PLANO DE GESTÃO DE RISCOS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

PGRTIC 2021-2026

Data: *13/05/2022*

Versão 1.0

Plano de Gestão de Riscos de Tecnologia da Informação e Comunicação no âmbito do Poder Judiciário do Estado do Paraná

Presidente do Tribunal de Justiça do Estado do Paraná (gestão 2021- 2022)
Desembargador José Laurindo de Souza Netto

1° Vice-Presidente
Desembargador Luiz Osório Moraes Panza

2° Vice-Presidente
Desembargadora Joeci Machado Camargo

Corregedor-Geral da Justiça
Desembargador Luiz Cezar Nicolau

Corregedor de Justiça
Desembargador Espedito Reis do Amaral

Supervisor de Tecnologia da Informação e Comunicação
Desembargador Marcelo Gobbo Dalla Dea

Comitê de Governança de Tecnologia da Informação e Comunicação do TJPR

Presidente do Comitê
Desembargador Rogério Etzel

Vice-Presidente do Comitê
Desembargador Marcelo Gobbo Dalla Déa

Juiz Auxiliar da Presidência
Dr. Anderson Ricardo Fogaça

Juíza Auxiliar da 1ª Vice-Presidência
Dra. Ângela Maria Machado Costa

Juiz Auxiliar da 2ª Vice-Presidência
Dr. Luciano Carrasco Falavinha Souza

Juiz Auxiliar da Corregedoria-Geral da Justiça
Dr. Alexandre Gomes Gonçalves

Representante da AMAPAR
Dr. Marcos Caires Luz

Secretária do Tribunal de Justiça
Mariana da Costa Turra Brandão

Diretor do Departamento de Planejamento
Vinícius Rodrigues Lopes

Diretor do Departamento de Tecnologia da Informação e Comunicação
Rafael Coninck Teigão

Servidor do Departamento de Tecnologia da Informação e Comunicação
Alessio Roman Junior

Servidor do Departamento de Tecnologia da Informação e Comunicação
Pablo Tavares

Assessor Jurídico-Administrativo da Presidência
Leonardo de Andrade Ferraz Fogaça

Servidor da Corregedoria-Geral da Justiça
Gerson Mikalixen Junior

Comitê de Gestão de Riscos do TJPR

Presidente do Comitê
Drª. Fabiane Pieruccini

Diretor do Departamento de Planejamento
Vinicius Rodrigues Lopes

Secretária do Tribunal de Justiça
Mariana da Costa Turra Brandão

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 Marcelo Gobbo Dalla Déa

Secretária do Tribunal de Justiça
Mariana da Costa Turra Brandão

Juiz Auxiliar da Presidência
Dr. Anderson Ricardo Fogaça

Diretor do Departamento de Tecnologia da Informação e Comunicação
Rafael Coninck Teigão

Juiz Auxiliar da Corregedoria-Geral da Justiça
Dr. Alexandre Gomes Gonçalves

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
Cideclei Machado
Danilo Kovalechyn
Ersan Rafael Holstein
Jean Paul Bonnevialle
Carlos José Johann Kolb
Luiz Fernando Moletta Alves
Magno Mario Bayer Filho
Márcio Mortensen Wanderley
Pablo Tavares
Paulo Alfredo Ribas Toledo
Paulo Henrique Waromby
Rafael Coninck Teigão

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

Grupo de Trabalho em Segurança da Informação e Comunicação do TJPR

Lauro Andrey de Souza Bueno (líder do grupo)
Adriano Witkovski
Altimar de Souza Junior
Danilo Kovalechyn
Daniel Ferreira Caetano dos Santos
Marcio William Ebuchi
Rodrigo Daniel Campaner de Lira
Gustavo Raphael Stein

Portaria TJPR nº 5050/2021 eDJ nº 2998 em 23/06/2021 (SEI!TJPR 0031716-37.2021.8.16.6000)

Equipe Técnica na elaboração deste documento (servidores do DTIC)

Alessio Roman Junior
Daniel Targa Dias Anastacio
Gustavo Malaquias de Paula
Jefferson Wanderley Jacob
Johnatan Daniel Fromholz Lima
Pablo Tavares
Paulo Alfredo Ribas Toledo
Renan Rafael Marcon
Ricardo Schrickte Gielow

