TRIBUNAL DE JUSTIÇA
DO ESTADO DO PARÁ

PLANO DE GESTÃO DE RISCOS DE TIC – PGRTIC

TRIBUNAL DE JUSTIÇA
DO ESTADO DO PARÁ

PLANO DE GESTÃO DE RISCOS DE TIC – PGRTIC

– SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO –

2025 - 2027

PRESIDENTE DO TJPA

DESEMBARGADOR ROBERTO GONÇALVES DE MOURA

VICE-PRESIDENTE DO TJPA

DESEMBARGADOR LUIZ GONZAGA DA COSTA NETO

DESEMBARGADOR CORREGEDOR GERAL DE JUSTIÇA

DESEMBARGADORA MARIA ELVINA GEMAQUE TAVEIRA

SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

SECRETÁRIO DE TIC

DIEGO BAPTISTA LEITÃO

SECRETÁRIO ADJUNTO DE TIC

BRUNO RODRIGUES CARDOSO

COORDENADOR DE APLICAÇÕES

ÁLVARO ROGERS CARDOSO ALVÃO

COORDENADORA DE ATENDIMENTO AO USUÁRIO

ALINE SANTOS DE OLIVEIRA

COORDENADORA DE GOVERNANÇA

LUCIANA MACHADO SILVEIRA MELLO

COORDENADOR DE INFRAESTRUTURA TECNOLÓGICA

ARILSON GALDINO DA SILVA

ASSESSORES DE INFORMÁTICA

ANDREY DIEGO DA SILVA ALBUQUERQUE

MARCIO GOES DO NASCIMENTO

MAURICIO DE FREITAS BRAGA

MIGUEL JOSE DE ALMEIDA PERNAMBUCO

PAULA NANCY LIMA DIOCESANO GUERREIRO

WELLEN DE PAULA MONTEIRO AMADOR

CHEFES DE DIVISÃO / SERVIÇO

ALEXANDER RICHARD VINSON

BRUNO VIEIRA DOS SANTOS

CARLOS DIEGO POJO DE BRITO

DANIEL FONTES PEREIRA

DENISON LEANDRO SERRAO SOARES

FÁBIO VENICIUS FERREIRA DOS REIS

IGOR PINTO SIMÕES

JOSÉ DE ANDRADE GOYANA JUNIOR

MARCUS SERGIO FERREIRA NEVES

MARILIA PAULOS TELES

MURILO DE MELO SILVA

PAULO ROBERTO LOURINHO DOS SANTOS

RAMON SANTOS DO NASCIMENTO

JORGE ANDRÉ SILVA ABDON

WANDERSON BENEDITO SOUZA DA COSTA

COMISSÃO DE INFORMÁTICA
(PORTARIA Nº 1570/2025-GP)

DESEMBARGADOR ALEX PINHEIRO CENTENO
J. EDMAR SILVA PEREIRA
Jª. KÁTIA PARENTE SENA
ARILSON GALDINO DA SILVA
BRUNO RODRIGUES CARDOSO
DIEGO BAPTISTA LEITÃO
PAULA NANCY LIMA DIOCESANO GUERREIIRO

COMITÊ DE GOVERNANÇA DE SEGURANÇA DA INFORMAÇÃO
(PORTARIA Nº 1093/2025-GP)

DESEMBARGADOR ALEX PINHEIRO CENTENO
Jª. PATRÍCIA DE OLIVEIRA SÁ MOREIRA
ARILSON GALDINO DA SILVA
DIEGO BAPTISTA LEITÃO
MIGUEL LUCIVALDO ALVES SANTOS
MAURÍCIO CRISPINO GOMES
HELLEN GEYSA DA SILVA MIRANDA BRANCALHÃO
TIAGO SILVA GUIMARÃES
PAULO VICTOR RAMOS CORRÊA
CEL. QOPM MARLON SILVA NASCIMENTO
FÁBIO DJAN OLIVEIRA DE LIMA
WILL MONTENEGRO TEIXEIRA

COMITÊ DE GOVERNANÇA DE TIC
(PORTARIA Nº 3477/2025-GP)

JOÃO VALÉRIO DE MOURA JUNIOR
DIEGO BAPTISTA LEITÃO
MIGUEL LUCIVALDO ALVES SANTOS
MAURÍCIO CRISPINO GOMES
TIAGO SILVA GUIMARÃES
LUCIANA SÁ FERNANDES
LUCIANA MACHADO SILVEIRA MELLO
PAULA NANCY LIMA DIOCESANO GUERREIRO
JEAN KARLO QUINTELA DE SOUZA
CARLOS ALBERTO MAGALHÃES BREMGARTNER
LORENA RAMOS DO VALE

COMITÊ DE GESTÃO DE TIC
(PORTARIAS Nº 2309/2025 E 2900/2025-GP)

ARILSON GALDINO DA SILVA
ALINE SANTOS DE OLIVEIRA
ÁLVARO ROGERS CARDOSO ALVÃO
BRUNO RODRIGUES CARDOSO
DIEGO BAPTISTA LEITÃO
LUCIANA MACHADO SILVEIRA MELLO
PAULA NANCY LIMA DIOCESANO GUERREIRO

FICHA DE CONTROLE DE VERSÃO E PUBLICIDADE DE DOCUMENTOS

Identificação do Documento			
Título:	Plano de Gestão de Riscos de TIC	Sigla:	PGRTIC
Tipo do documento:	() Norma () Política **(X) Plano** () Protocolo Outro: _____		
Elaborado por:	SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO		
Publicidade			
Classificação:	() Público **(X) Institucional** () Departamental () Restrito () Controlado		
Forma de Publicação:			
Documentos Relacionados:	PCN PSI	ID:	

Versão	Data	Autoria	Descrição da Alteração	Aprovado Por
Versão 1.0	20/10/2023	Fábio Azevedo, Cleber Rocha	Criação do documento.	COMITÊ DE GOVERNANÇA DE SEGURANÇA DE TIC (CGSI)
Versão 2.0	23/05/2024	Maurício Braga, Fábio Azevedo	Adequações ao Manual de Gestão de Risco e à Declaração de Apetite a Risco.	COMITÊ DE GOVERNANÇA DE SEGURANÇA DE TIC (CGSI)
Versão 3.0	28/07/2025	Paulo Lourinho, Fábio Azevedo	Revisão de conteúdo.	COMITÊ DE GOVERNANÇA DE SEGURANÇA DE TIC (CGSI)

SUMÁRIO

APRESENTAÇÃO 7

1. INTRODUÇÃO 7

1.1. VINCULAÇÃO 8

1.2. PRINCÍPIOS 8

1.3. OBJETIVOS 10

1.4. ABRANGÊNCIA / APLICABILIDADE 10

1.5. VIGÊNCIA E REVISÕES 11

1.6. REFERÊNCIAS NORMATIVAS E AUXILIARES 11

2. DIAGNÓSTICO DO AMBIENTE 13

2.1. VISÃO GERAL 13

2.2. CONTEXTUALIZAÇÃO 14

3. ESTRUTURA DE GESTÃO DE RISCOS DE TIC 15

3.1. ESTRUTURA 15

3.2. COMPETÊNCIAS E RESPONSABILIDADES 17

3.3. INTEGRAÇÃO AOS PROCESSOS ORGANIZACIONAIS 21

3.4. RECURSOS 23

3.5. CAPACITAÇÃO 25

4. PROCESSO DE GESTÃO DE RISCOS DE TIC 25

4.1. METODOLOGIA 25

4.2. ESCOPO 26

4.3. HIERARQUIA DE RISCOS 27

4.4. APETITE E TOLERÂNCIA AO RISCO 28

4.5. RELATÓRIO DE ANÁLISE E AVALIAÇÃO DE RISCOS 30

4.6. PLANO DE AÇÕES E CRONOGRAMA 31

4.7. INDICADORES DE PROCESSO 32

4.8. MONITORAMENTO E CONTROLE 33

5. CONSIDERAÇÕES FINAIS 35

GLOSSÁRIO 36

APRESENTAÇÃO

O Plano de Gestão de Riscos de Tecnologia da Informação e Comunicação (PGRTIC) marca um avanço essencial na governança de TIC do Poder Judiciário, reforçando o compromisso com segurança, inovação e continuidade dos serviços em um cenário digital em constante transformação. Diante da crescente dependência tecnológica, o Plano estabelece diretrizes para identificar, avaliar e tratar riscos, garantindo a integridade dos dados e a resiliência da infraestrutura. Trata-se de um instrumento estratégico, vivo e adaptável, que visa oferecer uma experiência digital segura e eficiente a magistrados, servidores e cidadãos. Com ele, reafirma-se a missão institucional de promover uma Justiça mais acessível, célere e eficaz.

1. INTRODUÇÃO

O fortalecimento da governança, elencado entre os macrodesafios do Plano Estratégico 2021-2026 do Tribunal de Justiça do Estado do Pará (TJPA), contempla a necessidade de aprimoramento da gestão de riscos operacionais, dos controles internos administrativos e da governança corporativa. O objetivo é assegurar que esses processos sejam conduzidos conforme o planejado, promovendo melhorias contínuas nas operações institucionais sob os pilares da economicidade, da eficiência e do desempenho.

Nesse cenário, a incorporação da perspectiva de riscos é essencial para fundamentar decisões mais racionais, alinhadas à identidade estratégica e aos objetivos do Poder Judiciário Estadual. A gestão de riscos contribui para a criação e preservação de valor, ao mesmo tempo em que fortalece a capacidade da instituição de responder adequadamente a eventos inesperados que possam comprometer suas metas e resultados.

As incertezas, por sua natureza, representam tanto ameaças quanto oportunidades, com potencial de impactar negativamente ou agregar valor às atividades organizacionais. Assim, a principal finalidade da Gestão de Riscos de TIC é garantir a eficiência e a eficácia institucionais, por meio da integração sistemática dos processos de gerenciamento de riscos à estrutura de governança e à cultura organizacional do TJPA.

Nesse contexto, e em consonância com as diretrizes do Manual de Gestão de Riscos do PJPA, o presente Plano de Gestão de Riscos de Tecnologia da Informação e Comunicação (PGRTIC) foi concebido para detalhar a abordagem metodológica, os componentes de gestão (incluindo procedimentos, práticas, responsabilidades, etapas e planos de ação) e os recursos a serem empregados na identificação, análise, avaliação e tratamento dos riscos de TIC. O Plano estabelece critérios objetivos e métricas claras, orientando estratégias de resposta e promovendo a internalização das boas práticas de gestão de riscos no cotidiano das equipes técnicas da Secretaria de Tecnologia da Informação e Comunicação do TJPA.

