

# **PLANO DE GESTÃO DE RISCOS**

de Tecnologia da Informação

**2021 - 2026**

Data: 20/08/2024  
Versão 3.1

Presidente do Tribunal de Justiça do Estado do Paraná (gestão 2023-2024)

**Desembargador Luiz Fernando Tomasi Keppen**

1° Vice-Presidente

**Desembargadora Joeci Machado Camargo**

2° Vice-Presidente

**Desembargador Fernando Antônio Prazeres**

Corregedor-Geral da Justiça

**Desembargador Hamilton Mussi Corrêa**

Corregedor de Justiça

**Desembargador Roberto Antonio Massaro**

Supervisor de Tecnologia da Informação e Comunicação

**Desembargador Rui Portugal Bacellar Filho**

### **Comitê de Governança de Tecnologia da Informação e Comunicação do TJPR**

---

Presidente do Comitê

**Desembargador Marcel Rotoli de Macedo**

Vice-Presidente do Comitê

**Desembargador Luciano Carrasco**

**Falavinha Souza**

Juiz Auxiliar da Presidência

**Dr. César Ghizoni**

Juiz Auxiliar da Presidência

**Dr. Márcio José Tokars**

Juiz Auxiliar da 2ª Vice-Presidência

**Dr. Lucas Cavalcanti da Silva**

Juiz Auxiliar da Corregedoria-Geral da Justiça

**Dr. Gustavo Hoffmann**

Representante da AMAPAR

**Dr. Marcos Caires Luz**

Secretário do Tribunal de Justiça

**José Luiz Faria de Macedo Filho**

Diretor da Secretaria de Planejamento

**Vinícius Rodrigues Lopes**

Diretor da Secretaria de Tecnologia da  
Informação

**Rafael Coninck Teigão**

Servidor da Secretaria de Tecnologia da  
Informação

**Alessio Roman Junior**

Servidora da Secretaria de Tecnologia da  
Informação

**Andreia Karla Dorce**

Servidor da Corregedoria-Geral da Justiça

**Gerson Mikalixen Junior**

### Comitê de Gestão de Riscos do TJPR

---

Presidente do Comitê  
**Dr<sup>a</sup>. Fernanda Karam de Chueiri Sanches**  
Secretário do Tribunal de Justiça  
**José Luiz Faria de Macedo Filho**

Diretor da Secretaria de Planejamento  
**Vinicius Rodrigues Lopes**  
Coordenador do Núcleo de Governança,  
Riscos e Compliance  
**Thiago Martini Ribeiro Pinto**

*Resolução nº 272/2020-OE/TJPR*

### Comitê de Segurança de Tecnologia da Informação e Comunicação do TJPR

---

Presidente do Comitê  
**Desembargador Rui Portugal Bacellar Filho**  
Encarregado de Dados  
**Desembargador Claudio Smirne Diniz**

Juiz Auxiliar da Presidência  
**Dr. César Ghizoni**  
Juiz Auxiliar da Corregedoria-Geral da Justiça  
**Dr. Gustavo Hoffmann**  
Secretário do Tribunal de Justiça  
**José Luiz Faria de Macedo Filho**  
Diretor da Secretaria de Tecnologia da  
Informação  
**Rafael Coninck Teigão**

*Portaria TJPR nº1841 e 1948/2021 (SEI/TJPR 0017196-72.2021.8.16.6000)*

**Comitê de Gestão de Tecnologia da Informação e Comunicação do TJPR**

---

Alberto Heitor Molinari

Alessio Roman Junior

Andreia Karla Dorce

Carlos José Johann Kolb

Cideclei Machado

Danilo Kovalechyn

Fábio Da Luz Caiut

Gustavo Raphael Stein

Jefferson Wanderley Jacob

Johnatan Daniel Fromholz Lima

Lauro Andrey De Souza Bueno

Luiz Fernando Moletta Alves

Luís Fernando Parizotto Mormul

Magno Mario Bayer Filho

Márcio Mortensen Wanderley

Marco Antônio Gomes Bernardino

Pablo Tavares

Paulo Henrique Waromby

Rafael Coninck Teigão

Zilei Carolina Da Silveira De Lara

*Portaria TJPR nº4217/2021 eDJ nº 2977 em 21/05/2021 (SEI/TJPR 0033045-60.2016.8.16.6000)*

**Equipe de elaboração (servidores da Assessoria de Governança de TIC)**

---

Andreia Karla Dorce

Danielle Trein Romanelli

Renan Rafael Marcon

Sibele Heil dos Santos

**HISTÓRICO DE ALTERAÇÕES**

| <b>Versão</b> | <b>Data</b> | <b>Autor(es)</b>   | <b>Descrição</b>   |
|---------------|-------------|--|--|
| 0.1           | 27/04/2022  | Equipe de Apoio a Gestão e Governança de TIC                       | Criação do Documento.  |
| 0.2           | 05/05/2022  | Equipe de Apoio a Gestão e Governança de TIC e Integrantes do NGRC | Sugestões de alguns integrantes do NGRC (Roberta Teigão e Fábio de Araújo) para melhoria no documento.   |
| 0.3           | 06/05/2022  | Equipe de Apoio a Gestão e Governança de TIC                       | Apresentado ao CGESTIC – Comitê de Gestor de TIC e encaminhado via SEI!TJPR 0055468-04.2022.8.16.6000.   |
| 1.0           | 13/05/2022  | Equipe de Apoio a Gestão e Governança de TIC                       | Correções com os apontamentos do NGRC solicitados via SEI!TJPR doc. 7661533.   |
| 1.1           | 12/06/2023  | Equipe da Assessoria de Governança de TIC                          | Atualização dos integrantes dos Comitês e equipe de revisão Atualização das áreas de TIC (Cap. 3) Atualização das listas de siglas, conceitos e definições (Cap. 4) Atualização das responsabilidades dos comitês (Cap. 6) Inclusão do cronograma de mapeamento de risco (Cap. 9) Atualização das tabelas de risco, de acordo com o NGRC (Cap. 11) |
| 1.2           | 14/06/2023  | Equipe da Assessoria de Governança de TIC                          | Alteração da cadeia de valor no qual foi classificado o objeto: "Mapeamento de dados sensíveis em banco de dados" para o macroprocesso → Governança → Gerir Riscos e Conformidade → Prover Segurança de Informações. (Cap. 9)  |
| 2.0           | 19/02/2024  | Equipe da Assessoria de Governança de TIC                          | Alteração da apresentação do Plano e inclusão de novo cronograma de riscos a serem mapeados em 2024.   |
| 2.1           | 19/03/2024  | CGESTIC  | Aprovação CGESTIC.   |
| 3.0           | 12/08/2024  | Equipe de Governança de TIC  | Alteração dos objetos de riscos a serem mapeados. Alteração do cronograma de mapeamento de riscos com vigência para 2024-2026.   |
| 3.1           | 20/08/2024  | CGESTIC  | Aprovação no CGESTIC.  |