HISTÓRICO DE ALTERAÇÕES

Versão	Data	Autor(es)	Descrição
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 Araujo) 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

SUMÁRIO

TABELAS

FIGURAS

1. APRESENTAÇÃO

A Tecnologia da Informação é fundamental para o alcance dos objetivos estratégicos do Tribunal de Justiça do Estado do Paraná, dessa forma, os riscos associados à área de TI devem ser gerenciados de forma eficiente e eficaz. Este documento define o Plano de Gestão de Riscos de TIC (PGRTIC) que deverá ser aplicado no Departamento de Tecnologia da Informação e Comunicação (DTIC).

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 que "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 atividades 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. OBJETIVO

Este documento visa direcionar as ações do Departamento de Tecnologia da Informação e Comunicação (DTIC), 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 que permita a identificação, a análise, a avaliação, o tratamento, a priorização, o monitoramento e a comunicação dos riscos aos processos e aos ativos de TIC.

3. SOBRE ESTE PLANO

Este documento tem aplicabilidade para todo o DTIC do TJPR, e abrange as áreas de infraestrutura de TI, redes, segurança da informação, suporte técnico, manutenção de equipamentos e soluções de TI, desenvolvimento de sistemas, governança e gestão de TI.

O escopo da Gestão de Riscos de TIC é o de analisar os possíveis riscos relacionados aos processos e aos ativos de TIC que podem afetar os objetivos estratégicos da organização.

Este documento está alinhado com o Planejamento Estratégico Institucional e Diretor do DTIC, portanto ao ciclo 2021-2026, porém será objeto de revisão periódica, pelo menos **Trimestralmente**, buscando adequações à realidade do órgão e da sociedade e de mudanças do Judiciário.

4. ABREVIAÇÕES E DEFINIÇÕES

ABREVIAÇÕES:

- **CNJ**: Conselho Nacional de Justiça
- **DTIC**: Departamento de Tecnologia da Informação e Comunicação
- **ENTIC-JUD**: Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário
- **PCSTIC**: Plano de Contratações de Solução de TIC
- **PCTIC**: Plano de Capacitação de TIC
- **PDTIC**: Plano Diretor de Tecnologia da Informação e Comunicação
- **PSI**: Política de Segurança da Informação
- **PTD**: Plano de Transformação Digital
- **SEI**: Sistema Eletrônico de Informações
- **SIC**: Segurança da Informação e Comunicação
- **TCU**: Tribunal de Contas da União
- **TIC**: Tecnologia da Informação e Comunicação
- **TJPR**: Tribunal de Justiça do Estado do Paraná

DEFINIÇÕES:

Ameaça: causa potencial de um incidente indesejado, que possui potencial para comprometer ativos através de exploração de vulnerabilidades.

Apetite a risco: nível de risco que a instituição está disposta a aceitar para atingir os objetivos identificados no contexto analisado.

Ativos de TIC: qualquer elemento de valor para organização, seja tangível ou intangível, que esteja relacionado à Tecnologia da Informação e Comunicação.

Causa de Risco: razão que pode promover a ocorrência do risco.

CGOVTIC – Comitê de Governança de Tecnologia da Informação e Comunicação: comitê responsável por apoiar e orientar as iniciativas, projetos e investimentos em Tecnologia da Informação e Comunicação, observando a estratégia institucional, dentre outros.

CGESTIC – Comitê Gestor de Tecnologia da Informação e Comunicação: comitê responsável pelos planos táticos e operacionais, análise de demandas, acompanhamento da execução de planos, estabelecimento de indicadores operacionais, dentre outros.

CSEGTI – Comitê de Segurança de Tecnologia da Informação: comitê responsável por apreciar, assessorar e aprovar a implementação das ações de segurança da informação e garantir a implementação da Política de Segurança de Tecnologia da Informação.

Consequências: resultado de um evento que afeta os objetivos estabelecidos.

Escopo: é a soma total de todos os produtos do processo de trabalho e seus requisitos ou características.

Evento: incidente ou ocorrência originada a partir de fontes internas ou externas que afetem a implementação da estratégia ou a realização dos objetivos.