Por fim, este PGRTIC também se configura como o registro formal da construção e manutenção da estrutura necessária à implementação, ao suporte e à gestão dos riscos de Tecnologia

da Informação e Comunicação no âmbito da Secretaria de Tecnologia da Informação e Comunicação do TJPA. O documento contempla, ainda, a definição clara de:

a) da integração aos demais instrumentos de planejamento estratégico;

b) da estratégia de incorporação do gerenciamento de riscos aos processos organizacionais e projetos, bem como à tomada de decisões;

c) dos critérios para tratamento dos riscos de TIC, em conformidade com o estabelecimento do apetite e da tolerância a riscos;

d) dos ciclos de planejamento, execução, monitoramento e avaliação das decisões sobre os riscos aos processos de TIC;

e) do escopo deste PGRTIC, incluindo-se as limitações e restrições conhecidas; e

f) dos recursos humanos, financeiros e tecnológicos necessários.

1.1. VINCULAÇÃO

A Gestão de Riscos de TIC deve seguir o **MANUAL DE GESTÃO DE RISCOS DO PJPA**, elaborado pela Coordenadoria de Gestão de Processos e Riscos, vinculada ao Departamento de Planejamento, Gestão e Estatística (DPGE), e considerar as diretrizes da **POLÍTICA DE GESTÃO DE RISCOS INSTITUCIONAL** instituída pela Portaria nº 3016/2019-GP, operando em conjunto, fornecendo a estrutura complementar, concentrando-se nas ameaças específicas desse domínio e garantindo uma abordagem abrangente e alinhada à missão da Organização.

1.2. PRINCÍPIOS

Em estrita observância aos princípios estabelecidos na **POLÍTICA DE GESTÃO DE RISCOS DO TJPA**, instituída pela Portaria nº 3016/2019-GP, este PGRTIC complementa conforme o que segue:

I. **Criar e proteger os valores institucionais:** o risco não deve ser gerenciado isoladamente. A Gestão de Riscos de TIC deve estar alinhada à gestão institucional, de maneira a alcançar os objetivos institucionais e aprimorar o seu desempenho;

II. **Integrar os processos organizacionais:** a Gestão de Riscos de TIC é parte das responsabilidades de todos os gestores e deverá integrar todos os processos de trabalho, projetos e planos de ação da Secretaria de Tecnologia da Informação e Comunicação e de suas subunidades;

III. **Fazer parte da tomada de decisões:** para a tomada de decisão, os gestores, com o apoio das unidades técnicas, deverão avaliar consistentemente os riscos que podem impedir ou oportunizar o alcance dos objetivos pretendidos pela Administração, o impacto de cada um deles no negócio e priorizar as ações com base nos planos de resposta ao risco;

IV. **Abordar explicitamente a incerteza:** abordar especificamente o efeito da incerteza nos objetivos estabelecidos pela Administração. O risco só poderá ser avaliado ou tratado com sucesso, se a natureza e a fonte da incerteza forem devidamente compreendidas;

V. **Ser sistemática, estruturada e oportuna:** fazer parte da gestão organizacional, no sentido de contribuir para a eficiência dos processos de trabalho, dos projetos, dos planos de ações e para o alcance de resultados consistentes, confiáveis e comparáveis;

VI. **Basear-se nas melhores informações disponíveis:** para que a tomada de decisão seja baseada em riscos, o processo de Gestão de Riscos de TIC deverá considerar fontes de informações tempestivas e confiáveis, observando dados históricos, experiências, retorno das partes interessadas, observações, previsões, pareceres de especialistas;

VII. **Atender às necessidades organizacionais:** a Gestão de Riscos de TIC deverá alinhar-se aos ambientes interno e externo, ao perfil e ao apetite de risco da Administração e da própria Secretaria de Tecnologia da Informação e Comunicação;

VIII. **Considerar a importância dos fatores humanos e culturais:** o processo de Gestão de Riscos de TIC deverá reconhecer as capacidades, as restrições, as percepções e as intenções de pessoas externas e internas, que podem facilitar o atingimento dos objetivos perseguidos e/ou potencializar seus resultados;

IX. **Ser transparente e inclusivo:** o processo de Gestão de Riscos deverá envolver, de maneira apropriada e oportuna, as partes interessadas e, em particular, os tomadores de decisões em todos os níveis da organização, a fim de assegurar que a Gestão de Riscos de TIC permaneça relevante, atualizada e disponível aos interessados;

X. **Ser dinâmico, iterativo e capaz de reagir a mudanças:** o processo de Gestão de Riscos de TIC deverá ser capaz de perceber continuamente as mudanças internas e externas e respondê-las adequada e tempestivamente;

XI. **Facilitar a melhoria contínua:** desenvolver e implementar estratégias para que a organização permaneça alerta a novas oportunidades de melhoria;

XII. **Fomentar a inovação e a ação empreendedora responsáveis:** promover um ambiente que encoraje a criatividade, o desenvolvimento de soluções inovadoras e a experimentação, ao mesmo tempo em que se mantém a responsabilidade e a consideração pelos riscos associados a essas atividades;

XIII. **Ser dirigido, apoiado e monitorado pela alta administração:** na busca pela efetividade do programa, a Alta Administração do TJPA, por meio de suas unidades de Gestão de Riscos, compromete-se de forma inequívoca pela implementação e acompanhamento do presente PGRTIC. O suporte para a boa consecução do Plano dar-se-á mediante a disponibilização dos recursos materiais e humanos necessários, a adoção de decisões baseadas na legalidade, ética e eficiência dos serviços públicos, bem como na implementação e no monitoramento dos controles propostos.

1.3. OBJETIVOS

Como principais objetivos deste PGRTIC, destacam-se:

a) Apoiar no alcance dos objetivos, através de informações que favoreça o entendimento de oportunidades e ameaças aos negócios de TIC;

b) Assegurar que a Alta Gestão tenha acesso às informações pertinentes aos fatores de risco de TIC aos quais o TJPA pode estar exposto;

c) Estabelecer uma base confiável para o planejamento e para a tomada de decisão;

d) Apoiar as lideranças da Secretaria de Tecnologia da Informação e Comunicação na definição e revisão de seu apetite e tolerância aos riscos, bem como das métricas para sua avaliação em âmbito corporativo e em observância ao Apetite a Risco institucional, declarado na Portaria nº. 483/2024-GP;

e) Apoiar as Unidades de Negócio e de Operações na identificação, na análise, na avaliação, na priorização, no tratamento e no monitoramento de riscos com impacto nos Negócios Jurisdicional e de Tecnologia da Informação;

f) Apoiar as Unidades de Negócio e de Operações na definição e no acompanhamento de planos de ação para tratamento dos riscos de TIC, incluindo socioambientais;

g) Oferecer às lideranças da Secretaria de Tecnologia da Informação e Comunicação uma visão consolidada e holística dos riscos associados ao alcance de objetivos estratégicos e/ou a continuidade dos negócios;

h) Promover a identificação de oportunidades, as quais deverão ser analisadas conforme a metodologia definida;

i) Promover o aproveitamento das oportunidades identificadas como parte integrante do processo de gerenciamento de riscos, por meio de investimentos em sistemas de gestão, capacitação de pessoas e melhorias de processos;

j) Promover identificação de riscos socioambientais e minimizar eventuais impactos de riscos iminentes ou emergentes de médio prazo;

k) Manter atualizados: metodologia, processos e ferramentas associadas ao processo de Gestão de Riscos de TIC; buscando alinhamento constante com boas práticas e tendências.

1.4. ABRANGÊNCIA / APLICABILIDADE

O presente documento tem aplicabilidade em toda a Secretaria de Tecnologia da Informação e Comunicação do TJPA, abrangendo as áreas de planejamento, de gestão, e as áreas operacionais (de infraestrutura, de aplicações, de segurança da informação, e de atendimento a usuários), incluindo empresas terceirizadas e prestadoras de serviços contratados.

Sua abrangência também deve considerar os ativos, os processos de trabalho e de tomada de decisões, os projetos, as ações e as atividades realizados por estas subunidades, sem prejuízo da utilização de outras metodologias e ferramentas complementares específicas.

Dessa forma, o gerenciamento de riscos deve estar incorporado em todos os níveis, quais sejam:

I. **ESTRATÉGICO:** nível em que se dá o contato político da Secretaria de Tecnologia da Informação e Comunicação com a Alta Administração, com outras unidades de negócio, e com a sociedade, estabelecendo-se a coerência da Administração. Decisões neste nível envolvem a formulação dos objetivos estratégicos e as prioridades para a alocação de recursos públicos em alinhamento com as políticas públicas e diretrizes do Poder Judiciário Estadual;

II. **TÁTICO:** nível em que se encontram as decisões de implementação e gerenciamento dos programas temáticos previstos no nível estratégico, mediante os quais são executadas as políticas e as ações organizacionais prioritárias;

III. **OPERACIONAL:** nível em que se encontram os projetos que contribuirão para o atingimento dos objetivos, programas e atividades relativas aos processos finalísticos e de suporte ao Negócio.

Todos os níveis são fundamentais: o estratégico para orientar a visão; o tático para desdobrar essa visão em programas, em projetos e em planos de ação; e o operacional para executá-los.

1.5. VIGÊNCIA E REVISÕES

O período de vigência do presente Plano de Gestão de Riscos de Tecnologia da Informação se alinha diretamente ao Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) da mesma Secretaria de Tecnologia da Informação e Comunicação.

Com a finalidade de, periodicamente, serem reavaliados os riscos no ambiente de TIC, o processo de Gestão de Riscos de TIC deverá ser aplicado no início de cada Gestão, mais especificamente, em até 90 (noventa) dias após a apresentação do PDTIC.

Este Plano poderá ser revisado a qualquer tempo, por iniciativa de qualquer parte que componha a estrutura de Gestão de Riscos de TIC ou sempre que houver algum incidente que justifique uma reavaliação dos riscos, decidindo-se por reavaliar parte ou todo o processo organizacional, bem como executar a metodologia completa ou apenas algumas de suas etapas.