## SUMÁRIO

|       |  |    |
|-------|--|----|
| 1.    | INTRODUÇÃO .....   | 7  |
| 2.    | SOBRE ESTE PLANO .....   | 8  |
| 2.1   | CONTEXTUALIZAÇÃO E JUSTIFICATIVA.....                                    | 8  |
| 2.2   | ESCOPO E ABRANGÊNCIA .....   | 8  |
| 2.3   | OBJETIVO .....   | 10 |
| 2.4   | RESPONSABILIDADES E PAPÉIS.....  | 10 |
| 2.5   | METODOLOGIA DO PROCESSO DE GESTÃO DE RISCOS NA SETI .....                | 12 |
| 2.5.1 | ESTABELECIMENTO DO CONTEXTO .....  | 13 |
| 2.5.2 | IDENTIFICAÇÃO DOS RISCOS.....  | 14 |
| 2.5.3 | ANÁLISE E AVALIAÇÃO DOS RISCOS .....                                     | 14 |
| 2.5.4 | TRATAMENTO DOS RISCOS.....   | 16 |
| 2.5.5 | COMUNICAÇÃO DOS RISCOS .....   | 17 |
| 2.5.6 | MONITORAMENTO CONTÍNUO DOS RISCOS.....                                   | 17 |
| 3.    | MATRIZ DE RESPONSABILIDADES DO PROCESSO DE GESTÃO DE RISCOS NA SETI..... | 17 |
| 4.    | FLUXO DO PROCESSO DE CRIAÇÃO/REVISÃO DO PLANO .....                      | 19 |
| 5.    | IMPORTÂNCIA DA CONSCIENTIZAÇÃO DA GESTÃO DE RISCOS .....                 | 19 |
| 6.    | APRENDIZADO E MELHORIA CONTÍNUA .....                                    | 19 |
| 7.    | REVISÃO E ATUALIZAÇÃO DO PLANO .....                                     | 20 |
| 8.    | CRONOGRAMA DE MAPEAMENTO DE RISCOS .....                                 | 20 |
| 9.    | ÍNDICE DE EXECUÇÃO DO PLANO .....  | 22 |
| 10.   | ABREVIATURAS E SIGLAS DE TI.....   | 22 |
| 11.   | CONSIDERAÇÕES FINAIS.....  | 23 |

## 1. INTRODUÇÃO

A Tecnologia da Informação e Comunicação (TIC) é fundamental para o alcance dos objetivos estratégicos do Tribunal de Justiça do Estado do Paraná (TJPR), dessa forma, os riscos associados à área de TIC devem ser gerenciados de forma eficiente e eficaz. Este documento define o Plano de Gestão de Riscos de TIC (PGRTIC) que deverá ser aplicado na Secretaria de Tecnologia da Informação (SETI).

A Resolução nº 370/2021 do CNJ, que estabelece a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD), para o período 2021 a 2026, dispõe no Art. 37:

*“Cada órgão deverá elaborar Plano de Gestão de Riscos de TIC, com foco na continuidade de negócios, manutenção dos serviços e alinhado ao plano institucional de gestão de riscos, objetivando mitigar as ameaças mapeadas para atuar de forma preditiva e preventiva às possíveis incertezas.”*

Nesse contexto, o presente plano contempla um conjunto de **diretrizes** que permitem identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos associados à Tecnologia da Informação e Comunicação, contribuindo para o fortalecimento da Governança de TIC, a tomada de decisões e o alcance dos objetivos institucionais.

## 2. SOBRE ESTE PLANO

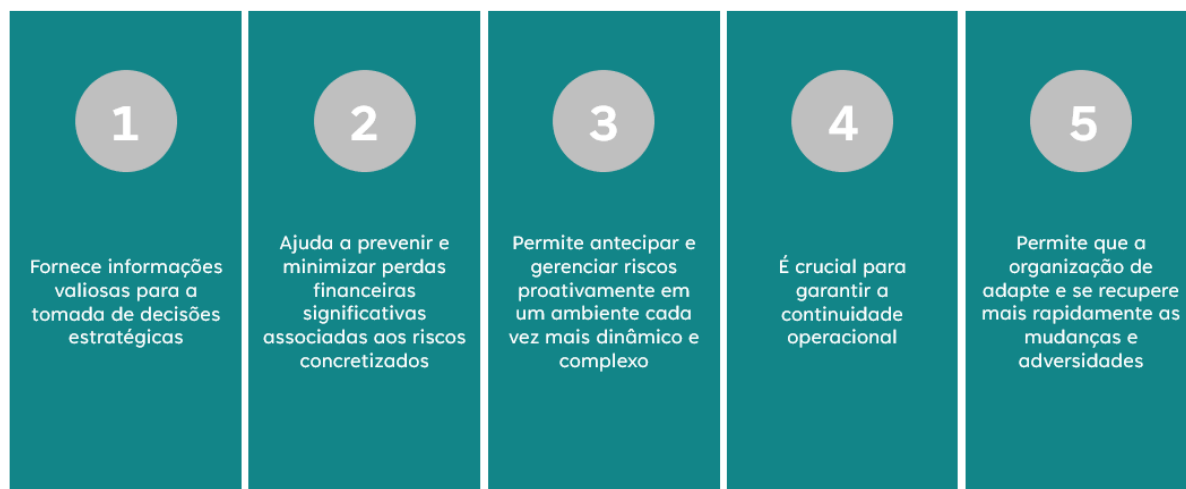
### 2.1 CONTEXTUALIZAÇÃO E JUSTIFICATIVA

A gestão de riscos de TIC é crucial para garantir a segurança, a continuidade e o sucesso das organizações em um ambiente cada vez mais dependente da tecnologia.