Fonte de Risco: elemento que, individualmente ou combinado, tem potencial para dar origem a um risco específico, podendo ou não estar sob controle.

Impacto: efeito da ocorrência do evento nos objetivos.

Gestão de Riscos: processo contínuo aplicado a toda a instituição que consiste no desenvolvimento de um conjunto de ações destinadas a identificar, analisar, avaliar, tratar e monitorar eventos em potencial, contribuindo para a sua redução ou neutralização.

Matriz de Riscos: representação formal na qual são registrados os riscos identificados, considerando as probabilidades e os impactos, de forma a permitir a definição das ações necessárias ao seu gerenciamento.

Nível de Risco: representação numérica da magnitude do risco, que é expressa pelo produto das variáveis “impacto” e “probabilidade”.

Parte interessada (*Stakeholder*): pessoa ou organização que pode afetar, ser afetada ou perceber-se afetada por uma decisão ou atividade.

Plano de Contingência: documento que apresenta detalhadamente os procedimentos e recursos a serem utilizados em caso de ocorrência de eventos que possam afetar a segurança de pessoas, do patrimônio ou de sistemas de informação, bem como outros que possam interromper a continuidade da prestação de serviços jurisdicionais.

Probabilidade: possibilidade de ocorrência do evento.

Risco: evento capaz de afetar positiva ou negativamente os objetivos e metas do Poder Judiciário do Estado do Paraná.

Risco-Chave: risco com elevado impacto nos objetivos da instituição.

Risco Inerente: é aquele ao qual a instituição está exposta, considerando os controles existentes, mas quando não são estabelecidos nem adotados tratamentos para alterar a probabilidade ou o impacto dos eventos.

Risco Residual: risco remanescente após estabelecimento e adoção de tratamento.

5. REFERÊNCIAS NORMATIVOS

ID	Documento	Descrição
RN01	CNJ - Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD), no período de 2021-2026.	Dispõe sobre a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD), no período de 2021-2026. Resolução nº 370 do CNJ, 28/01/2021.
RN02	CNJ - Política de Governança das Contratações Públicas no Poder Judiciário.	Dispõe sobre a Política de Governança das Contratações Públicas no Poder Judiciário. Resolução nº 347 do CNJ, 13/10/2020.
RN03	Política de Segurança de Tecnologia da Informação do TJPR.	Dispõe sobre a Política de Segurança de Tecnologia da Informação, no âmbito do Poder Judiciário do Estado do Paraná, e estabelece competências administrativas aos seus órgãos integrantes. Objetiva instituir responsabilidades e diretrizes corporativas para a proteção dos ativos de Tecnologia da Informação e a prevenção de responsabilidade legal para todas as autoridades judiciais, servidores e usuários do Poder Judiciário do Estado do Paraná. Documento 0964880 no SEI!TJPR 0063818-25.2015.8.16.6000. Decreto Judiciário nº 631/2016 publicado no diário da justiça nº 1827 em 23/06/2016.
RN04	Política de Gestão de Riscos do TJPR.	Dispõe sobre a Política de Gestão de Riscos e institui o Comitê de Gestão de Riscos do Poder Judiciário do Estado do Paraná. Resolução nº 272/2020 - OE do TJPR, 14/09/2020.
RN05	Manual de Gestão de Riscos do TJPR.	Documento que apresenta, resumidamente, os principais conceitos, princípios e atores da gestão de riscos, possibilitando que qualquer pessoa possa compreender e gerir os riscos nos processos de trabalho em que atue.