1.6. REFERÊNCIAS NORMATIVAS E AUXILIARES

Este PGRTIC se fundamenta nos seguintes documentos:

a) **Política de Gestão de Riscos do TJPA**, instituída pela Portaria nº 3016/2019-GP, de 05/07/2019, que dispõe sobre a Política de Gestão de Riscos do Poder Judiciário do Estado do Pará, define objetivos, conceitos, princípios, estrutura e responsabilidades, disponível na área da Coordenadoria de Gestão de Processos e Riscos (https://www.tjpa.jus.br/PortalExterno/institucional/Coordenadoria-de-Gestao-de-Processos-e-Riscos/);

b) **Planejamento Estratégico do Poder Judiciário do Estado do Pará**, para o período de 2021-2026, consubstanciado na Resolução TJPA nº 09/2021, na Resolução TJPA nº 2, de 1º de fevereiro de 2023 (Revisada), no Mapa Estratégico e no Glossário de Indicadores do Planejamento Estratégico 2021-2026, encontrados no sítio da internet: (https://www.tjpa.jus.br/PortalExterno/hotsite/planejamento-estrategico/instrumentos.xhtml?idPagina=669281)

c) **Manual de Gestão de Riscos do PJPA**, que detalha o processo de Gestão de Riscos e se apresenta como um instrumento de apoio e orientação para o efetivo gerenciamento de riscos no âmbito de atuação do TJPA, disponível na área da Coordenadoria de Gestão de Processos e Riscos (https://www.tjpa.jus.br/PortalExterno/institucional/Coordenadoria-de-Gestao-de-Processos-e-Riscos/);

d) **Resolução n°. 370, de 28 de janeiro de 2021, do Conselho Nacional de Justiça**, que estabelece a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD);

e) **Resolução n°. 396, de 07 de junho de 2021, do Conselho Nacional de Justiça**, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);

f) **Portaria n°. 162, de 10 de junho de 2021, do Conselho Nacional de Justiça**, que aprova Protocolos e Manuais criados pela Resolução CNJ nº 396/2021, que instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);

g) **Resolução n°. 347, de 13 de outubro de 2020, do Conselho Nacional de Justiça**, que dispõe sobre a Política de Governança das Contratações Públicas no Poder Judiciário;

h) **Lei nº 13.709, de 14 de agosto de 2018** – Lei Geral de Proteção de Dados Pessoais (LGPD);

i) **Norma ABNT NBR ISO 31000:2018**, Gestão de Riscos – Princípios e Diretrizes, com o objetivo de disseminar princípios e diretrizes para gestão de riscos;

j) **Norma ABNT NBR ISSO/IEC 31010:2021**, Gestão de Riscos – Técnicas para o processo de avaliação de riscos;

k) **Norma ABNT NBR ISO/IEC 27005:2019**, Tecnologia da Informação – Técnicas de segurança – Gestão de riscos de segurança da informação;

l) **"Cartilha de Gestão de Riscos" do Conselho Nacional de Justiça**, agosto de 2019, encontrado no sítio da internet: https://bibliotecadigital.cnj.jus.br/jspui/handle/123456789/218;

m) **"Manual de Gestão de Riscos" do Tribunal de Contas da União (TCU)**, encontrado no sítio da internet: https://portal.tcu.gov.br/planejamento-governanca-e-gestao/gestao-de-riscos/manual-de-gestao-de-riscos/;

n) **"Gestão de Riscos: Avaliação da Maturidade" do Tribunal de Contas da União (TCU)**, encontrado no sítio da internet: https://portal.tcu.gov.br/gestao-de-riscos-avaliacao-da-maturidade.htm;

o) **Guia de Gestão de Riscos do Conselho da Justiça Federal**, encontrado no sítio da internet: https://www.cjf.jus.br/cjf/unidades/estrategia-e-governanca/gestao-de-riscos;

2. DIAGNÓSTICO DO AMBIENTE

2.1. VISÃO GERAL

A Secretaria de Tecnologia da Informação e Comunicação do TJPA, criada pela Lei 6.850/2006 de 02/05/2006 e reestruturada pela Lei nº 10.852, de 31 de janeiro de 2025 tem por missão prover soluções de tecnologia da informação efetivas e eficazes para que o Poder Judiciário do Estado do Pará cumpra sua função institucional.

Neste sentido, é responsável por conduzir o planejamento e a execução das ações relacionadas à aplicação da Tecnologia da Informação e Comunicação (TIC), seguindo as diretrizes e metas de trabalho definidas no Planejamento Estratégico Institucional do Poder Judiciário do Estado do Pará. Buscando ser reconhecida pela qualidade de seus serviços, deve nortear suas ações em valores éticos, buscando qualidade e eficiência com segurança e responsabilidade socioambiental.

As diretrizes de trabalho são definidas pela Presidência do Tribunal, que por meio da Comissão Permanente de Informática, coordena as direções da Secretaria, mantendo o alinhamento estratégico com o Planejamento Estratégico e a Presidência do TJPA.

Fazem parte de estrutura organizacional da Secretaria de Tecnologia da Informação e Comunicação:

a. **COORDENADORIA DE APLICAÇÕES (CA):** esta unidade tem como missão o desenvolvimento e a manutenção das ferramentas de software que apoiam a prestação jurisdicional, seja na atividade fim, seja na atividade meio (administrativa) do PJPA;

b. **COORDENADORIA DE ATENDIMENTO AO USUÁRIO (CAU):** sua missão é coordenar, gerenciar, planejar e administrar todas as atividades relativas ao atendimento ao usuário final dos serviços de informática, bem como a manutenção de equipamentos do TJPA;

c. **COORDENADORIA DE INFRAESTRUTURA TECNOLÓGICA (CIT):** a missão desta unidade é prover a infraestrutura de recursos tecnológicos de informática e telecomunicações exigidos para garantir a prestação dos serviços com qualidade e segurança.

d. **COORDENADORIA DE GOVERNANÇA (CGOV):** sua missão é assegurar boa governança interna: apoio à gestão de projetos estratégicos, mapeamento e monitoramento de processos, implementação de compliance e transparência institucional.

Fazem parte de estrutura de governança de TIC:

a) **COMISSÃO PERMANENTE DE INFORMÁTICA:** de caráter estratégico e deliberativo, é composta por representantes da instituição, sendo presidida por um Desembargador. Os membros foram designados por meio da Portaria nº 1570/2025-GP. Tem por finalidade apreciar toda a matéria relativa aos métodos e técnicas de computação de dados no âmbito

do Poder Judiciário Estadual. Esta Comissão segue as diretrizes do Regimento Interno do Tribunal de Justiça do Estado do Pará;

b) **COMITÊ DE GOVERNANÇA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO (CGOVTIC):** de caráter estratégico, deliberativo e multidisciplinar, instituído pela Portaria 2299/2025-GP, é composto por representantes da instituição e tem por finalidade deliberar sobre políticas, diretrizes e planos relativos à TIC e à Governança Digital. Esse comitê segue as diretrizes da Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD 2021-2026);

c) **COMITÊ DE GESTÃO DE TECNOLOGIA DA INFORMAÇÃO (CGESTIC):** instituído pela Portaria 2309/2025-GP, tem como objetivos: a elaboração de planos táticos e operacionais, o acompanhamento de suas respectivas execuções, a análise das demandas de TIC, o estabelecimento de indicadores operacionais e a proposição de replanejamento das ações relativas à TIC. Esse comitê segue as diretrizes da Estratégia Nacional de TIC do Poder Judiciário (ENTIC-JUD 2021-2026);

d) **COMITÊ DE GOVERNANÇA DE SEGURANÇA DA INFORMAÇÃO (CGSI):** instituído pela Portaria 1093/2025-GP, visa promover a cultura de Segurança da Informação, bem como para estabelecer um Modelo de Gestão que permita a criação e a manutenção de um Sistema de Gestão de Segurança da Informação apoiado por uma política de segurança, normas e procedimentos. Esse comitê segue as diretrizes da Estratégia Nacional de TIC do Poder Judiciário (ENTIC-JUD 2021-2026).

2.2. CONTEXTUALIZAÇÃO

Abordar o diagnóstico do Processo de Gerenciamento de Riscos de TIC, de forma abrangente, é uma tarefa crucial para garantir a eficiência e a segurança das operações. Nesse cenário, evidenciou-se a necessidade de enfrentamento de desafios significativos.

Primeiramente, embora as práticas de gestão de riscos de TIC tenham sido instituídas desde 2019, a aplicabilidade atual dessas práticas se concentra majoritariamente no escopo de gestão de contratações. Expandir as boas práticas do gerenciamento de riscos para as demais áreas da Secretaria de Tecnologia da Informação e Comunicação e promover revisões com uma periodicidade mais curta – de modo geral, estas revisões ocorrem anualmente ou a cada mudança de gestão (biênio) – são iniciativas fundamentais para assegurar uma visão holística e integrada dos riscos em todas as áreas da TIC. Esta abordagem permitirá a atualização e adequação contínua das práticas existentes às novas ameaças e vulnerabilidades emergentes no ambiente tecnológico.

Ademais, também foi constatada a necessidade de uma estrutura mais formal e robusta para identificar, analisar, avaliar e tratar adequadamente os riscos associados à tecnologia da informação e comunicação. A consistência, a proatividade e a maior padronização nos processos de gerenciamento de riscos de TIC podem ser aprimoradas para permitir a implementação de medidas preventivas que atenuem ou mitiguem potenciais ameaças antes que venham a se materializar, fortalecendo a segurança e a resiliência das operações.

Outro aspecto observado é a maturidade em gerenciamento de processos de trabalho. Apesar da existência de processos mapeados, alguns ainda apresentam lacunas que precisam ser

resolvidas para melhorar a eficiência e a capacidade de resposta da Secretaria de Tecnologia da Informação e Comunicação a incidentes e mudanças no ambiente de TIC. Processos bem definidos e documentados são essenciais para a gestão eficaz das atividades.

Adicionalmente, a formalização na atribuição de papéis e responsabilidades é um fator que pode ser aprimorado para aumentar a eficácia na gestão de riscos. A clareza sobre quem é responsável por identificar, avaliar e tratar os riscos de TIC é fundamental para uma governança eficiente, assegurando responsabilidade e prestação de contas.

Apesar dos desafios supramencionados, há aspectos positivos a serem destacados. A Secretaria demonstra um compromisso contínuo com o desenvolvimento profissional de seus servidores, investindo ativamente em treinamentos e capacitações, inclusive nos temas afetos ao gerenciamento de riscos e de controles internos, contribuindo para o aprimoramento geral das competências técnicas e de gestão.

Além disso, a Secretaria de Tecnologia da Informação e Comunicação apresenta um grau avançado de maturidade em monitoramento de infraestrutura e aplicações**.** Essa capacidade permite a detecção proativa de anomalias e a resposta ágil a incidentes operacionais, contribuindo para a redução do tempo de indisponibilidade e o aumento da resiliência dos sistemas de TIC.

Em conclusão, este diagnóstico revela uma série de desafios que precisam ser enfrentados para fortalecer a gestão de riscos de TIC na Secretaria, ao mesmo tempo em que reconhece os investimentos e avanços em áreas complementares que podem servir de base para futuras melhorias. A implementação de uma estrutura robusta e a capacitação específica em gestão de riscos são passos essenciais para elevar a maturidade da organização e garantir uma abordagem proativa na mitigação de riscos, alinhada às melhores práticas de governança de TIC.

3. ESTRUTURA DE GESTÃO DE RISCOS DE TIC

3.1. ESTRUTURA

Conforme orientações contidas na Norma ABNT NBR ISO 31000:2018 e no Manual de Gestão de Riscos do TJPA, o gerenciamento de riscos deve ser precedido da definição de uma estrutura de suporte que envolve basicamente:

a) entendimento da organização e seu contexto;

b) definição de política interna;

c) atribuição de responsabilidades;

d) integração nos processos organizacionais;

e) alocação de recursos necessários (pessoas, processos, tecnologia da informação);

f) estabelecimento de meios de divulgação do conhecimento gerado e de comunicação com partes envolvidas e interessadas.