Fazer um plano de gestão de riscos é fundamental para garantir a resiliência, o sucesso contínuo e a sustentabilidade da Secretaria de Tecnologia da Informação (SETI), proporcionando uma abordagem estruturada para lidar com a complexidade e à falta de conhecimento ou previsibilidade sobre eventos futuros.

Reconhecer e gerenciar a incerteza é uma habilidade crítica para os gestores em um mundo em constante mudança. Estratégias eficazes de gestão de riscos, aprendizado contínuo e flexibilidade são fundamentais para navegar com sucesso em ambientes incertos.

A importância dessa gestão de riscos pode ser destacada por vários motivos:



### 2.2 ESCOPO E ABRANGÊNCIA



Este documento tem aplicabilidade para toda a SETI e abrange as áreas de: Governança, Planejamento, Gestão e Infraestrutura de TIC, Segurança da Informação e Atendimento aos Usuários.

O escopo da gestão de riscos de TIC é o de analisar os possíveis riscos relacionados aos processos, projetos, estratégia e aos ativos de TIC que podem afetar os objetivos estratégicos do TJPR.

Inicialmente, o presente plano considera os riscos de TIC que envolvem os seguintes pilares:

- ✓ **Riscos Estratégicos:** riscos identificados e analisados no escopo da elaboração dos artefatos, nos sistemas e serviços estratégicos. Após o levantamento, será atribuído a uma área proprietária, ainda que outras áreas possam estar envolvidas na mitigação e controle. Os gestores destas áreas serão os proprietários destes riscos.
- ✓ **Riscos de Segurança:** riscos identificados e analisados no escopo de segurança da informação e comunicação ou normas relacionadas, considerando-se principalmente os sistemas e serviços críticos de TIC e aqueles identificados no Plano de Continuidade de Serviços de TIC. Os responsáveis pelos sistemas, serviços e pelos ativos que os suportam são identificados juntamente com a avaliação de cada controle, cabendo a estes o monitoramento do risco residual após o tratamento.
- ✓ **Riscos em Contratações:** riscos identificados, avaliados, tratados e monitorados no âmbito de cada contratação, desde a fase de planejamento até a fase de execução, incluindo a vigência contratual da solução ou serviço de TIC. Com o término da vigência do contrato, os riscos serão avaliados quanto à pertinência em manter na base de riscos de TIC. A equipe de planejamento da contratação é responsável por identificar e monitorar os riscos referentes ao processo licitatório (contratação) até a etapa de homologação, enquanto o gestor do contrato é responsável por gerenciar os riscos inerentes à execução do contrato.
- ✓ **Riscos em Projetos:** riscos gerenciados no âmbito de cada projeto de TIC, devendo ser identificados pelo PMO (Project Management Office) ou pelo líder de projeto. Os riscos em projetos de TIC são monitorados pelos seus líderes.
- ✓ **Riscos em Processos:** riscos identificados nos processos mapeados e/ou instituídos pela SETI. Os riscos em processos de TIC são monitorados pelos donos do processo ou, na falta destes, pela principal área responsável.

Novos pilares poderão ser incluídos no plano sempre que houver a necessidade.

## 2.3 OBJETIVO

Este documento visa fornecer as **diretrizes** para alcançar os objetivos da SETI com relação a gestão de riscos de TIC, em cumprimento às diretrizes da Política de Gestão de Riscos do Poder Judiciário do Estado do Paraná, estabelecidas na Resolução TJPR nº 272/2020-OE, de forma a prever eventos ou situações que possam comprometer a execução dos objetivos estratégicos definidos no Plano Diretor de TIC (PDTIC), reduzindo surpresas e prejuízos operacionais, otimizando o capital, fortalecendo as decisões em resposta aos riscos e aproveitando oportunidades, por meio de um processo de Gestão de Riscos de TIC.

## 2.4 RESPONSABILIDADES E PAPÉIS

A responsabilidade pelo gerenciamento de riscos é compartilhada por todos os envolvidos nos processos de trabalho, atividades, projetos, contratações ou iniciativas.

Com relação ao assunto Riscos de TIC, reforçamos abaixo as principais atribuições e responsabilidades:

|   |   |
|---|---|
| <b>Comitê de Gestão de Riscos</b>                         | <ul style="list-style-type: none"> <li>* Receber, apreciar e encaminhar ao Presidente do Tribunal proposta de limites de exposição a riscos de abrangência institucional;</li> <li>* Acompanhar o gerenciamento de riscos e propor alterações na Política de Gestão de Riscos;</li> <li>* Aprovar o Manual de Gestão de Riscos e suas atualizações;</li> <li>* Apoiar as ações que incentivem e promovam a cultura e a capacitação em Gestão de Riscos;</li> <li>* Dirimir dúvidas sobre a Gestão de Riscos.</li> </ul>   |
| <b>Coordenadoria de Governança, Riscos e Conformidade</b> | <ul style="list-style-type: none"> <li>* Propor ações de sensibilização e capacitação em Gestão de Riscos;</li> <li>* Elaborar o Manual de Gestão de Riscos do Poder Judiciário do Estado do Paraná e propor atualizações;</li> <li>* Coordenar e monitorar o gerenciamento de riscos;</li> <li>* Consolidar e remeter ao Comitê de Gestão de Riscos a matriz de riscos que estão fora do apetite a riscos da instituição;</li> <li>* Prestar apoio técnico aos gestores de risco nas atividades afetas ao gerenciamento de riscos;</li> <li>* Dirimir dúvidas sobre a Gestão de Riscos.</li> </ul> |

