamento de riscos.
Gestor de Riscos	<ul style="list-style-type: none"> • Identificar e avaliar os riscos no âmbito das atividades desenvolvidas pela área de Tecnologia da Informação. • Elaborar e manter atualizado o Mapa de Gerenciamento de Riscos de TI e o plano de ação para tratamento de riscos. • Monitorar o risco ao longo do tempo, de modo a garantir que as respostas adotadas resultem na manutenção do risco em níveis adequados, de acordo com a política de gestão de riscos. • Atuar na primeira linha de defesa, com a implementação de ações corretivas para resolver deficiências nos mapas e nos planos de ação de riscos. • Manter controles eficazes e conduzir procedimentos de resposta aos riscos. • Acompanhar as inovações e adotar boas práticas na gestão de riscos de TI.

5. Monitoramento e Controle

Este documento será revisado anualmente ou quando necessário. Todas as situações ou atividades não previstas neste documento deverão ser submetidas à Secretaria de TI que juntamente com sua equipe irão avaliá-las e aprová-las.

O Plano de Gestão de Riscos deve ser revisado ainda ao final de cada novo ciclo de planejamento estratégico e, a qualquer tempo, se houver alteração significativa no padrão de riscos do Tribunal, devendo o Plano refletir essa mudança.

Imediatamente após sua aprovação, o Plano de Gestão de Riscos de Tecnologia da Informação e os Mapas de Gerenciamento de Riscos serão atualizados com o devido registro das alterações e encaminhados para o Comitê Gestor de TI.

6. Cronograma de Ações

A aplicação deste plano deve abranger, direta ou indiretamente, todas as áreas da SECTI até o final de 2026. Para este período serão mapeados os riscos associados aos serviços essenciais de TI, processos estratégicos de TI e riscos de Segurança da Informação.

Ação	Justificativa	Responsável	Prazo	Status
Mapeamento de riscos relativos aos sistemas de eleição, durante o período eleitoral	Serviço essencial de TI	Comitê Executivo de TI (CETI)	maio/2025	Não iniciado
Mapeamento de riscos relativos aos sistemas de atendimento ao eleitor/cadastro	Serviço essencial de TI	Coordenadoria de Sistemas (COSIS)	agosto/2025	Não iniciado
Mapeamento de riscos relativos ao Processo Judicial Eletrônico (PJE)	Serviço essencial de TI	Coordenadoria de Sistemas (COSIS)	agosto/2025	Não iniciado
Mapeamento de riscos relativos ao Diário de Justiça Eletrônico (DJE)	Serviço essencial de TI	Coordenadoria de Sistemas (COSIS)	agosto/2025	Não iniciado
Mapeamento de riscos relativos aos sistemas de processos administrativo digital (PAD e SEI)	Serviço essencial de TI	Coordenadoria de Sistemas (COSIS)	agosto/2025	Não iniciado
Mapeamento de riscos relativos aos serviços de e-mail e colaboração em nuvem	Serviço essencial de TI	Coordenadoria de Serviços e Ambiente (COSA)	maio/2025	Não iniciado
Mapeamento de riscos relativos ao Sistema de Acompanhamento de Documentos e Processos (SADP)	Serviço essencial de TI	Coordenadoria de Sistemas (COSIS)	dezembro/2025	Não iniciado
Mapeamento de riscos relativos a Urnas	Processo escolhido para monitoramento em 2025 junto ao CGER	Coordenadoria de Serviços e Ambiente (COSA)	abril/2025	Em andamento

Ação	Justificativa	Responsável	Prazo	Status
Mapeamento de riscos de Segurança da Informação	Processo estratégico	Coordenadoria de Segurança, Inteligência Artificial e Governança (COSIG)	dezembro/2025	Em andamento