Deste modo, em estrita aderência à abordagem em três linhas de gestão (ou defesa) definida no **MANUAL DE GESTÃO DE RISCOS DO PJPA**, elaborado pela Coordenadoria de Gestão de Processos e Riscos, vinculado ao Departamento de Planejamento, Gestão e Estatística (DPGE), a estrutura de governança da Gestão de Riscos de TIC fica composta da seguinte forma:

a) **PRIMEIRA LINHA:** de natureza operacional, deverá ser exercida pelos Núcleos de Gestão de Riscos de cada Coordenadoria (NGR), compreendidos pelos gestores e servidores responsáveis pelos processos afetos a cada uma das unidades administrativas da Secretaria de Tecnologia da Informação e Comunicação (SETIC);

b) **SEGUNDA LINHA:** de natureza tática, deverá ser exercida pelo Grupo Estratégico de Governança de TIC (GEGTIC), pela Comissão Permanente de Informática, pelo Comitê de Gestão da Área de TIC (CGesTIC/PJPA), pelo Comitê de Governança de TIC (CGovTIC/PJPA) e pelo Comitê de Governança da Segurança da Informação (CGSI/PJPA);

c) **TERCEIRA LINHA:** de natureza fiscalizatória, deverá ser exercida pela unidade de auditoria interna, mais precisamente pelo Núcleo Estratégico de Governança de Auditoria e Risco da Secretaria de Auditoria Interna (SEAUD), responsável pela avaliação independente das ações de gestão de riscos da SETIC.

Mais detalhadamente, a estrutura de governança do gerenciamento de riscos da Secretaria de Tecnologia da Informação e Comunicação será constituída pelas seguintes instâncias:

A Comissão Permanente de Informática e os Comitês de Gestão de TIC (CGesTIC/PJPA), de Governança de TIC (CGovTIC/PJPA) e de Governança da Segurança da Informação (CGSI/PJPA) são as instâncias deliberativas do plano e do processo de Gestão de Riscos de TIC.

O **Grupo Estratégico de Governança de TIC (GEGTIC) da Secretaria de Tecnologia da Informação e Comunicação**, será composto pelos respectivos Coordenadores de cada subunidade e, eventualmente, por servidores por estes designados, em quantitativo necessário para resguardar o cumprimento regular de suas competências. É a instância de coordenação e supervisão do processo de Gestão de Riscos de TIC. Tem o papel de coordenar as atividades de Gestão de Riscos, monitorar riscos específicos (regulatórios/*compliance*), ajudar a desenvolver controles e monitorar riscos e controles, garantir que a primeira linha funcione conforme pretendido.

A **Secretaria de Auditoria Interna (SEAUD)** é a unidade responsável pela avaliação contínua do processo de gestão de riscos e pelo monitoramento contínuo da eficácia e da eficiência dos controles internos aplicados para mitigar riscos.

Figura 1 – Estrutura de governança do gerenciamento de riscos de TIC.

3.2. COMPETÊNCIAS E RESPONSABILIDADES

Compete à **Comissão Permanente de Informática**, ao **Comitê de Governança de TIC (CGovTIC/PJPA)**, ao **Comitê de Gestão da Área de TIC (CGesTIC/TJPA)** e ao **Comitê de Governança de Segurança da Informação (CGSI/TJPA)**, conjunta ou isoladamente com relação à Gestão de Riscos de TIC, no âmbito de suas atribuições:

a) Promover a revisão periódica e a atualização do Plano de Gestão de Riscos de TIC;

b) Avaliar a adequação, a suficiência e a eficácia da estrutura de Gestão de Riscos de TIC;

c) Operacionalizar, no âmbito das unidades da Secretaria de Tecnologia da Informação e Comunicação, a aplicação dos recursos disponibilizados para a Gestão de Riscos de TIC;

d) Garantir o apoio institucional para promover a gestão de riscos e controles internos, em especial os seus recursos e o relacionamento entre as partes interessadas;

e) Deliberar sobre a Política de Gestão de Riscos de TIC (se houver) e o Plano de Gestão de Riscos de TIC, os níveis de apetite e tolerância a riscos, bem como avaliar seu desempenho;

f) Aprovar os ativos, processos de trabalho, projetos e ações que terão os riscos gerenciados com prioridade;

g) Aprovar o relatório de análise crítica, o mapa de riscos de TIC e os plano de resposta/tratamento aos riscos mapeados;

h) Deliberar sobre os riscos considerados extremos e os riscos residuais considerados altos, que lhe forem submetidos;

i) Deliberar sobre os riscos considerados médios e altos que, eventualmente, lhes forem apresentados pelos proprietários de risco;

j) 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;

k) Decidir a respeito da solução mais adequada quando o risco for avaliado em nível superior à tolerância estabelecida e o custo para reduzi-lo ou eliminá-lo for desproporcional aos benefícios a serem obtidos;

l) Deliberar acerca de eventuais casos omissos e excepcionalidades;

Compete ao **Grupo Estratégico de Governança de TIC (GEGTIC) da Secretaria de Tecnologia da Informação e Comunicação**, com relação à gestão de riscos de TIC:

a) Coordenar o processo e acompanhar a execução das atividades relacionadas ao gerenciamento de riscos de TIC;

b) Acompanhar a execução dos planos de ação para implementação da Gestão de Riscos de TIC e zelar pela sua adequada comunicação;

c) Apoiar os Núcleos de Gestão de Riscos no processo de gerenciamento dos riscos de TIC, com base na metodologia estabelecida;

d) Acompanhar e consolidar as informações pertinentes à Gestão de Riscos de TIC;

e) Revisar os relatórios de análise crítica e o mapa de riscos de TIC;

f) Revisar e monitorar os planos de respostas a riscos relacionados à estratégia;

g) Estabelecer controles proporcionais aos riscos mapeados, considerando suas causas, suas consequências e a relação custo-benefício;

h) Aperfeiçoar o processo de decisão baseado em riscos;

i) Atender às requisições da Comissão de Informática e dos Comitês de Governança de TIC (CGovTIC), de Gestão da Área de TIC (CGesTIC), e de Governança da Segurança da Informação (CGSI);

j) Subsidiar a Secretaria de Tecnologia da Informação e Comunicação, a Comissão Permanente de Informática e os Comitês de Governança de TIC (CGovTIC), de Gestão da Área de TIC (CGesTIC), e de Governança da Segurança da Informação (CGSI) com informações técnicas, visando auxiliá-los no processo de tomada de decisão;

k) Dar conhecimento às instâncias pertinentes quando o risco for avaliado em nível superior à tolerância estabelecida e o custo para reduzi-lo ou eliminá-lo seja desproporcional aos benefícios a serem obtidos;

l) Avaliar e divulgar as melhores práticas de gestão de riscos para utilização no âmbito da Secretaria de Tecnologia da Informação e Comunicação;

m) Validar o estabelecimento de metodologias específicas de gestão de riscos, quando exigidas por Órgãos Superiores ou decorrentes de especificidades técnicas;

n) Elaborar e manter atualizado o Manual de Gestão de Riscos de TIC do TJPA (se houver);

o) Zelar pelo estrito cumprimento da Política de Gestão de Riscos do TJPA (se houver);

p) Fomentar a cultura de gestão de riscos e propor ações de sensibilização e capacitação;

Compete aos servidores **responsáveis pelo gerenciamento dos riscos de TIC** dos processos organizacionais da Secretaria de Tecnologia da Informação e Comunicação:

a) Identificar, analisar e avaliar os riscos dos processos sob sua responsabilidade, em conformidade com o define este PGRTIC;

b) Propor respostas tempestivas e respectivas medidas de controle a serem implementadas nos processos organizacionais sob sua responsabilidade;

c) Monitorar a evolução dos níveis de risco e a efetividade das medidas de controle implementadas nos processos organizacionais sob sua responsabilidade;

d) Informar ao Núcleo de Gestão de Riscos correspondente sobre mudanças significativas nos processos organizacionais sob sua responsabilidade e nos níveis de risco a eles vinculados;

e) Responder às requisições do Núcleo de Gestão de Riscos associado;

f) Disponibilizar informações adequadas quanto à gestão dos riscos dos processos sob sua responsabilidade à Secretaria de Tecnologia da Informação e Comunicação e demais partes interessadas;

g) Notificar seus superiores hierárquicos sempre que identificar eventuais riscos não mapeados em processos organizacionais fora de sua responsabilidade; e

h) Participar da elaboração do Plano de Gerenciamento dos Riscos de TIC.

Os responsáveis pelo Gerenciamento de Riscos dos processos organizacionais da Secretaria de Tecnologia da Informação e Comunicação devem ter competência suficiente para orientar e acompanhar as etapas de identificação, análise, avaliação e implementação das respostas aos riscos de TIC.

Compete a **Secretaria de Auditoria Interna (SEAUD)**:

a) Auditar os processos de gerenciamento de riscos e os controles implementados pelas unidades organizacionais do TJPA;

b) Realizar auditorias internas baseadas em riscos;

c) Disponibilizar à Secretaria de Tecnologia da Informação e Comunicação, mais especificamente ao GEGTIC, as ferramentas e técnicas utilizadas pela auditoria interna para analisar riscos e controles administrativos na área de TI;

d) Prover aconselhamento, facilitar grupos de discussão, orientar os proprietários de risco sobre riscos e controles administrativos, bem como promover o desenvolvimento de uma linguagem, estrutura e entendimento comuns.

Compete a **todos os servidores da Secretaria de Tecnologia da Informação e Comunicação**:

- Monitorar a evolução dos níveis de risco e da efetividade das medidas de controle implementadas nos processos organizacionais em que estiverem envolvidos ou que tiverem conhecimento. Neste monitoramento, caso sejam identificadas mudanças ou fragilidades nos processos organizacionais, o servidor deverá reportar imediatamente o fato ao responsável pelo gerenciamento de riscos do processo em questão e ao Núcleo de Gestão de Riscos correspondente.

Para que gerenciamento de riscos ocorra adequadamente, é imprescindível que cada ator esteja consciente do papel que desempenha. Dessa forma, foi adotada a matriz RACI, conforme indicada a seguir, a fim de auxiliar na definição das responsabilidades dos envolvidos nesse processo:

I. **Responsável (R):** quem executa a atividade;

II. **Autoridade/Aprovador (A):** quem aprova a tarefa, podendo delegar a função desde que mantida a responsabilidade;

III. **Consultado (C):** quem pode agregar valor ou é essencial para a implementação;

IV. **Informado (I):** quem deve ser notificado de resultados ou ações tomadas, embora não necessite tomar parte da decisão.