|  |  |
|--|--|
| <p><b>Gestores de Risco</b></p>  | <ul style="list-style-type: none"> <li>* Identificar, analisar, avaliar, tratar, monitorar e comunicar os riscos dos processos de trabalho, atividades, projetos ou iniciativas sob sua responsabilidade;</li> <li>* Realizar a seleção dos riscos que deverão ser priorizados para tratamento por meio de ações de caráter imediato ou de aperfeiçoamento contínuo;</li> <li>* Definir e implementar as ações de tratamento de riscos, estabelecendo prazos e meios para avaliação dos resultados;</li> <li>* Propor os níveis aceitáveis de exposição ao risco, de modo a subsidiar o apetite a risco da instituição;</li> <li>* Garantir que as informações sobre o risco estejam disponíveis para tomada de decisões;</li> <li>* Subsidiar o CGSI com informações técnicas, visando auxiliá-lo no processo de tomada de decisão.</li> </ul>            |
| <p><b>Auditoria Interna - AUDI</b></p>   | <ul style="list-style-type: none"> <li>* Realizar auditoria com o objetivo de avaliar e melhorar a maturidade e a eficácia dos processos de gerenciamento de riscos;</li> <li>* Comunicar os resultados da auditoria à Alta Administração por ocasião dos reportes administrativo e funcional.</li> </ul>  |
| <p><b>Comitê de Governança de Tecnologia da Informação e Comunicação - CGOVTIC</b></p> | <ul style="list-style-type: none"> <li>* Assegurar a alocação dos recursos necessários à Gestão de Riscos de TIC;</li> <li>* Avaliar a adequação, a suficiência e a eficácia da estrutura de Gestão de Riscos de TIC;</li> <li>* Gerir os riscos da área de TIC;</li> <li>* Deliberar sobre os riscos considerados altos e extremos que, eventualmente, lhes forem apresentados.</li> </ul>  |
| <p><b>Comitê de Governança de Segurança da Informação - CGSI</b></p>                   | <ul style="list-style-type: none"> <li>* Propor atividades de priorização de ações e gestão de riscos de segurança;</li> <li>* Deliberar sobre os riscos altos e extremos, que, eventualmente, lhes forem apresentados, relacionados à Segurança da Informação.</li> </ul>   |
| <p><b>Comitê de Gestão de Tecnologia da Informação e Comunicação - CGESTIC</b></p>     | <ul style="list-style-type: none"> <li>* Operacionalizar, no âmbito das unidades da SETI, a aplicação dos recursos disponibilizados para a gestão de riscos de TIC;</li> <li>* Dirimir eventuais dúvidas dos proprietários de risco, na execução da Gestão de Riscos de TIC;</li> <li>* Deliberar sobre os riscos considerados altos e extremos que, eventualmente, lhes forem apresentados;</li> <li>* Revisar continuamente a estrutura de Gestão de Riscos de TIC, e submetê-la à aprovação do CGSI;</li> <li>* Conscientizar os gestores sobre a importância da Gestão de Riscos de TIC e a responsabilidade inerente a cada proprietário dos riscos;</li> <li>* Escolher os processos de trabalho que devam ter os riscos gerenciados e tratados com prioridade em cada área técnica, à vista da dimensão dos prejuízos que possam causar.</li> </ul> |
| <p><b>Servidores da SETI</b></p>   | <ul style="list-style-type: none"> <li>* Executar suas atividades em conformidade com a Política de Segurança de Tecnologia da Informação e Comunicação, garantindo a minimização dos riscos à confidencialidade, integridade e disponibilidade das informações.</li> </ul>  |
| <p><b>Assessoria de Governança de TIC</b></p>  | <ul style="list-style-type: none"> <li>* Propor diretrizes para compor o Plano de Gestão de Riscos de TIC;</li> <li>* Acompanhar os riscos classificados como de nível alto e extremo, ou seja, fora do apetite a riscos da instituição, de forma a verificar se as ações de tratamento e monitoramento estão sendo cumpridas pelos responsáveis dentro dos prazos estabelecidos;</li> <li>* Reportar os riscos de TIC (altos e extremos) aos comitês (CGESTIC, CGSI e ao CGOVTIC);</li> </ul>   |

|  |  |
|--|--|
|  | * Manter interlocução com o Núcleo de Governança, Riscos e <i>Compliance</i> deste Tribunal sobre os Riscos de TIC.  |
| <b>Divisão de Processos e Eficiência Operacional de TI</b> | * Coordenar e monitorar a execução das atividades relativas à Gestão de Riscos em Processos de TIC, considerando inclusive aqueles presentes na cadeia de valor institucional. |
| <b>Divisão de Projetos e Portfólios de TI</b>              | * Coordenar e monitorar a execução das atividades relativas à Gestão de Riscos em Projetos de TIC.   |
| <b>Divisão de Gestão de Segurança da Informação</b>        | * Coordenar e monitorar a execução das atividades relativas à Gestão de Riscos de Segurança da Informação e Comunicação, relacionadas ao ambiente tecnológico da instituição.  |

## 2.5 METODOLOGIA DO PROCESSO DE GESTÃO DE RISCOS NA SETI

A Gestão de Riscos de TIC segue a Metodologia de Gerenciamento de Riscos deste Tribunal (Decreto Judiciário TJPR nº 461/2021), que se baseia nas diretrizes estabelecidas pela ABNT NBR ISO 31000:2018, adicionalmente à norma ABNT NBR ISO 27005:2019. Ambas consideram que o processo de gestão de riscos interage de forma cíclica através do: Estabelecimento do Contexto, Identificação, Análise e Avaliação dos Riscos, Tratamento de Riscos, Monitoramento e Comunicação dos Riscos.



Processo de Gestão de Riscos

O Gestor do Risco deverá realizar o mapeamento de riscos, logo após a revisão do processo, realizado com a Divisão de Processos e Eficiência Operacional.

Caso os gestores encontrem qualquer dificuldade durante este mapeamento de riscos, devem entrar em contato com a Assessoria de Governança, que estará à

disposição para fornecer o auxílio necessário para a realização do mapeamento de riscos. Dessa forma, a Assessoria de Governança realizará uma Oficina para auxiliar no mapeamento, com duração de 1h (uma hora). Essa Oficina pode ser realizada de forma *on line* pelo aplicativo Teams, ou até mesmo presencial, iniciando com uma breve apresentação sobre a Gestão de Riscos, e na sequência, é realizado o processo de mapeamento dos riscos, com o suporte do MS Excel.