ID	Documento	Descrição
		SEI!TJPR 0021241-22.2021.8.16.6000. Decreto Judiciário nº 461/2021 publicado no diário da justiça nº 3030 em 06/08/2021.
RN06	Política de Proteção aos Dados Pessoais, conforme a Lei nº 13.709/2018 (LGPD).	Estabelece medidas para o processo de adequação à Lei Geral de Proteção de Dados Pessoais a serem adotadas pelos tribunais.
RN07	Comitê de Segurança de Tecnologia da Informação (CSEGTI) do TJPR.	Instituir o Comitê de Segurança de Tecnologia da Informação e a Política de Segurança de TI. Decreto Judiciário nº 631/2016, em 23/06/2016.
RN08	Comitê Gestor de Tecnologia da Informação e Comunicação (CGESTIC) do TJPR.	Institui o Comitê Gestor de Tecnologia da Informação e Comunicação (CGESTIC), no âmbito do Tribunal de Justiça do Estado do Paraná. Decreto Judiciário nº 506 do TJPR, em 22/08/2019.
RN09	Comitê de Governança de Tecnologia da Informação e Comunicação (CGOVTIC)	Institui o Comitê de Governança de Tecnologia da Informação e Comunicação e define suas diretrizes no âmbito do Tribunal de Justiça do Estado do Paraná. Decreto Judiciário nº 361 do TJPR, em 04/06/2019.
RN10	NS - Normas de segurança para a utilização do Serviço de Correio Eletrônico institucional no âmbito do Poder Judiciário do Estado do Paraná.	Estabelece normas de segurança para a utilização do serviço de Correio Eletrônico institucional no âmbito do Poder Judiciário do Estado do Paraná. SEI!TJPR 0029764-62.2017.8.16.6000. Instrução Normativa TJPR nº 03/2018, publicado no diário da justiça nº 2294 em 04/07/2018.
RN11	NS - Normas de segurança para Acesso à Internet no âmbito do Poder Judiciário do Estado do Paraná.	Estabelece normas para o acesso à Internet no âmbito do Poder Judiciário do Estado do Paraná. SEI!TJPR 0029904-96.2017.8.16.6000. Instrução Normativa TJPR nº 07/2018, publicado no diário da justiça nº 2295 em 05/07/2018.
RN12	NS - Normas para fornecimento, uso e recolhimento de Ativos de TIC disponibilizados aos usuários pelo DTIC no âmbito do Poder Judiciário do Estado do Paraná.	Instrução Normativa que estabelece normas para fornecimento, uso e recolhimento de Ativos de Tecnologia da Informação e Comunicação disponibilizados aos usuários pelo Departamento de Tecnologia da Informação e Comunicação no âmbito do Poder Judiciário do Estado do Paraná. SEI!TJPR 0091648-24.2019.8.16.6000. Instrução Normativa TJPR nº 63/2021, publicado no diário da justiça nº 320 em 23/07/2021.
RN13	ABNT NBR ISO/IEC 31000:2018	ABNT NBR ISO/IEC 31000:2018 – Gestão de riscos – Diretrizes.

ID	Documento	Descrição
RN14	ABNT NBR ISO/IEC 27005:2019	ABNT NBR ISO/IEC 27005:2019 – Tecnologia da informação — Técnicas de segurança — Gestão de riscos de segurança da informação.
RN15	Manual de Gestão de Riscos do TCU.	Manual de Gestão de Riscos do TCU (2020). Disponível em: https://portal.tcu.gov.br/, acessado em 04/05/2022.
RN16	Plano de Gestão de Riscos de TI do TRE-PI.	Plano de Gestão de Riscos de TI do TRE-PI (2021). Disponível no https://connect.cnj.jus.br, acessado em 18/04/2022.
RN17	TRT1-RJ-2021-Plano de Gesto de Riscos de TIC	Disponível no https://connect.cnj.jus.br, acessado em 18/04/2022.

Tabela 1 - Documentos de Referência para elaborar o PGRTIC do TJPR

6. RESPONSABILIDADES

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

Comitê de Gestão de Riscos do TJPR

- Receber, apreciar e encaminhar ao Presidente do Tribunal proposta de limites de exposição a riscos de abrangência institucional;
- Receber, apreciar e encaminhar o Plano de Tratamento de Riscos-Chave;
- Acompanhar o gerenciamento de riscos e propor alterações na Política de Gestão de Riscos;
- Aprovar o Manual de Gestão de Riscos e suas atualizações;
- Dirimir dúvidas sobre a Gestão de Riscos.

CGOVTIC

- Assegurar a alocação dos recursos necessários à Gestão de Riscos de TIC;
- Avaliar a adequação, a suficiência e a eficácia da estrutura de Gestão de Riscos de TIC;
- Gerir os riscos da área de TIC;
- Reportar Riscos de TIC (altos e extremos) ao Núcleo de Governança, Riscos e Compliance deste Tribunal.