Tabela 1 – Matriz RACI

#	ATIVIDADE	COORDENADORIAS	GEGTIC	COMISSÃO /COMITÊS	SEAUD
		1ª. LINHA	2ª. LINHA		3ª. LINHA
1.	Definir Plano de Gestão de Riscos	C / I	R	A	C / I
2.	Treinar e capacitar equipes internas	R	R	A	I
3.	Designar membros para o GEGTIC	I	- - - -	A	I
4.	Sensibilizar equipes internas	R	R	I	I
5.	Mapear os processos organizacionais de TIC	R	A	I	I
6.	Definir o escopo da avaliação de riscos de TIC	R	R	A	I
7.	Analisar o Contexto e identificar ativos de TIC	R	R	A	I

8.	Realizar a identificação e análise dos riscos	R	C	A	I
9.	Realizar a avaliação dos riscos de TIC	R	R	A	I
10.	Realizar a priorização dos riscos de TIC	C	R	A	I
11.	Desenvolver estratégias de tratamento	C	R	A	I
12.	Definir a(s) resposta(s) aos riscos mapeados	R	C	A	C / I
13.	Validar os riscos mapeados	I	R	A	I
14.	Implementar controles e medidas de mitigação	R	R	A	I
15.	Monitorar e revisar continuamente os riscos	R	R	A	C
16.	Realizar análise de conformidade	I	R	I	R
17.	Produzir relatório de análise e avaliação de riscos	C	R	I	I
18.	Aprovar relatório de análise e avaliação de riscos	I	I	A	C / I
19.	Comunicar as pastes interessadas	R	R	I	I
20.	Monitorar o processo de Gestão de Riscos de TIC	R	R	I	I
21.	Avaliar o processo de gerenciamento de riscos	I	R	C	R

3.3. INTEGRAÇÃO AOS PROCESSOS ORGANIZACIONAIS

De forma a possibilitar a integração da Gestão de Riscos à Gestão de Processos se faz necessário compreender de forma ampla e detalhada tanto o processo de Gerenciamento de Processos como o processo de Gerenciamento de Riscos de TIC. Por esse motivo, ambos os processos supramencionados devem ser trabalhados como pilotos da metodologia de Gestão de Processos da Secretaria de Tecnologia da Informação e Comunicação, priorizando-se o processo de gerenciamento de processos organizacionais.

Primeiramente, o gerenciamento de processos estabelece uma compreensão clara e sistemática dos fluxos de trabalho e das operações essenciais da Secretaria de Tecnologia da Informação e Comunicação. Esta compreensão detalhada é crucial para identificar, mapear e otimizar processos críticos, garantindo que as atividades sejam realizadas de maneira eficiente e com menor desperdício de recursos. Sem uma base sólida de processos bem gerenciados, as tentativas de gerenciamento de riscos podem ser fragmentadas e menos eficazes, pois a falta de clareza nos processos subjacentes pode obscurecer potenciais riscos e dificultar a implementação de medidas preventivas ou corretivas.

Além disso, o gerenciamento de processos promove uma cultura de melhoria contínua e padronização, o que é essencial para a adaptação e resposta eficaz a mudanças e desafios. Com processos bem definidos e otimizados, a Secretaria está mais bem equipada para incorporar práticas de gerenciamento de riscos de maneira integrada e menos disruptiva. A priorização do gerenciamento de processos também facilita a criação de métricas e indicadores de desempenho, que são vitais para o monitoramento e avaliação contínua dos riscos.

Por último, ao estabelecer o gerenciamento de processos organizacionais como prioridade, a Secretaria de Tecnologia da Informação e Comunicação assegura que os fundamentos operacionais estejam robustos e bem alinhados com os objetivos estratégicos institucionais. Isso cria um ambiente propício para a implantação subsequente de um sistema de gerenciamento de riscos mais eficaz, que poderá se apoiar em processos já otimizados e bem documentados.

De forma geral, espera-se que esse trabalho traga melhorias substanciais para ambos os processos, cabendo destacar as seguintes:

a) Melhor entendimento das etapas e dos fluxos dos processos;

b) Melhor entendimento do papel dos atores nos processos;

c) Otimização das etapas dos processos e consequente dimensionamento do custo operacional e temporal;

d) Automação de partes dos processos;

e) Visão mais holística das operações de TIC, permitindo a identificação, a análise, a avaliação e o tratamento de riscos de maneira mais abrangente;

f) Promove da cultura de Gestão de Riscos, tornando-a parte intrínseca dos processos organizacionais, contribuindo para a segurança e a qualidade contínua das operações.

A opção pela integração de ambos os processos busca a otimização do custo operacional geral, a derrubada de resistências internas e uma redução significativa no impacto para as áreas executoras dos processos organizacionais.

Por se tratar de processos transversais a todas as áreas de TIC e que atuam em outros processos organizacionais, ambos resultarão em um mesmo “produto final”: Planos de Ação; ainda que com focos distintos: melhoria do processo e tratamento de riscos, respectivamente.

A estratégia adotada para a seleção dos processos deve ser elaborada Grupo Estratégico de Governança de TIC (GEGTIC), baseando-se em critérios pré-estabelecidos, e posteriormente validados pelo Comitê de Governança de TIC (CGovTIC). Destaca-se que um dos critérios a serem utilizados deve ser a percepção de riscos pelos membros da Secretaria de Tecnologia da Informação e Comunicação.

Entende-se que essa estratégia deva ser adotada até que todos os processos de TIC tenham sido efetivamente postos em gerenciamento, com previsão para conclusão até dezembro/2026. Neste momento o GEGTIC deverá adotar critérios de priorização próprios para a seleção dos processos anualmente. Essa metodologia deverá ser atualizada na ocasião de forma a incluir tais critérios.

3.4. RECURSOS

Conforme definido na Política de Gestão de Riscos dos TJPA, faz-se necessário que a organização aloque recursos apropriados para a gestão de riscos de TIC. Tais recursos podem ser pessoas, processos, tecnologia da informação, comunicação e treinamento.

PESSOAS:

Servidores responsáveis pelo processo de gestão de riscos aos níveis estratégico, tático e operacional; por reconhecer a existência de riscos em suas atividades; por aplicar os controles internos para mitigação de riscos; pela avaliação contínua do processo de gestão de riscos e pelo monitoramento contínuo da eficácia e da eficiência dos controles internos.

PROCESSOS:

O Plano de Gestão de Riscos de TIC representa o principal recurso no que tange à estruturação do processo de Gestão de Riscos de TIC no TJPA, com a definição de uma metodologia comum e alinhada ao Manual de Gestão de Riscos institucional, mas também reconhecendo as capacidades e restrições da Secretaria de Tecnologia da Informação e Comunicação.

O objetivo é padronizar a linguagem de gerenciamento de riscos na organização e facilitar o levantamento e tratamento de riscos que impactam nos macroprocessos e nos processos de gestão.

A compreensão das capacidades e restrições do ambiente de TIC é crucial para a implementação eficaz do plano, garantindo que os riscos sejam gerenciados de maneira proativa e alinhada com os objetivos estratégicos do TJPA.

TECNOLOGIA DA INFORMAÇÃO:

A Gestão de Riscos de TIC deve ter suporte do recurso de tecnologia da informação e comunicação, principalmente no que tange ao registro de eventos, no processo de avaliação, de classificação e de monitoramento de riscos, assim como no acompanhamento das estratégias de tratamento. A plataforma abaixo faz parte dos recursos de TIC que apoiam a Gestão de Riscos institucional:

> **PLATAFORMA DE COLABORAÇÃO MICROSOFT:** utilizado por todos os magistrados e servidores da Justiça Estadual do Estado do Pará, por meio de suas ferramentas multifuncionais de escritório, correio eletrônico, agenda, formulários eletrônicos, sendo utilizada como apoio aos processos de Gestão de Processos e de Riscos de TIC.

COMUNICAÇÃO:

Todas as etapas do levantamento, análise, avaliação e tratamento de riscos de TIC devem incluir a constante e irrestrita comunicação com as partes interessadas, com o objetivo principal de legitimar o conhecimento sobre riscos e dar transparência às ações desenvolvidas. Dentre as atividades de comunicação que serão desenvolvidas no processo de Gestão de Riscos de TIC, pode-se enumerar:

a) **REGISTRO DAS ETAPAS DO PROCESSO DE GERENCIAMENTO DE RISCOS DE TIC:** as etapas do processo de gerenciamento de riscos (desde a definição do escopo, a identificação de eventos, a análise e avaliação e, por fim, a estratégia de tratamento dos riscos) deverão ser construídas em conjunto com partes interessadas, e para isso será necessário definir

o que, por que, para quem, quando, onde e como estas partes serão comunicadas e consultadas, executando de forma automatizada o processo de Gestão de Riscos de TIC.

b) **REGISTROS DE EVENTOS DE RISCO DE TIC:** o monitoramento contínuo e a análise crítica acerca do processo de Gerenciamento de Riscos de TIC devem se valer de um registro fiel dos eventos de riscos que venham a ocorrer, haja vista o controle da ocorrência dos eventos se constituir em ferramenta primária para a avaliação da eficácia dos controles internos aplicados e para a definição da necessidade de se revisar planos de tratamento ou mesmo identificar novos riscos que estejam atingindo os objetivos organizacionais;

c) **RELATÓRIOS GERENCIAIS DE RISCO DE TIC:** os riscos devem ser monitorados continuamente no intuito de servir como fonte de informações para o processo de tomada de decisão, o que poderá ser materializado pela emissão de relatórios gerenciais acerca da ocorrência de riscos e seus impactos na organização, além da prestação de contas dos gestores de riscos acerca das providências adotadas para mitigar os riscos de TIC já identificados e tratados.

TREINAMENTO:

A Secretaria de Tecnologia da Informação e Comunicação, por meio do Grupo Estratégico de Governança de TIC (GEGTIC) e demais estruturas de apoio, deverá prover a sensibilização dos gestores de riscos e ações de treinamento aos interessados e envolvidos com a Gestão de Riscos de TIC, objetivando desenvolver competências técnicas necessárias.

Os treinamentos poderão ser ministrados presencialmente ou à distância (EaD), utilizando os ambientes e tecnologias existentes no TJPA.

OUTROS RECURSOS:

Além dos recursos citados, este PGRTIC enumera outros que poderão ser utilizados:

a) Técnicas e ferramentas de mapeamento e de orquestração de processos;

b) Sistemas acessórios de gestão, de controle orçamentário e financeiro, de auditoria e monitoramento operacional e de inteligência de negócio;

c) Bases de conhecimento de gestão de riscos de organizações públicas com nível de maturidade em gestão de riscos mais avançado (e.g. Tribunal de Contas da União – TCU);

d) Parcerias estratégicas com outras instituições do judiciário, agências governamentais ou entidades privadas para compartilhar informações de segurança, melhores práticas e recursos de gestão de riscos de TIC;

e) Programas de conscientização para educar todos os servidores e demais colaboradores sobre as melhores práticas no uso adequado e responsável de recurso de tecnologia da informação e comunicação, incluindo questões de segurança cibernética, proteção de dados, privacidade, uso ético de recursos digitais e conformidade com políticas internas e regulamentações externas.

3.5. CAPACITAÇÃO

A crescente dependência da Tecnologia da Informação e Comunicação (TIC) em órgãos públicos do judiciário trouxe consigo a necessidade de desenvolver e implementar estratégias sólidas para a gestão de riscos nesse ambiente. A elaboração de um Plano de Gestão de Riscos de TIC é crucial para garantir a segurança, a confiabilidade e a eficiência dos processos judiciais e administrativos.