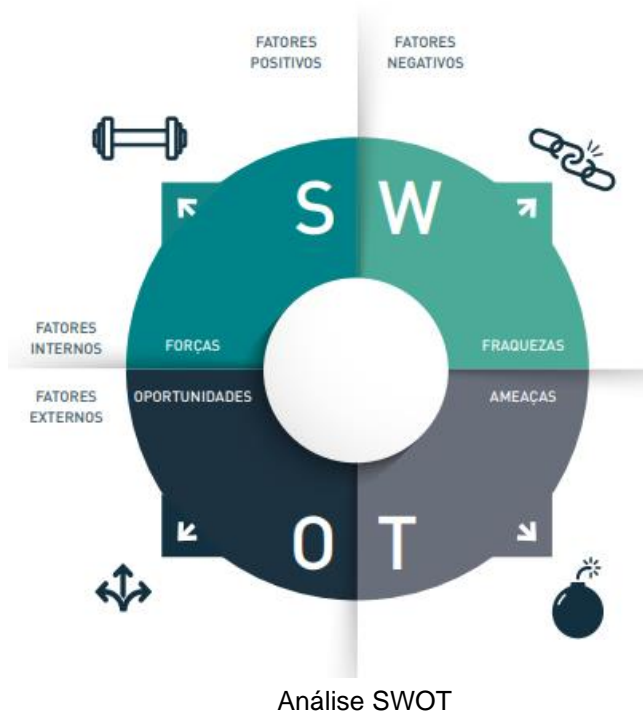
Caso essa Oficina não seja o suficiente para finalizar o mapeamento de riscos, é de **responsabilidade do Gestor do Risco realizar o término deste mapeamento.**

Durante a Oficina, percorre-se o passo a passo abaixo:

### 2.5.1 ESTABELECIMENTO DO CONTEXTO

Consiste em compreender o ambiente externo e interno no qual o objeto de gestão de riscos está inserido e identificar parâmetros e critérios a serem considerados no processo de gerenciamento de riscos.

Uma das ferramentas de gestão mais utilizadas para a análise é a técnica SWOT, que se baseia nestas definições de forças (Strengths), fraquezas (Weakness), oportunidades (Opportunities) e ameaças (Threats), e pode auxiliar no mapeamento dos fatores que impactam o processo de trabalho:



## 2.5.2 IDENTIFICAÇÃO DOS RISCOS

A etapa de Identificação dos Riscos consiste no mapeamento dos eventos de risco capazes de impactar o processo de trabalho, bem como em definir suas causas e consequências.

Para executar esta etapa, podem ser utilizadas diversas técnicas que auxiliam na identificação dos eventos de risco, tais como brainstorming, brainwriting, entrevistas ou questionários. Neste plano, recomenda-se o uso do brainstorming por conta da facilidade de execução e aplicação no levantamento dos riscos.

Verifica-se que o evento de risco é originado por uma ou mais causas que trarão determinadas consequências ao processo de trabalho, projeto ou atividade:



## 2.5.3 ANÁLISE E AVALIAÇÃO DOS RISCOS

Consiste em compreender a natureza do risco e determinar o respectivo nível de risco, mediante a combinação da probabilidade de sua ocorrência e dos impactos possíveis, levando-se em consideração os controles existentes.

| PROBABILIDADE | DESCRIÇÃO   | GRAU |
|---------------|---|------|
| Muito baixa   | Evento sem histórico de ocorrência, podendo ocorrer em circunstâncias excepcionais. | 1    |
| Baixa         | Evento sem histórico de ocorrência, mas com possibilidade excepcional.              | 2    |
| Média         | Evento com histórico de ocorrência, mas com frequência mínima.                      | 3    |
| Alta          | Evento com histórico de ocorrência, com alta frequência.                            | 4    |
| Muito alta    | Evento com histórico de ocorrência.<br>O evento só não ocorre excepcionalmente.     | 5    |

Tabela de Probabilidades

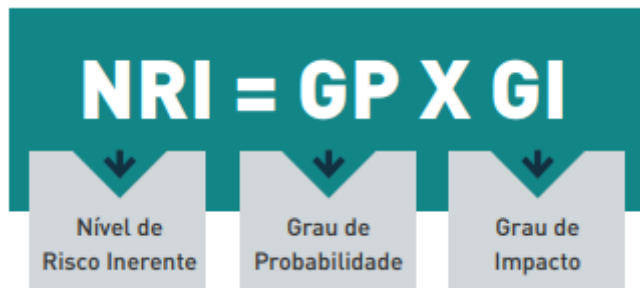
| IMPACTO     | DESCRIÇÃO   | GRAU |
|-------------|---|------|
| Muito baixo | Impacto insignificante no objetivo.                                     | 1    |
| Baixo       | Impacto pequeno no objetivo.  | 2    |
| Médio       | Impacto moderado no objetivo.   | 3    |
| Alto        | Impacto significativo no objetivo, tornando improvável seu atingimento. | 4    |
| Muito alto  | Impacto catastrófico no objetivo, impossibilitando seu atingimento.     | 5    |

Tabela de Impacto

| EFICÁCIA DO CONTROLE | SITUAÇÃO DO CONTROLE EXISTENTE  |
|----------------------|---|
| Inexistente          | Quando não há nenhum controle, ou o controle não é funcional ou é mal implementado.   |
| Fraco                | Existe algum tipo de controle, geralmente executado manualmente, porém apenas o executor conhece o procedimento. A responsabilidade pelo controle é individual e há dependência total da pessoa que realiza este controle.  |
| Mediano              | Existe um controle, porém não é o mais adequado, por não considerar todos os aspectos relevantes do risco. O controle é capaz de mitigar algum aspecto do risco, mas não é capaz de contemplar todas as perspectivas, pois há deficiências na forma como ele foi desenhado. |
| Satisfatório         | Existe um controle formalizado, que pode não considerar todos os aspectos relevantes, mas consegue mitigar o risco com auxílio de ferramentas apropriadas.  |
| Forte                | O controle empregado é o ideal. Este controle é formalizado e capaz de mitigar o risco considerando todos os seus aspectos relevantes.  |

Tabela de Definição da Eficácia dos Controles

É possível obter o Nível de Risco Inerente (NRI) de cada evento identificado, a partir do resultado da multiplicação da Probabilidade (P) pelo Impacto (I), considerando os controles existentes, conforme a fórmula que segue:



Nível de Risco Inerente

Após a fase de Análise de Riscos, inicia-se a fase de Avaliação, que consiste na definição de quais riscos necessitam ser tratados e quais terão prioridade, de acordo com o apetite aos riscos da instituição, ou seja, de acordo com o nível de riscos que a instituição está disposta a aceitar, e qual tratamento será empregado.