CSEGTI

- Deliberar, após apreciação do CGESTIC, sobre os riscos considerados altos e extremos, que se encontram fora do apetite a riscos da instituição e que lhe forem submetidos por aquele Comitê Gestor;
- Assegurar que os riscos identificados pelo processo de gestão de riscos serão tratados por meio de ações a curto, médio ou longo prazos ou de aperfeiçoamento contínuo.

CGESTIC

- Operacionalizar, no âmbito das unidades do DTIC, a aplicação dos recursos disponibilizados para a gestão de riscos de TIC;
- Dirimir eventuais dúvidas dos proprietários de risco, na execução da Gestão de Riscos de TIC;
- Deliberar sobre os riscos considerados altos e extremos que, eventualmente, lhes forem apresentados pelos proprietários de risco;
- Submeter ao CSEGTI, após sua apreciação e manifestação, os riscos considerados altos e extremos;
- Subsidiar o CSEGTI com informações técnicas, visando auxiliá-lo no processo de tomada de decisão;
- Revisar continuamente a estrutura de Gestão de Riscos de TIC, e submetê-la à aprovação do CSEGTI;
- Conscientizar os gestores sobre a importância da Gestão de Riscos de TIC e a responsabilidade inerente a cada proprietário dos riscos;
- 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.

Grupo de Trabalho de Segurança de TIC

- Executar a Gestão de Riscos de TIC relacionados a Segurança de TIC;
- Subsidiar os comitês (CGESTIC, CSEGTI e ao CGOVTIC) com informações técnicas, para auxiliar na tomada de decisão;
- Alertar ou acionar demais envolvidos na Gestão de Riscos de TIC.

Proprietário de Risco de TIC / Gestor de Risco de TIC / Gestor de Unidade do DTIC

- Identificar, analisar, avaliar, tratar, monitorar e comunicar os Riscos de TIC dos seus respectivos processos de trabalho, atividades, sistemas, serviços, projetos, contratos ou iniciativas sob sua responsabilidade;
- Realizar a seleção dos riscos que deverão ser priorizados para tratamento por meio de ações de caráter imediato ou de aperfeiçoamento contínuo;

- Definir e implementar as ações de tratamento de riscos, estabelecendo prazos, responsáveis e meios para avaliação dos resultados;
- Reportar para Assessoria de Governança de TIC os riscos considerados altos ou extremos;
- Garantir que as informações sobre o risco estejam disponíveis para tomada de decisões;
- Realizar reuniões periódicas com envolvidos para monitorar os riscos de TIC identificados com alto ou extremo;
- Acompanhar a Gestão de Riscos de TIC e comunicar ao gestor imediato e Assessoria de Governança de TIC.

Assessorias, Divisões e Consultorias do DTIC

- Executar suas atividades em conformidade com a Política de Segurança de Tecnologia da Informação, garantindo a minimização dos riscos à confidencialidade, integridade e disponibilidade das informações.

Assessoria de Governança de TIC

- Propor diretrizes para compor o Plano de Gestão de Riscos de TIC;
- 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;
- Reportar Riscos de TIC (altos e extremos) aos comitês (CGESTIC, CSEGTI e ao CGOVTIC);
- Manter interlocução com o Núcleo de Governança, Riscos e Compliance deste Tribunal sobre os Riscos de TIC.

Divisão de Gestão de Projetos e Processos de TIC

- Coordenar e monitorar a execução das atividades relativas à Gestão de Riscos em Projetos de TIC;
- 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.

Divisão de Gestão da Segurança de TIC

- Coordenar e monitorar a execução das atividades relativas à Gestão de Riscos de Segurança da Informação e Comunicação, relacionadas ao ambiente tecnológico da instituição;

- Propor definições na área de TIC que envolvam segurança, proteção de dados, serviços em nuvem, continuidade de serviços essenciais, incidentes e riscos de segurança e assuntos correlatos.