No entanto, o sucesso desse plano depende, em grande parte, do treinamento e da capacitação adequados dos servidores, sendo pilares fundamentais na mitigação proativa de riscos, na salvaguarda dos valiosos ativos de TIC e na preservação intransigente da confiança do público.

Conforme estabelecido na **POLÍTICA DE GESTÃO DE RISCOS DO TJPA**, instituída pela Portaria nº 3016/2019-GP, a capacitação de gestores, e demais colaboradores em gerenciamento de riscos, é um dos pressupostos para a implantação da cultura de gestão de riscos em uma organização.

Portanto, investir assertivamente em programas de treinamento emerge como um passo imperativo e inadiável na salvaguarda da integridade, segurança e eficiência dos sistemas de TIC do judiciário paraense. Torna-se crucial estabelecer e implementar um plano de capacitação abrangente, que inclua desde treinamentos técnicos específicos até a conscientização sobre boas práticas de governança, gerenciamento de riscos e de segurança cibernética.

Além disso, a capacitação não deve ser vista como um evento isolado, mas como um processo contínuo e integrado à cultura organizacional. Isso inclui a realização de simulações de incidentes, de exercícios de identificação e de resposta a crises, a disseminação constante das melhores práticas de uso de sistemas/dados e de segurança da informação, conformidade com regulamentações de segurança e procedimentos de emergência.

A eficácia deste plano depende diretamente da expertise e do preparo dos servidores, que se tornam a primeira linha de defesa contra potenciais ameaças e vulnerabilidades. Esta abordagem proativa não apenas fortalecerá a resiliência do TJPA frente a ameaças digitais em constante evolução, mas também promoverá uma cultura organizacional que valoriza a segurança da informação como pilar fundamental do serviço público.

4. PROCESSO DE GESTÃO DE RISCOS DE TIC

4.1. METODOLOGIA

A Gestão de Riscos de TIC deve seguir a metodologia de Gerenciamento de Riscos deste Tribunal de Justiça Estadual, conforme estabelecido no **MANUAL DE GESTÃO DE RISCO DO PJPA,** elaborado pela Coordenadoria de Gestão de Processos e Riscos, vinculada ao Departamento de Planejamento, Gestão e Estatística (DPGE).

O plano supramencionado se baseia nas diretrizes definidas pela norma ABNT NBR ISO 31000:2018 e 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.

O processo de Gestão de Riscos de TIC será coordenado pelo Grupo Estratégico de Governança de TIC (GEGTIC), tendo na sua execução a participação das Coordenadorias da Secretaria de Tecnologia da Informação e Comunicação e por meio da Comissão Permanente de Informática, do Comitê Gestor de TIC (CGESTIC), do Comitê de Governança da Segurança da Informação (CGSI) e do Comitê de Governança de TIC (CGOVTIC).

4.2. ESCOPO

O escopo do presente PGRTIC inclui a identificação, a avaliação, a priorização, o tratamento e o monitoramento dos riscos associados às atividades operacionais, táticas e estratégicas da Secretaria de Tecnologia da Informação e Comunicação, bem como aos projetos, às iniciativas estratégicas, aos ativos de TI e aos processos de contratação de soluções de TIC.

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

I. **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;

II. **RISCOS DE INFRAESTRUTURA DE TIC:** riscos identificados e analisados no escopo dos potenciais problemas e ameaças relacionados à infraestrutura tecnológica utilizada pelo Tribunal. Esses riscos envolvem questões como falhas de hardware, indisponibilidade de servidores, interrupções de rede e outros eventos que possam impactar a disponibilidade e o desempenho dos sistemas e serviços de TIC. Os responsáveis pela gestão da infraestrutura de TIC serão os principais envolvidos na identificação, análise, tratamento e monitoramento desses riscos, visando assegurar a estabilidade e a eficiência dos recursos tecnológicos essenciais para o funcionamento do TJPA;

III. **RISCOS DE SEGURANÇA DA INFORMAÇÃO:** riscos identificados e analisados no escopo de segurança da informação ou normas relacionadas, considerando-se principalmente os sistemas e serviços críticos de TIC para o Tribunal e aqueles identificados no Plano de Gestão de Continuidade de Negócios 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 seu tratamento;

IV. **RISCOS DE CONFORMIDADE/COMPLIANCE:** abrange os riscos relacionados ao não cumprimento de normas, regulamentações e políticas aplicáveis à tecnologia da informação e comunicação no contexto do TJPA. Isso inclui o risco de não conformidade com leis, regulamentos, padrões de segurança, políticas internas e requisitos contratuais relevantes para as operações de TIC. A identificação e análise desses riscos visam garantir que a Secretaria de Tecnologia da Informação e Comunicação esteja em conformidade com os requisitos legais e regulamentares, bem como com as melhores práticas de governança e segurança de TIC. Os responsáveis pela conformidade e compliance serão designados para monitorar e mitigar esses riscos, garantindo a aderência contínua às obrigações legais e o cumprimento dos padrões estabelecidos para as atividades de TIC do Tribunal;

V. **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 à pertinência em ser mantidos 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 etapa de homologação do processo/certame, enquanto o gestor do contrato é responsável por gerenciar os riscos inerentes à execução do contrato;

VI. **RISCOS EM PROJETOS DE TIC:** são gerenciados no âmbito de cada projeto de TIC, devendo ser identificados e monitorados pelo responsável direto ou líder de projeto;

VII. **RISCOS EM PROCESSOS DE TIC:** riscos identificados nos processos mapeados e/ou instituídos pela Secretaria de Tecnologia da Informação e Comunicação do TJPA. Os riscos em processos de TIC são monitorados pelos donos do processo ou, na falta deste, pelo Gestor Principal da área responsável.

Novos pilares poderão ser incluídos no plano sempre que uma necessidade for identificada.

Este PGRTIC deverá ser implementado em todos os níveis da Secretaria de Tecnologia da Informação e Comunicação do TJPA, de forma gradual, em prazo e extensão a serem definidos pelo **Grupo Estratégico de Governança de TIC (GEGTIC)** da própria SETIC – seguindo o cronograma proposto neste PGRTIC – que também realizará o acompanhamento da execução do processo de gestão de Riscos de TIC. Os procedimentos operacionais e a dinâmica do acompanhamento serão divulgados em documento específico.

As ações definidas neste Plano terão a sua execução acompanhada pela Comissão Permanente de Informática e pelos comitês CGESTIC, CGSI e CGOVTIC, bem como qualquer deliberação que seja necessária daquele fórum, considerando as suas atribuições e responsabilidades, definidas na **POLÍTICA DE GESTÃO DE RISCOS DO TJPA**, instituída pela Portaria nº 3016/2019-GP.

A gestão de riscos deverá estar integrada aos processos de planejamento estratégico, à gestão, à operação e à cultura organizacional da Secretaria de Tecnologia da Informação e Comunicação.

4.3. HIERARQUIA DE RISCOS

O direcionamento para o gerenciamento de riscos é dado pela Alta Gestão, mas deve ser gerenciado em três níveis de forma integrada, observando:

a) **ESTRATÉGICO:** é no nível estratégico onde ocorre o acordo político da Administração com a sociedade e é estabelecida a coerência da sua estratégia institucional. Decisões neste nível envolvem a formulação dos objetivos estratégicos e as prioridades para a alocação de recursos públicos em alinhamento com as políticas estabelecidas;

b) **PROGRAMAS E PLANOS:** trata-se do nível tático. Nele se encontram as decisões de implementação e gerenciamento de programas e planos previstos no nível estratégico, através dos quais são executadas as políticas e as ações prioritárias da instituição;

c) **PROJETOS E PROCESSOS:** no nível operacional estão os projetos que contribuirão para o atingimento dos objetivos estabelecidos na estratégia, nos programas e nos planos.

As lideranças, em todos os níveis da organização, devem estar conscientes, capacitadas e motivadas com relação à relevância do gerenciamento de riscos de acordo com essa hierarquia, que são interdependentes.

O gerenciamento de riscos, portanto, deve ser incorporado aos programas, planos, projetos e processos, ou seja, a Administração precisa ter meios de assegurar que o gerenciamento de riscos esteja acontecendo de forma apropriada em cada nível, de acordo com os planos definidos.

4.4. APETITE E TOLERÂNCIA AO RISCO

O APETITE AO RISCO DE TIC refere-se ao nível de risco que a Secretaria de Tecnologia da Informação e Comunicação está disposta a aceitar para atingir seus objetivos estratégicos e operacionais, bem como para enfrentar incertezas e buscar oportunidades, enquanto equilibra os potenciais impactos adversos dos riscos de TIC. Também deve expressar as capacidades reais da Secretaria de Tecnologia da Informação e Comunicação e precisa estar embasado nas estratégias que influenciam os comportamentos organizacionais, cruciais para orientar a tomada de decisões, a alocação de recursos e a implementação de controles.

Importa destacar que o apetite ao risco não é uma medida isolada, mas sim parte de um processo mais amplo de gestão de riscos. Ele fornece uma orientação geral sobre a disposição da Secretaria de Tecnologia da Informação e Comunicação para assumir riscos, enquanto a tolerância ao risco define os limites práticos dentro dos quais os riscos são considerados aceitáveis em diferentes contextos operacionais.

A definição do apetite ao risco da Secretaria de Tecnologia da Informação e Comunicação (ou o APETITE AO RISCO DE TIC) demanda uma análise abrangente, que vai além dos objetivos específicos da área de TIC. É imperativo considerar também as diretrizes, os valores e as restrições que permeiam toda a organização. Portanto, requer uma abordagem holística, que integre as perspectivas da liderança sênior, dos profissionais de TIC, dos auditores internos e externos, e de outras partes interessadas relevantes.

Dada a vinculação hierárquica da Secretaria de Tecnologia da Informação e Comunicação, o APETITE AO RISCO DE TIC precisa se harmonizar com a DECLARAÇÃO DE APETITE A RISCO INSTITUCIONAL, formalizada por meio da Portaria nº. 483/2024-GP, de 01 de fevereiro de 2024. Esta harmonização garante que as ações e decisões da área de TIC estejam alinhadas com a postura geral de risco adotada pelo Poder Judiciário Estadual, propicia uma abordagem integrada e consistente na gestão de riscos, estabelecendo os limites dentro dos quais a Secretaria de Tecnologia da Informação e Comunicação deve operar, promovendo a eficácia dos controles e a resiliência dos sistemas de TIC, além de contribuir de forma eficaz para a missão e os objetivos institucionais, e de fortalecer a governança e a confiança das partes interessadas.

A DECLARAÇÃO DE APETITE A RISCO INSTITUCIONAL fixou um limite aceitável de exposição BAIXO, na faixa de 5,99. Este nível de risco foi definido com o intuito de evitar um excesso de controles – onerosos em termos de tempo e custo – e de preservar a capacidade de inovação, de adaptação e de agilidade do TJPA diante de desafios e oportunidades.