O Nível de Risco para cada evento identificado se dará de acordo com a classificação da tabela abaixo:

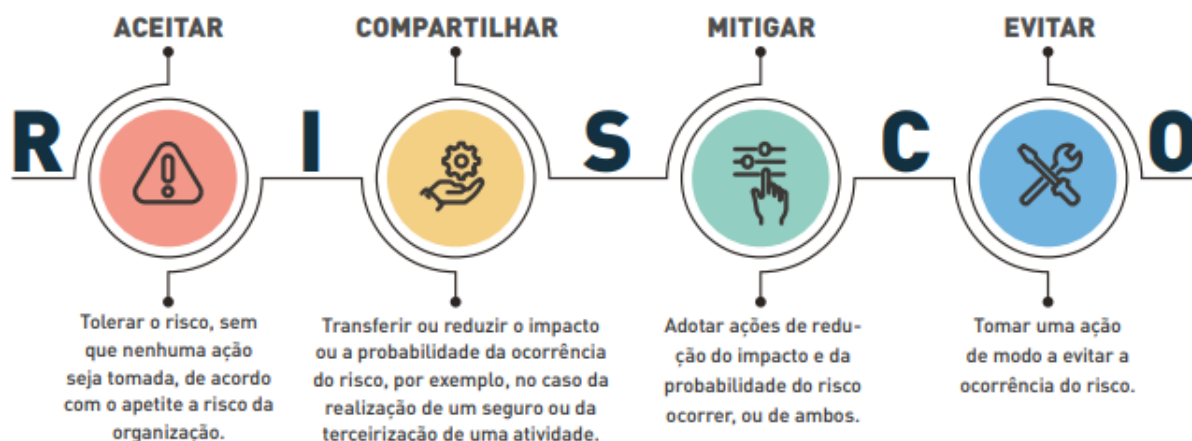
| LIMITE DE EXPOSIÇÃO | NÍVEL DO RISCO | DIRETRIZ PARA A RESPOSTA   |
|---------------------|----------------|--|
| Extremo             | 20-25          | <b>Nível de risco inaceitável:</b> Os riscos contidos nesta faixa estão acima do limite de exposição e serão prioridade absoluta. O adiamento do seu tratamento pode ocorrer exclusivamente sob justificativa do Diretor do Departamento ou cargo equivalente e com autorização do Presidente do Tribunal. |
| Alto                | 12-16          | <b>Nível de risco inaceitável:</b> Os riscos compreendidos na faixa laranja são inaceitáveis e devem ser monitorados e tratados no prazo definido pelo Gestor do Risco. O adiamento do seu tratamento pode ocorrer exclusivamente sob justificativa do Diretor do Departamento ou cargo equivalente.       |
| Médio               | 3-10           | <b>Nível de risco aceitável:</b> Os riscos contidos na faixa amarela estão dentro do apetite a riscos da instituição, mas visando a manter o nível de risco, devem ser monitorados e os controles existentes devem ser revistos.   |
| Baixo               | 1-2            | <b>Nível de risco adequado:</b> Os riscos contidos nesta faixa podem ser aceitos por estarem dentro do apetite a riscos da instituição.  |

Tabela de Diretrizes para Priorização de Riscos

## 2.5.4 TRATAMENTO DOS RISCOS

Consiste na adoção de uma ou mais ações de resposta que irão mitigar, compartilhar ou evitar os eventos, alterando, assim, o nível do risco a ser tratado.

Seguem abaixo as possíveis opções de resposta ao risco:



Para cada risco identificado, é definida uma ou mais ações de tratamento, com prazo de resolução e responsável por sua execução:

| AÇÃO DE TRATAMENTO X | RESPONSÁVEL | PRAZO      |
|----------------------|-------------|------------|
| XXXXXXXXXX           | XXXXXXXXXX  | dd/mm/aaaa |



## 2.5.5 COMUNICAÇÃO DOS RISCOS

Essa comunicação é realizada após a conclusão da Oficina de Mapeamento de Riscos.

Consiste no fornecimento das informações relativas ao risco e ao seu tratamento para todos aqueles que possam influenciar ou ser influenciados pelo risco, observada a classificação da informação quanto ao sigilo.

**A comunicação referente a gestão de riscos é realizada através da abertura de um SEI (Artefato: RELATÓRIO DE GERENCIAMENTO DE RISCOS), pelo Gestor do Risco**, garantindo uma padronização e evitando o risco de perda de informações. Importante destacar que neste SEI devem ser informadas as alterações e mudanças nos riscos e nas ações de tratamento que venham a ocorrer após a Oficina de Mapeamento dos Riscos.

## 2.5.6 MONITORAMENTO CONTÍNUO DOS RISCOS

O monitoramento é uma prática fundamental para garantir o bom funcionamento, a eficiência e o sucesso da Gestão de Riscos na STI. Atualmente, ele é realizado em planilha MS Excel pela Assessoria de Governança.

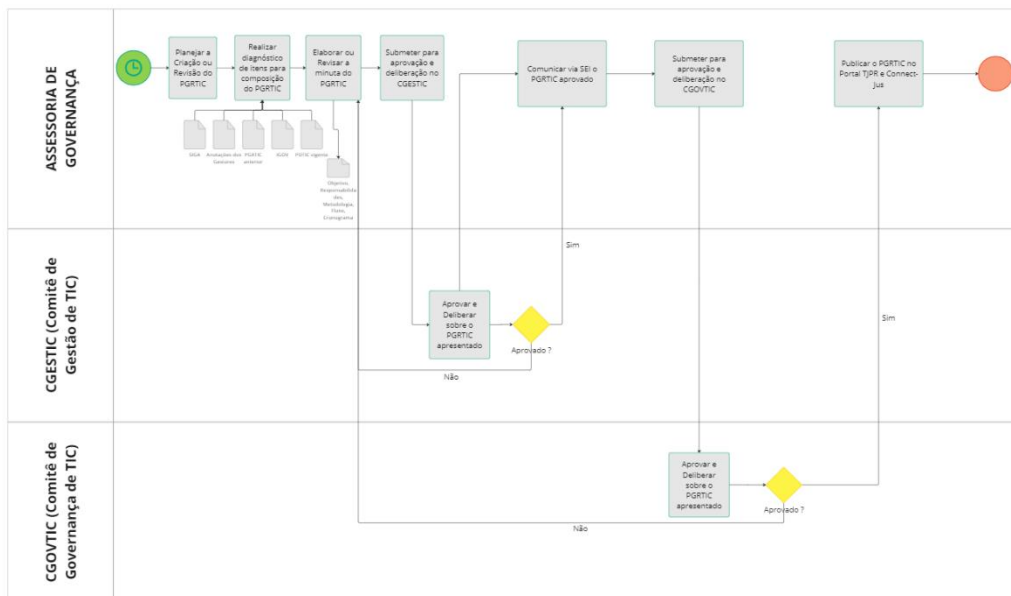
As ações abaixo são de **responsabilidade do Gestor do Risco**:

- Apresentar os resultados do monitoramento das ações de tratamento, quinzenalmente, durante as reuniões do CGESTIC (Comitê de Gestão de Tecnologia da Informação e Comunicação);
- Comunicar a Assessoria de Governança quando for identificado um novo risco, quando um risco for excluído ou alterado;
- Avaliar a eficácia das ações de tratamento de mitigação existentes.

## 3. MATRIZ DE RESPONSABILIDADES DO PROCESSO DE GESTÃO DE RISCOS NA SETI

| Atividades  | Assessoria de Governança | Gestor do Risco | Equipe do Gestor do Risco |
|---|--------------------------|-----------------|---------------------------|
| Solicitar a realização da Oficina de Mapeamento de Riscos   |                          | X               |                           |
| Criar expediente no SEI para início do Processo de Mapeamento de Riscos   | X                        |                 |                           |
| Executar o Mapeamento de Riscos (Estabelecimento do Contexto, Identificação, Análise, Avaliação e Tratamento de Riscos) |                          | X               | X                         |
| Comunicar via SEI os Riscos mapeados  |                          | X               |                           |
| Comunicar no SEI os novos Riscos/Ações de Tratamento, suas alterações e exclusões                                       |                          | X               |                           |
| Comunicar em reunião do CGESTIC os riscos mapeados  |                          | X               |                           |
| Executar as Ações de Tratamento estabelecidas   |                          | X               | X                         |
| Monitorar as Ações de Tratamento estabelecidas  | X                        |                 |                           |
| Prestar informações atualizadas nas reuniões do CGESTIC sobre a execução das Ações de Tratamento estabelecidas          |                          | X               |                           |
| Reportar os Riscos altos e extremos aos comitês (CGESTIC, CSEGTI, CGOVTIC e CGRC)                                       | X                        |                 |                           |

## 4. FLUXO DO PROCESSO DE CRIAÇÃO/REVISÃO DO PLANO



## 5. IMPORTÂNCIA DA CONSCIENTIZAÇÃO DA GESTÃO DE RISCOS

A conscientização sobre um plano de gestão de riscos é fundamental em toda a SETI para criar uma cultura organizacional resiliente, capaz de enfrentar desafios, garantir a continuidade dos negócios e aproveitar oportunidades de maneira eficaz e sustentável.

Promover a conscientização sobre a gestão de riscos deve ser parte integrante da cultura da SETI, envolvendo treinamentos regulares, comunicação clara e a incorporação de práticas de gestão de riscos em todas as Coordenadorias da SETI.

## 6. APRENDIZADO E MELHORIA CONTÍNUA

O aprendizado e a melhoria contínua são aspectos essenciais para o desenvolvimento e eficácia de qualquer plano de gestão de riscos.

Esta Assessoria de Governança sugere a realização do curso de “*Gerenciamento de Riscos no Poder Judiciário do Estado do Paraná*”, disponível na EJUD, para todos os envolvidos neste processo de mapeamento de riscos. Este curso irá facilitar o entendimento e compreensão da metodologia de gestão de riscos do Tribunal de Justiça.

## 7. REVISÃO E ATUALIZAÇÃO DO PLANO

Este documento está alinhado com o Plano Diretor de TIC (PDTIC), porém é objeto de revisão periódica, pelo menos anualmente, permitindo adaptações em decorrência das mudanças nas circunstâncias, garantindo assim sua relevância ao longo do tempo, promovendo a consistência, eficiência e qualidade em uma variedade de contextos.

Sugere-se que anualmente ou quando surgirem novos riscos altos ou extremos, promova-se uma prestação de contas de Riscos de TIC aos membros dos seguintes comitês: CGESTIC, CGSI e CGOVTIC.

## 8. CRONOGRAMA DE MAPEAMENTO DE RISCOS

O novo cronograma para mapeamento dos riscos relaciona-se com os processos mapeados da SETI. Para o ano 2024 - 2026, serão mapeados/revisados os riscos dos processos abaixo, conforme o novo cronograma:

| PLANO DE AÇÃO SOBRE RISCOS DE TIC (2024-2026) |   |  |                     |                                |
|---|---|--|---------------------|--------------------------------|
| GESTOR DO RISCO                               |   | PROCESSO DA GESTÃO DE RISCOS                     | MÊS DO MAPEAMENTO   | CADEIA DE VALOR                |
| 1   | CSI-ENG - Divisão de Engenharia de Sistemas | Metodologia de Desenvolvimento de Software - MDS | Realizado em Jan/24 | Gerir Software de TIC          |
| 2   | CQ-DQA - Divisão de Qualidade               | Gerenciamento do Conhecimento                    | Realizado em Jun/24 | Gerir Serviços de TIC          |
| 3   | SETI-AT-Assessoria Técnica                  | Gestão da Capacitação de TIC                     | Realizado em Ago/24 | Gerir Pessoas                  |
| 4   | SETI-AT-Assessoria Técnica                  | Gestão por Competências                          | Realizado em Ago/24 | Gerir Pessoas                  |
| 5   | SETI-GOV - Assessoria de Governança de TIC  | Gerenciamento de Níveis de Serviço               | Set/24              | Prover Serviços de TIC         |
| 6   | SETI-GOV - Assessoria de Governança de TIC  | Gerenciamento de Portfólio de Serviço            | Out/24              | Prover Serviços de TIC         |
| 7   | SETI-GOV - Assessoria de Governança de TIC  | Gestão do iGovTIC-JUD                            | A revisar Nov/24    | Gerir Estratégia Institucional |
| 8   | SETI-GOV - Assessoria de Governança de TIC  | Gestão do PDTIC                                  | A revisar Dez/24    | Gerir Estratégia Institucional |