Divisão de Gestão de Contratos TIC

- Coordenar e monitorar a execução das atividades relativas à Gestão de Riscos em Contratações de TIC;

Núcleo de Governança, Riscos e *Compliance*

- Propor ações de sensibilização e capacitação em Gestão de Riscos;
- Elaborar o Manual de Gestão de Riscos do Poder Judiciário do Estado do Paraná e propor atualizações;
- Coordenar e monitorar o gerenciamento de riscos;
- Consolidar a matriz de riscos-chave;
- Elaborar e encaminhar o Plano de Tratamento de Riscos-Chave;
- Prestar apoio técnico aos gestores de risco nas atividades afetas ao gerenciamento de riscos.

Departamento de Auditoria Interna

- Avaliar a eficácia da Gestão de Riscos de TIC;
- Comunicar à Alta Administração os resultados da avaliação da Gestão de Riscos de TIC.

7. METODOLOGIA E PROCESSO DE GESTÃO DE RISCOS DE TIC

A Gestão de Riscos de TIC no TJPR deve seguir 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 dos Riscos, Análise e Avaliação dos Riscos, Tratamento, Monitoramento e Comunicação dos Riscos.

Fonte da imagem: Manual de Gestão de Riscos do TJPR (SEI!TJPR 0021241-22.2021.8.16.6000 doc. 6666099)