No entanto, a natureza das operações de TIC pode exigir um nível de risco mais conservador em situações específicas, devido às implicações diretas na segurança, na conformidade regulatória e na continuidade dos serviços críticos. Estas situações incluem:

a) **Proteção de Dados Pessoais:** no tratamento de dados pessoais identificáveis (PII), dados de transações financeiras (PCI), dados de crianças e adolescentes, dados pessoais sensíveis, dados judiciais protegidos por sigilo ou qualquer outra informação custodiada pelo TJPA, a Secretaria de Tecnologia da Informação e Comunicação deve adotar um apetite ao risco mais conservador. A exposição a qualquer risco que possa comprometer a confidencialidade, a integridade ou a disponibilidade destes dados deve ser minimizada ao máximo, devido às graves consequências legais e éticas de uma violação de dados;

b) **Conformidade Regulatória:** em situações que envolvem conformidade com regulamentações específicas, como a Lei Geral de Proteção de Dados (LGPD) e outras legislações aplicáveis ao setor público e ao judiciário, o apetite ao risco deve ser mais rigoroso. O não cumprimento dessas normas pode resultar em penalidades severas, prejuízos financeiros e danos à reputação institucional;

c) **Continuidade de Serviços Críticos:** Para sistemas e serviços críticos que suportam operações judiciais essenciais, o apetite ao risco deve ser muito baixo. A interrupção desses serviços pode afetar a administração da justiça e a confiança pública no sistema judiciário. Portanto, é crucial assegurar a alta disponibilidade e resiliência desses sistemas;

d) **Segurança Cibernética em Ambientes de Alta Ameaça:** Em contextos em que há um aumento significativo nas ameaças cibernéticas, como durante eventos de grande visibilidade ou em períodos de instabilidade política, a Secretaria de Tecnologia da Informação e Comunicação deve adotar um apetite ao risco mais restrito. Medidas adicionais de segurança e vigilância reforçada são necessárias para mitigar riscos potenciais.

Nesse sentido, assume-se que o APETITE AO RISCO DE TIC deve se limitar ao máximo nível de risco tolerável, que por sua vez, não deve superior ao maior valor definido na escala de impacto dos fatores de risco, considerando-se a mesma estrutura de matriz de risco proposta no MANUAL DE GESTÃO DE RISCO do TJPA, com escalas de impacto e probabilidade definidas em 5 (cinco) níveis. Ou seja, o APETITE AO RISCO DE TIC fica definido em 5 (cinco).

APETITE AO RISCO DE TIC = TOLERÂNCIA AO RISCO DE TIC = 5

Impende destacar que um apetite a risco baixo não significa uma aversão total ao risco, mas sim uma abordagem prudente e cuidadosa na avaliação e na gestão dos riscos de TIC. Ao estabelecer limites claros e criteriosos para a exposição ao risco, a Secretaria de Tecnologia da Informação e Comunicação reduz a probabilidade de incidentes e contratempos que possam prejudicar suas operações. Essa abordagem conservadora cria um ambiente de estabilidade e confiança, incentivando a experimentação e a busca por soluções inovadoras dentro de um contexto controlado.

Além disso, um apetite a risco mais baixo não implica em uma postura inflexível ou estática. Pelo contrário, promove uma cultura de avaliação contínua de ameaças e também de oportunidades,

estimulando a adaptação proativa às mudanças do ambiente externo e interno. Ao antecipar e gerenciar cuidadosamente os riscos de TIC, o TJPA está mais bem preparado para aproveitar as oportunidades emergentes e responder de forma ágil e eficaz aos desafios que surgirem.

Neste sentido, ainda que a implementação de controles e medidas de mitigação mais conservadores onerem recursos do ponto de vista financeiro, operacional e temporal, ao considerar a materialização de um risco com um impacto acentuado, fica evidente que os custos associados podem ser significativamente mais elevados.

Um incidente de segurança grave ou uma interrupção em sistemas de missão crítica, por exemplo, pode resultar em danos financeiros substanciais, abalo de reputação, processos judiciais e outros efeitos adversos de longo prazo para o TJPA. Além disso, a recuperação de tais incidentes pode exigir recursos consideráveis, tanto em termos de tempo quanto de esforço humano e financeiro.

Para operacionalizar essa abordagem, todos os fatores de risco com impactos classificados como 5 (Muito Alto), cujos planos de mitigação não permitam uma atenuação efetiva dos efeitos adversos (e.g. riscos relacionados à segurança da informação e à utilização indevida, roubo ou vazamento de dados), devem receber tratamento adequado para mitigar sua probabilidade de ocorrência até que seja classificada como 1 (Muito Baixa).

Contudo, é fundamental reconhecer que nenhum esforço será suficiente para garantir a eficácia deste PGRTIC se os problemas apontados na SEÇÃO 2 – Diagnóstico do Ambiente não forem superados. A ausência de uma cultura de riscos consolidada e a baixa capacitação em gestão de riscos representam obstáculos significativos que podem comprometer a segurança, a eficiência e a resiliência das operações de TIC da Secretaria de Tecnologia da Informação e Comunicação. Sem uma abordagem proativa e um entendimento sólido dos riscos de TIC, a Secretaria de TIC estará exposta a vulnerabilidades e ameaças que podem resultar em incidentes graves e custos substanciais para o TJPA.

4.5. RELATÓRIO DE ANÁLISE E AVALIAÇÃO DE RISCOS

O relatório de análise e avaliação de riscos, documento produzido pelo Grupo Estratégico de Governança de TIC (GEGTIC), é o produto resultado da aplicação do processo de gestão de riscos, o qual conterá as informações referentes as ações que serão adotadas para tratar os riscos identificados, dentro do escopo estabelecido pelos Comitês, devendo conter minimamente:

a) Definição do contexto/escopo estabelecido;

b) Justificativas para o escopo definido;

c) Grupo de trabalho designado;

d) Avaliação do relatório de análise e avaliação de risco anterior;

e) Planilha de Análise e Avaliação de Riscos (Anexo II);

f) Descrição complementar das ações de tratamento de risco, indicando unidades responsáveis e prazos, caso necessário.

O GEGTIC será responsável por monitorar a execução do plano, a partir do relatório de análise e avaliação de riscos.

4.6. PLANO DE AÇÕES E CRONOGRAMA

As equipes de cada unidade administrativa da Secretaria de Tecnologia da Informação e Comunicação devem se reunir e proceder ao início da elaboração das etapas do Plano de Gerenciamento de Riscos. Para fins de realização deste processo inicial, são os prazos:

Tabela 2 – Cronograma do plano de ações.

#	AÇÃO	PRAZO (MESES)												
		JUL/2025	AGO/2025	SET/2025	OUT/2025	NOV/2025	DEZ/2025	JAN/2026	FEV/2026	MAR/2026	ABR/2026	..	NOV/2026	DEZ/2026
22.	Revisão Plano de Gestão de Riscos	●												
23.	Treinar e capacitar equipes internas		●	●										
24.	Designar membros para o GEGTIC				●									
25.	Sensibilizar equipes internas				●	●								
26.	Mapear os processos organizacionais de TIC					●	●	●	●	●	●			
27.	Definir o escopo da avaliação de riscos de TIC					●								
28.	Analisar o Contexto e identificar ativos de TIC					●	●							
29.	Realizar a identificação e análise dos riscos							●	●	●				
30.	Realizar a avaliação dos riscos de TIC								●	●				
31.	Realizar a priorização dos riscos de TIC									●	●			
32.	Desenvolver estratégias de tratamento								●	●	●			
33.	Definir a(s) resposta(s) aos riscos mapeados								●	●	●	●		
34.	Validar os riscos mapeados										●	●		
35.	Implementar controles e medidas de mitigação									●	●	●	●	
36.	Monitorar e revisar continuamente os riscos										●	●	●	
37.	Realizar análise de conformidade										●	●	●	
38.	Produzir relatório de análise e avaliação de riscos												●	
39.	Aprovar relatório de análise e avaliação de riscos												●	

#	AÇÃO	PRAZO (MESES)												
		JUL/2025	AGO/2025	SET/2025	OUT/2025	NOV/2025	DEZ/2025	JAN/2026	FEV/2026	MAR/2026	ABR/2026	...	NOV/2026	DEZ/2026
40.	Comunicar as partes interessadas		●	●	●	●	●	●	●	●	●	●	●	
41.	Monitorar o processo de Gestão de Riscos de TIC					●	●	●	●	●	●	●	●	●
42.	Avaliar o processo de gerenciamento de riscos										●	●	●	●

4.7. INDICADORES DE PROCESSO

Os indicadores propostos para avaliação e monitoramento da Gestão de Riscos de TIC estão relacionados na tabela a seguir.

Estes indicadores devem ser adaptados às necessidades específicas da Secretaria de Tecnologia da Informação e Comunicação e ao seu contexto. É importante revisar e ajustar regularmente os indicadores para garantir que eles continuem sendo relevantes e úteis na avaliação da Gestão de Riscos de TIC.

Tabela 3 – Indicadores para avaliação e monitoramento da Gestão de Riscos de TIC.

#	DESCRIÇÃO	MÉTODO DE APURAÇÃO/MEDIÇÃO	FREQUÊNCIA
1.	**Taxa de Identificação de Riscos**	mede a frequência com que novos riscos são identificados. Um aumento constante na taxa de identificação de riscos pode indicar uma melhoria na conscientização e no processo de identificação.	Mensal
2.	**Taxa de Mitigação de Riscos**	proporção de riscos identificados que foram mitigados com sucesso. Isso ajuda a avaliar a eficácia das medidas de mitigação implementadas.	Anual
3.	**Índice de Risco Residual**	avalia o risco restante após a implementação das medidas de mitigação. Pode ser calculado como uma porcentagem do risco inicial e ajuda a determinar o nível de exposição ao risco.	Anual
4.	**Tempo Médio de Resolução de Incidentes**	quanto tempo leva para resolver incidentes de segurança de TI. Um tempo de resolução mais curto pode indicar uma equipe de resposta a incidentes eficiente.	Mensal

5.	**Taxa de Incidentes de Segurança**	frequência e a gravidade dos incidentes de segurança de TI. Isso pode incluir violações de dados, interrupções de serviço e outras falhas de segurança.	Mensal
6.	**Custo de Gerenciamento de Riscos**	custos associados à gestão de riscos de TI, incluindo ferramentas, treinamento, pessoal e outras despesas. Isso ajuda a avaliar a eficiência dos recursos alocados para a gestão de riscos.	Anual

4.8. MONITORAMENTO E CONTROLE

O fluxo regular de informações, revisões dos níveis de riscos e dos controles existentes deverá ser realizada entre os diversos agentes envolvidos, propiciando o acompanhamento da efetividade e eficácia das medidas adotadas.