|    |  |   |                     |                                       |
|----|--|---|---------------------|---------------------------------------|
| 9  | CIN-DSUST -<br>Divisão de<br>Sustentação   | Gerenciamento de<br>Eventos   | Jan/25              | Prover Serviços de TIC                |
| 10 | SETI-GOV -<br>Assessoria de<br>Governança de TIC                                       | Indicadores de<br>Desempenho de TIC   | Fev/25              | Gerir Estratégia Institucional        |
| 11 | CGP-DPROJ -<br>Divisão de Gestão<br>de Projetos e<br>Portfólios de TIC                 | Gestão de Demandas  | A revisar<br>Abr/25 | Gerir Serviços de TIC                 |
| 12 | CGP-DPROC -<br>Divisão de Gestão<br>de Processos e<br>Eficiência<br>Operacional de TIC | Gerenciamento de<br>Configuração e Ativos<br>de Serviço                         | Mai/25              | Gerir Infraestrutura de TIC           |
| 13 | CGP-Coordenadoria<br>de Gestão e<br>Planejamento de<br>TIC                             | Gerenciamento de<br>Contratações de TIC   | Jul/25              | Adquirir bens e contratar<br>serviços |
| 14 | CIN-DSUST -<br>Divisão de<br>Sustentação   | Metodologia de<br>Sustentação de<br>Software - MSS                              | Ago/25              | Gerir Software de TIC                 |
| 15 | CQ-DQA - Divisão<br>de Qualidade   | Pesquisa de Satisfação<br>de Usuários   | Out/25              | Gerir Serviços de TIC                 |
| 16 | SETI-GOV -<br>Assessoria de<br>Governança de TIC                                       | Gestão de<br>Conformidade de TIC  | Nov/25              | Gerir Conformidade                    |
| 17 | CIN-DSUST -<br>Divisão de<br>Sustentação   | Gerenciamento da<br>Capacidade  | Dez/25              | Gerir Infraestrutura de TIC           |
| 18 | CQ-DAT - Central de<br>atendimentos  | Gerenciamento do<br>Catálogo de Serviço   | Jan/26              | Prover Serviços de TIC                |
| 19 | CIN-DSUST -<br>Divisão de<br>Sustentação   | Gerenciamento de<br>Mudanças, Liberação e<br>Implantação                        | Mar/26              | Gerir Infraestrutura de TIC           |
| 20 | SETI-GOV -<br>Assessoria de<br>Governança de TIC                                       | Gestão Orçamentária<br>de TI - Plano de<br>Contratações                         | Mar/26              | Elaborar Planos<br>Orçamentários      |
| 21 | SETI-GOV -<br>Assessoria de<br>Governança de TIC                                       | Gestão de Riscos de<br>TIC  | Abr/26              | Prover Gestão de Riscos               |
| 22 | CGP-DSEG -<br>Divisão de<br>Segurança de TIC   | Gerenciamento de<br>Continuidade  | Jun/26              | Gerir Infraestrutura de TIC           |
| 23 | CQ-DAT - Central de<br>atendimentos  | Gerenciamento da<br>Central de Serviço,<br>Incidente e Requisição<br>de Serviço | Jul/26              | Prover Serviços de TIC                |
| 24 | CGP-DPROC -<br>Divisão de Gestão<br>de Processos e                                     | Gestão de Processos<br>(BPMO)   | Set/26              | Gerir Processos de Trabalho           |

|    |   |                                   |                  |                             |
|----|---|-----------------------------------|------------------|-----------------------------|
|    | Eficiência Operacional de TIC                                 |                                   |                  |                             |
| 25 | CIN-DSUST - Divisão de Sustentação                            | Gerenciamento de Problemas de TIC | Out/26           | Gerir Serviços de TIC       |
| 26 | CGP-DPROJ - Divisão de Gestão de Projetos e Portfólios de TIC | Gerenciamento de Projetos de TIC  | A revisar Nov/26 | Gerir Projetos              |
| 27 | CIN-DSUST - Divisão de Sustentação                            | Gerenciamento de Disponibilidade  | Dez/26           | Gerir Infraestrutura de TIC |

**Cadeia de valor do TJPR disponível em:**

<https://www.tjpr.jus.br/documents/959390/0/Cadeia+de+Valor.pdf/1be1dbfb-981c-4387-cce2-c5a5b18b6906>

## 9. ÍNDICE DE EXECUÇÃO DO PLANO

Este plano tem como meta atingir o percentual de **80%, 85% e 90% de execução respectivamente nos anos de 2024, 2025 e 2026**, através da realização das Oficinas de Mapeamento de Riscos referentes aos Objetos da Gestão de Riscos estabelecidos no item 8 - CRONOGRAMA DE MAPEAMENTO DE RISCOS.

A porcentagem de execução anual será calculada usando a fórmula:

$$\text{Índice de Execução Anual} = \frac{\text{Objetos de Riscos Mapeados no ano}}{\text{Total de Objetos previstos no ano}} \times 100$$

## 10. ABREVIATURAS E SIGLAS DE TI

A lista de Abreviaturas e Siglas de TI está disponível no endereço abaixo:

<https://dtic.tjpr.jus.br/siglarior-e-glossario>

## 11. CONSIDERAÇÕES FINAIS

A área da Tecnologia da Informação e Comunicação se mostra cada vez mais estratégica para o Tribunal, e entender os riscos de TIC que podem afetar os objetivos institucionais é um caminho crucial para uma gestão de excelência, contribuindo para a tomada de decisão.

Tais técnicas podem não ser suficientes para garantir que eventos negativos ocorram, no entanto, o domínio sobre estes eventos serve para reduzir a probabilidade ou o impacto de efetivamente ocorrerem.

Em suma, a adoção da Gestão de Riscos de TIC é parte integrante positiva para a efetividade da gestão governamental.