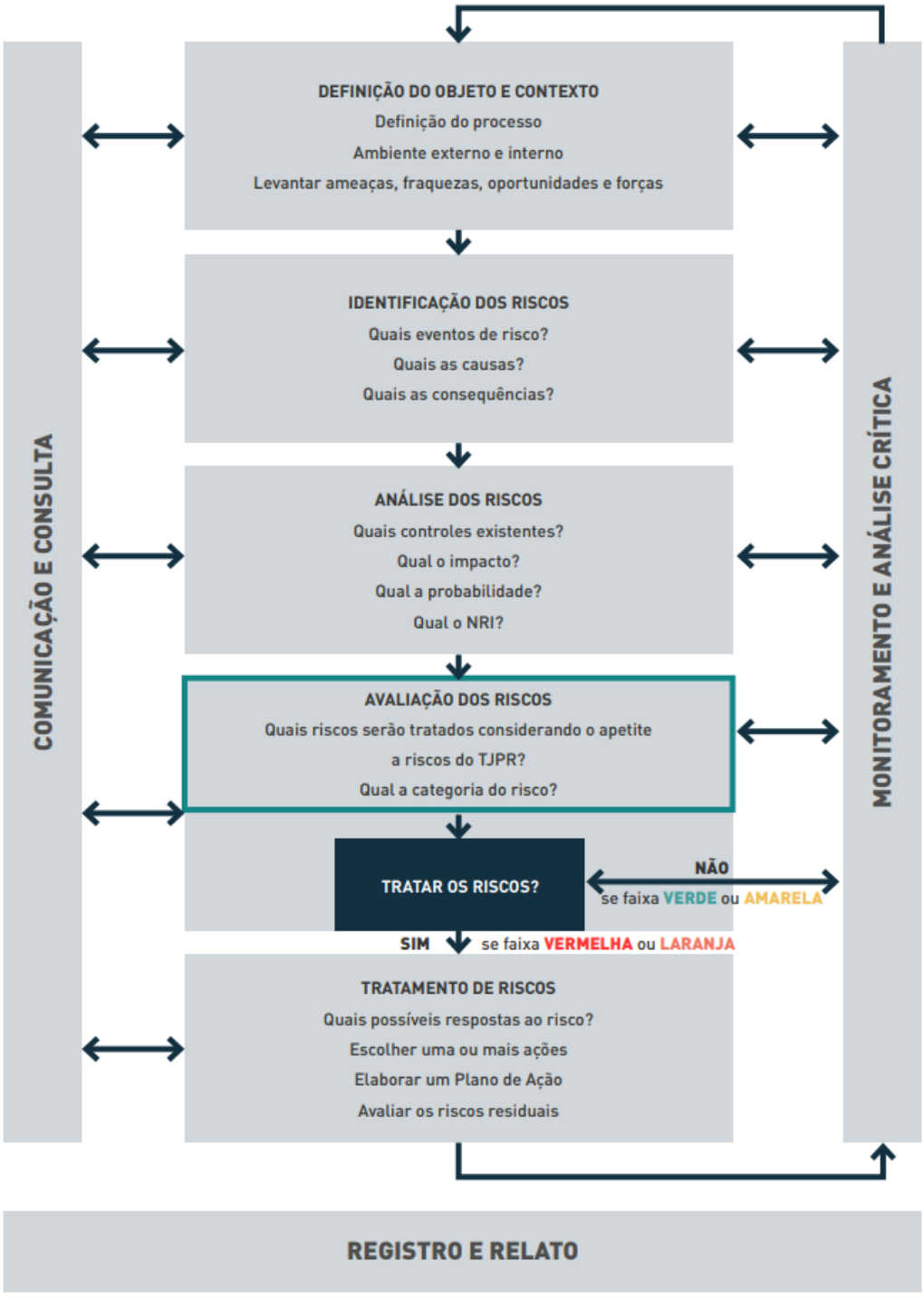

Figura 1 - Fluxo do Processo de Gestão de Riscos do TJPR

O processo de Gestão de Riscos de TIC é coordenado pela Assessoria de Governança de TIC, tendo na sua execução a participação das demais unidades do DTIC, do Grupo de Trabalho de Segurança de TIC, do Comitê Gestor de TIC (CGESTIC), do Comitê Gestor de Segurança da Informação (CSEGTI) e do Comitê de Governança de TIC (CGOVTIC).

A operacionalização dos dados ficará a cargo dos gestores de riscos através da ferramenta Microsoft Excel conforme modelo apresentado na seção de anexos deste documento e o calendário das reuniões será apresentado oportunamente pela Assessoria de Governança de TIC.

8. PRINCIPAIS RISCOS TRATADOS

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

a) **Riscos Estratégicos de TIC**: riscos identificados e analisados no escopo da elaboração dos artefatos e nos sistemas e serviços estratégicos para o Tribunal. 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. Com o término da vigência do PDTIC, os riscos serão avaliados quanto a pertinência em transportá-los para as futuras versões do plano.

b) **Riscos de Segurança da Informação e Comunicação (SIC)**: 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 para o Tribunal 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.

c) **Riscos em Contratações de TIC**: 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 a 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 de licitatório (contratação) até etapa de homologação, enquanto o gestor do contrato é responsável por gerenciar os riscos inerentes à execução do contrato.

d) **Riscos em Projetos de TIC:** são gerenciados no âmbito de cada projeto de TIC, devendo ser identificados pelo PMO ou Líder de Projeto do mesmo. Os riscos em projetos de TIC são monitorados pelos Líderes de Projetos.

e) **Riscos em Processos de TIC:** riscos identificados nos processos mapeados e/ou instituídos pelo DTIC.

Assim que todo os riscos citados acima forem contemplados no Processo de Riscos de TIC, outros poderão ser sugeridos.

A Assessoria de Governança de TIC fará reuniões de acompanhamento da execução do processo de gestão de Riscos de TIC, conforme acordado na Matriz dos Riscos de TIC (ver sugestão de modelo de matriz no anexo 11). Os procedimentos operacionais e dinâmica das reuniões serão divulgados em documento específico.

Sugere-se **semestralmente ou quando surgirem novos riscos altos ou extremos** que de demandem uma prestação de contas de Riscos de TIC aos membros do CGESTIC, CSEGTI e CGOVTIC.

As ações definidas neste Plano terão a sua execução acompanhada pelos comitês CGESTIC, CSEGTI e CGOVTIC, bem como qualquer deliberação que seja necessária daquele fórum, considerando as suas atribuições e responsabilidades, definidas na Política.

9. PLANO DE AÇÃO SOBRE RISCOS DE TIC

Atividades necessárias ou próximas ações para continuidade da análise dos riscos de TIC, a serem realizadas no período de julho de 2022 a julho de 2023:

ID	Título
1	Revisar a Política de Segurança de TI e seus normativos
2	Definir a Lista de Serviços de TIC Estratégicos para o Tribunal
3	Revisar a lista de sistemas e serviços Críticos de TIC para o DTIC
4	Realizar o processo de gestão de riscos de TIC para os serviços de TIC estratégicos
5	Realizar o processo de gestão de riscos de TIC para os sistemas e serviços críticos de TIC ou originados pelo Plano de Gestão da Continuidade de Serviços de TIC
6	Realizar o processo de gestão de riscos nas Contratações de TIC para exercício 2022 e 2023
7	Realizar o processo de gestão de riscos de TIC nos contratos de TIC vigentes.
8	Realizar o processo de gestão de riscos TIC nos projetos de TIC estratégicos.
9	Realizar o processo de gestão de riscos TIC nos processos de TIC estratégicos.