O gerenciamento de riscos deverá ser implementado de forma gradual e continuada em todas as áreas no âmbito da Secretaria de Tecnologia da Informação e Comunicação. O monitoramento e a análise crítica configuram etapa contínua e essencial do Processo de Gestão de Riscos, tendo em vista que:

a) possibilitam identificar mudanças no perfil do risco e ajustar a resposta, a prioridade e os planos de ação adotados, com base na reavaliação dos contextos internos e externos;

b) asseguram o acompanhamento dos eventos de risco, suas alterações, sucessos e fracassos;

c) garantem a eficácia e eficiência dos controles adotados;

d) identificam os riscos emergentes que poderão surgir após o processo de análise crítica, permitindo que o ciclo do processo de Gestão de Riscos seja reiniciado; e

e) possibilitam a atualização e melhoria contínua do processo de Gestão de Riscos de TIC, de sua estrutura e políticas.

São responsáveis pela realização dessa etapa:

I. **Coordenadorias da SETIC:** monitoram os riscos levantados da atividade/projeto sob sua responsabilidade e o tratamento atribuído a eles;

II. **GRUPO ESTRATÉGICO DE GOVERNANÇA DE TIC (GEGTIC):** realiza a análise crítica de todos os riscos mapeados pelas unidades organizacionais da Secretaria de Tecnologia da Informação e Comunicação e monitora os riscos classificados como “Muito Alto”, “Alto” e “Médio”.

O GEGTIC deve realizar o monitoramento dos riscos por meio da Matriz Gerencial de Riscos de TIC, que será composta de todos os riscos classificados como “Muito Alto”, “Alto” e “Médio”. A matriz de Riscos deve ser formada, além do formulário de mapeamento de risco, pelo plano de implementação dos controles.

O acompanhamento mensal com a devida análise crítica das Coordenadorias, precisa fazer parte da implementação da Gestão de Riscos de TIC, para assegurar a eficácia dos tratamentos propostos. Caso não haja opção de tratamento disponível ou caso as opções de tratamento não alterem o risco de forma relevante, convém que este seja registrado e mantido sob análise crítica.

Essas recomendações podem contribuir para a eficácia do Plano de Gestão de Riscos de TIC. A seleção dos tratamentos de riscos deve ser feita de acordo com os objetivos da organização, apetite ao risco de TIC, critérios de aversão ao risco e recursos disponíveis. Ao selecionar tais opções, a Secretaria de Tecnologia da Informação e Comunicação precisa considerar valores, percepções, potencial envolvimento das partes interessadas e os meios para com elas se comunicar e interagir.

É importante ressaltar que os integrantes do GEGTIC estejam conscientes da natureza e extensão do risco remanescente após as ações de tratamento. A realização do tratamento pode gerar novos riscos que também precisam ser acompanhados. O risco remanescente deve ser documentado e submetido a monitoramento, análise crítica e, quando apropriado, tratamento adicional.

Este documento deve ser minimamente revisado com periodicidade anual, ou sempre que necessário. Todas as situações ou atividades não previstas neste documento deverão ser submetidas à Comissão Permanente de Informática e aos Comitês de Governança de TIC (CGovTIC), de Gestão de TIC (CGesTIC) e de Governança de Segurança da Informação (CGSI), que juntamente com o Grupo Estratégico de Governança de TIC (GEGTIC), deverão avaliar e deliberar a respeito das providências a serem adotadas.

Tabela 4 – Controles do processo de gerenciamento de riscos de TIC.

#	CONTROLE	MÉTODO DE EXECUÇÃO	FREQUÊNCIA
1	Auditoria	realizar uma reunião com as equipes executoras do processo, para avaliar a aderência, os benefícios gerados e oportunidades de melhoria do processo. Essa reunião deve identificar se o processo necessita de revisão.	Anual

O Plano de Gestão de Riscos de TIC 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 TJPA, 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 GEGTIC e para o Comitês de Governança e Gestão.

5. CONSIDERAÇÕES FINAIS

A área da Tecnologia da Informação e Comunicação (TIC), representada pela Secretaria de Tecnologia da Informação e Comunicação, se mostra cada vez mais estratégica para o Tribunal de Justiça do Estado do Pará. 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 ou o impacto de efetivamente ocorrerem.

Além das etapas descritas acima, este Plano de Gestão de Riscos de TIC pode incluir as seguintes recomendações:

a) Implementação de sistemas de orquestração e de automação de processos;

b) Implementação de um sistema específico de registro e acompanhamento de riscos de TIC;

c) Realização de exercícios de simulação de incidentes;

d) Divulgação do PGRTIC para todas as partes interessadas;

Ainda que bem elaborada e instruída, a Gestão de Riscos de TIC pode não produzir os resultados esperados e trazer consequências não pretendidas. Isso destaca a necessidade crítica de adoção de uma abordagem holística e em constante evolução, que não apenas identifique e mitigue riscos, mas também promova a aprendizagem contínua e a adaptação diante de um cenário de ameaças em constante mutação.

No entanto, pouco valor terá este PGRTIC se a prática da Gestão de Riscos de TIC não for internalizada por todos. É fundamental que a Gestão de Risco deixe de ser apenas uma obrigação a ser cumprida e passe a ser um instrumento que contribua para o alcance dos objetivos estabelecidos no âmbito do Poder Judiciário Estadual.

GLOSSÁRIO

Esta seção se presta a reforçar e complementar os termos e definições fixados no Glossário do **MANUAL DE GESTÃO DE RISCOS DO PJPA**, elaborado pela Coordenadoria de Gestão de Processos e Riscos, vinculada ao Departamento de Planejamento, Gestão e Estatística (DPGE).

TERMO	DESCRIÇÃO
Ameaça	fonte potencial de dano, perigo ou qualquer outro resultado indesejável. Normalmente as ameaças são externas e, em razão disso, difíceis de serem controladas.
Apetite a risco	nível de exposição aos riscos que o TJPA está disposto a aceitar ou assumir em busca de seus objetivos estratégicos. Ele representa a quantidade e o tipo de riscos que o Tribunal está disposto a enfrentar em busca de oportunidades ou para alcançar seus objetivos, levando em consideração fatores como tolerância aos riscos, capacidade de resiliência e preferências de stakeholders.
Ativo de TIC	para efeitos do processo de Gestão de Riscos, compreende os serviços tecnológicos ofertados e os sistemas computacionais geridos pela SETIC.
Causa	aquilo que determina a existência ou fonte de um evento de risco e que pode ter outras causas antecedentes.
Consequência	resultado ou grau de importância dos efeitos de um acontecimento (evento de risco) para a instituição.
Contexto	conjunto de fatores internos e externos à organização que, juntamente com os critérios de riscos, definirão o ambiente de gerenciamento dos riscos;
Controles internos da Gestão	engloba o conjunto de regras, procedimentos, diretrizes, protocolos, rotinas de sistemas informatizados, conferências e trâmites de documentos e informações, entre outros, operacionalizados de forma integrada, destinados a enfrentar os riscos e fornecer segurança razoável de que os objetivos organizacionais serão alcançados.
Evento	acontecimento, ocorrência ou fato capaz de gerar impacto positivo ou negativo com potencial para destruir ou agregar valor aos objetivos institucionais.
Fator de risco	variável ou condição que aumenta a probabilidade de ocorrência de um evento indesejado ou impacto negativo em uma determinada situação. Ele pode ser uma característica intrínseca do ambiente, uma ação específica ou qualquer outro elemento que contribua para a materialização de riscos.
Frequência	número de vezes que um evento de risco ocorre, podendo ser observada ou estimada na razão de sua probabilidade;

Gerenciamento de riscos	Concentra-se nas atividades operacionais e técnicas de identificação, avaliação e mitigação de riscos específicos. Voltado para tarefas práticas de controle (planos de contingência, avaliação de impacto e implementação de controles) e monitoramento.
Gestão de riscos	enfatiza uma abordagem mais ampla e estratégica para o gerenciamento de riscos. Inclui não apenas a identificação, avaliação e mitigação de riscos, mas também o desenvolvimento de políticas, estratégias e cultura organizacional relacionadas aos riscos. Envolve a integração da gestão de riscos em todos os níveis da organização e em todos os aspectos de suas operações, indo além daqueles puramente técnicos e financeiros.
Mapa de riscos	representação formal na qual são registrados os principais fatores de riscos institucionais de forma a permitir a identificação e análise dos riscos, bem como a definição de ações necessárias para o seu gerenciamento.
Medida de controle	medida aplicada pela organização para tratar os riscos, aumentando a probabilidade de que os objetivos e as metas organizacionais estabelecidos sejam alcançados.
Monitoramento de riscos	verificação, supervisão, observação crítica ou identificação da situação, executadas de forma contínua, a fim de identificar mudanças no nível de desempenho requerido ou esperado;
Nível de risco	avaliação qualitativa ou quantitativa da probabilidade de ocorrência de um evento adverso e do potencial de impacto associado a esse evento. Ele representa a medida da exposição a riscos em uma determinada situação ou contexto.
Organização estendida	compreende as organizações que operam de forma interdependentes dentro e fora do âmbito da Secretaria de Tecnologia da Informação e Comunicação e que devem ser levadas em consideração (e.g. empresas terceirizadas).
Parâmetros de medição de riscos	referem-se às informações quantitativas ou qualitativas, obtidas direta ou indiretamente, que permitam avaliar as dimensões dos riscos identificados a partir da probabilidade de sua ocorrência e das consequências possíveis.
Parte interessada	pessoa ou organização que pode afetar, ser afetada, ou perceber–se afetada por uma decisão ou atividade
Proprietário do risco	pessoa com a responsabilidade e autoridade para gerenciar o evento que pode se tornar um risco para a instituição.
Processo de trabalho	conjunto definido de atividades inter-relacionadas executadas por humanos ou máquinas para alcançar determinado resultado, produto ou serviço predefinido.
Risco inerente ou bruto	risco a que uma organização está exposta sem considerar quaisquer medidas de controle que possam reduzir a probabilidade de sua ocorrência ou seu impacto.

Risco negativo	evento ou condição incerta que, se ocorrer, provocará um efeito negativo nos objetivos estabelecidos;
Risco positivo	vislumbram as oportunidades sugeridas que podem representar ganhos à instituição;
Risco residual	risco a que uma organização está exposta após a implementação de medidas de controle para o tratamento do risco.
Tratamento de riscos	processo de seleção e implementação de medidas para modificar o nível de risco, visando alcançar um nível aceitável de exposição aos riscos identificados.
Tolerância risco	limite máximo de riscos que o TJPA está disposto a aceitar ou suportar em relação a seus objetivos estratégicos. Ela representa a capacidade da organização de lidar com a incerteza e de absorver perdas sem comprometer significativamente a realização de seus objetivos ou a continuidade de suas operações. A tolerância a risco é uma medida mais concreta e específica do que o apetite a risco, indicando os limites aceitáveis de exposição aos riscos em termos de probabilidade e impacto.
Vulnerabilidade	fraquezas, falhas que podem facilitar o surgimento de ameaças a um ativo. Normalmente as vulnerabilidades são internas e podem ser tratadas, diminuindo-se a possibilidade de ameaças aos objetivos institucionais.