** obs.: em virtude da reestruturação do DTIC os nomes das unidades responsáveis serão atualizados na próxima revisão deste documento.*

10. CONSIDERAÇÕES FINAIS

A área da Tecnologia da Informação e Comunicação (TIC) 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 e contribui 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 que ocorram ou o impacto ao efetivamente ocorrerem.

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

11. ANEXOS

11.1. ESCALA DE VALORES PARA APURAÇÃO DO NÍVEL DE RISCO

Tabelas obtidas na proposta do "***Manual de Gestão de Riscos***" para o TJPR, conforme documento **6513902** SEI!TJPR **0021241-22.2021.8.16.6000**.

- PROBABILIDADE (1 a 5):

TABELA DE PROBABILIDADES

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. O evento só não ocorre excepcionalmente.	5

Tabela de Probabilidades

- IMPACTO (1 a 5):

TABELA DE IMPACTO

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

- NÍVEL DE RISCO, calculado por (probabilidade X impacto):

NÍVEL DE RISCO	
Baixo	1-2
Médio	3-10
Alto	12-16
Extremo	20-25

11.2. Planilha modelo para Gestão de Riscos de TIC (parte 1)

1.0.0	Unidade do DTIC:	Assessoria Técnica	Data Última Revisão:
	Processo / Atividade:	(Informar Nome do Processo ou Atividade, quando aplicável)	05/04/2022
	Objetivo:	(Informar Objetivo do Processo ou Atividade de TIC, quando aplicável)	Data Próxima Revisão:
			05/05/2022

TJPR - PLANO DE GESTÃO DE RISCOS DE TIC

		IDENTIFICAÇÃO DE RISCOS				AVALIAÇÃO DOS RISCOS				
ID	CONTEXTO	EVENTOS DE RISCO	CAUSA (fonte + vulnerabilidade)	CONSEQUÊNCIAS (impacto no objetivo)	CATEGORIA DO RISCO	CONTROLES EXISTENTES	EFICÁCIA DOS CONTROLES	PROBABILIDADE	IMPACTO	NÍVEL de Risco Nível do Risco 1 a 2 = Baixo 3 a 10 = Médio 12 a 16 = Alto 20 a 25 = Extremo
	(Nome do Contexto dos Riscos)	*(uma linha para cada evento de risco)*	*(informar vários itens na mesma célula)*	*(informar vários itens na mesma célula)*	*(selecionar o item)*	*(informar vários itens na mesma célula)*	*(selecionar o item)*			Probabilidade x Impacto
R01			1. 2. n.	1. 2. n.		1. 2. n.				
R02			1. 2. n.	1. 2. n.		1. 2. n.				
R03			1. 2. n.	1. 2. n.		1. 2. n.				

11.3. Planilha modelo para Gestão de Riscos de TIC (parte 2)

TRATAMENTO DOS RISCOS							MONITORAMENTO	
TIPO DE RESPOSTA AO RISCO *(selecionar o item)*	AÇÃO DE PREVENÇÃO *(descrever várias ações na mesma célula)*	RESPONSÁVEL PELO RISCO (Nome e Cargo) *(pessoa ou unidade)*	PRAZO PARA RESPOSTA *(data limite dd/mm/aaa)*	AÇÃO DE CONTINGÊNCIA *(descrever várias ações na mesma célula)*	RESPONSÁVEL PELA CONTIGÊNCIA (Nome e Cargo) *(pessoa ou unidade)*	PRAZO PARA CONTINGÊNCIA *(data dd/mm/aaa)*	OBSERVAÇÕES GERAIS *(descrições)*	STATUS (selecionar o item)
								0.Não Iniciado