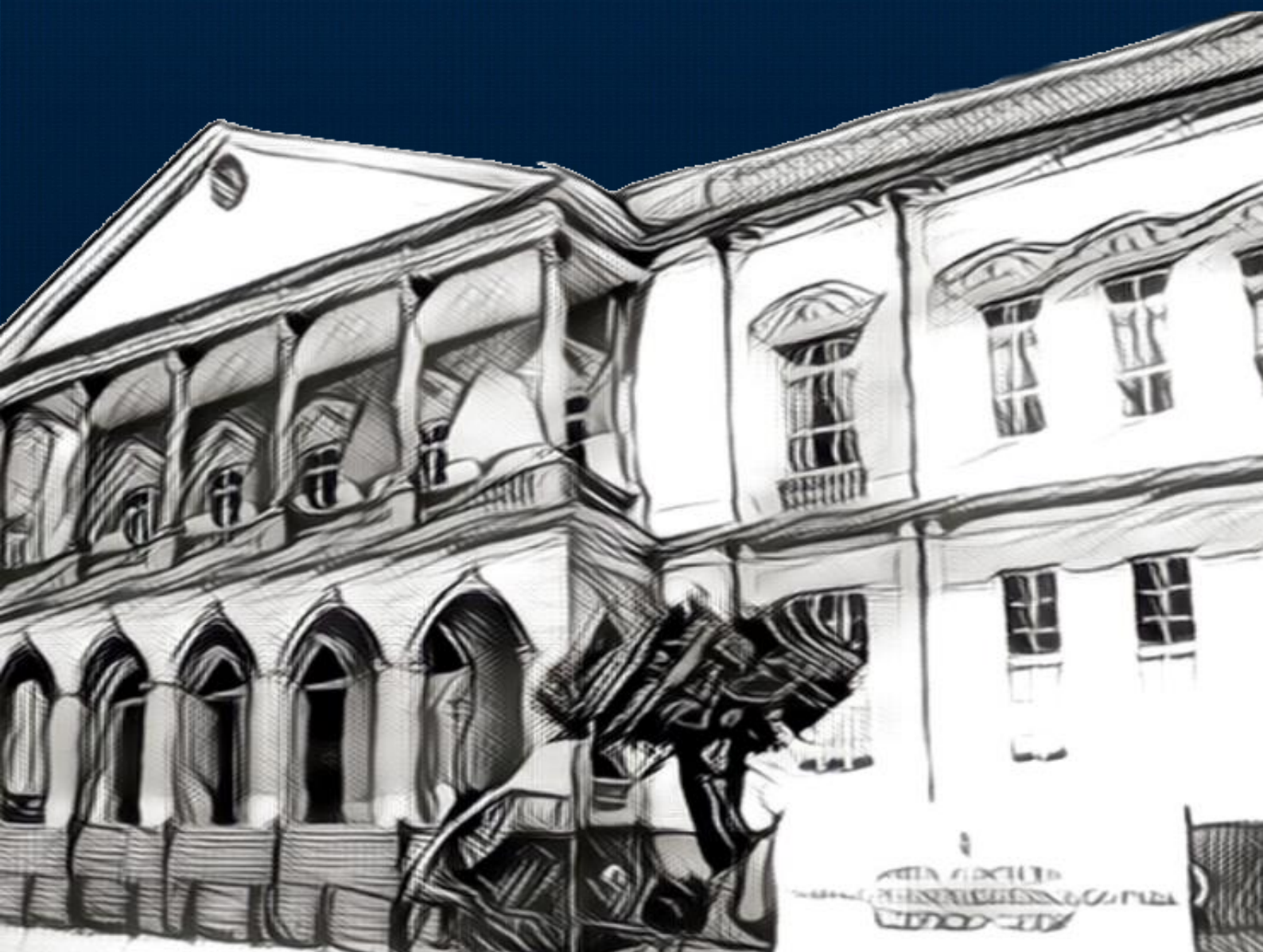
TRIBUNAL DE JUSTIÇA
DO ESTADO DO PARÁ

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 INFORMÁTICA –

2023 - 2025

OUTUBRO / 2023

SECRTARIA DE INFORMÁTICA

SECRETÁRIO DE INFORMÁTICA
MÁRCIO GÓES DO NASCIMENTO

COORDENADOR DE APLICAÇÕES
ÁLVARO ROGERS CARDOSO ALVÃO

COORDENADOR DE ATENDIMENTO AO USUÁRIO
RAMON SANTOS DO NASCIMENTO

COORDENADOR DE SUPORTE TÉCNICO
ERICK JOHNY MACIEL BOL

ASSESSORES DE INFORMÁTICA
LUCIANA MACHADO SILVEIRA MELLO
RONILDO JOJI MATSUURA

CHEFES DE DIVISÃO/SERVIÇO
BRUNO VIEIRA DOS SANTOS
CARLOS DIEGO POJO DE BRITO
DANIEL FONTES PEREIRA
FÁBIO VENICIUS FERREIRA DOS REIS
LEONARDO JUNQUEIRA DA SILVA VALENTE
LUIZ FERNANDO MONTEIRO SENA
MARCUS VINICIUS BARBOSA E SILVA
SIMONNE SOARES BATISTA

COMITÊ DE GOVERNANÇA DE TIC

(PORTARIA Nº. 3127/2023-GP)

CHARLES MENEZES BARROS
SÍLVIO CÉSAR DOS SANTOS MARIA
FÁBIO ROBERTO ALBUQUERQUE AZEVEDO
LUCIANA MACHADO SILVEIRA MELLO
LUCIANA SÁ FERNANDES
MÁRCIO GÓES DO NASCIMENTO
MIGUEL LUCIVALDO ALVES SANTOS
TIAGO SILVA GUIMARÃES
VICENTE DE PAULA BARBOSA MARQUES JÚNIOR

COMITÊ DE GESTÃO DE TIC

(PORTARIA Nº. 2585/2023-GP)

ÁLVARO ROGERS CARDOSO ALVÃO
ERICK JOHNY MACIEL BOL
FÁBIO CEZAR MASSOUD SALAME DA SILVA
FÁBIO ROBERTO ALBUQUERQUE AZEVEDO
IGOR PINTO SIMÕES
LUCIANA MACHADO SILVEIRA MELLO
MÁRCIO GÓES DO NASCIMENTO
RAMON SANTOS DO NASCIMENTO

COMITÊ DE GOVERNANÇA DE SEGURANÇA DA INFORMAÇÃO

(PORTARIA Nº. 847/2023-GP)

DESª. LUZIA NADJA GUIMARÃES NASCIMENTO
SÍLVIO CÉSAR DOS SANTOS MARIA
ADIL BAHIA DA SILVA REZENDE
CAMILA AMADO SOARES
CRISTHIANNE DE CAMPOS CORRÊA
ERICK JOHNY MACIEL BOL
FÁBIO DJAN OLIVEIRA DE LIMA
MÁRCIO GÓES DO NASCIMENTO
MIGUEL LUCIVALDO ALVES SANTOS
TEN.CEL.QOPM RODRIGO ALEIXO MELO DOS SANTOS
TIAGO SILVA GUIMARÃES
VICENTE DE PAULA BARBOSA MARQUES JÚNIOR

CONTROLE DE REVISÃO		
ATIVIDADE	**DATA**	**RESPONSÁVEL**
Revisão v2.0	20/10/2023	Secretaria de Informática
Aprovação v2.0	20/10/2023	Secretaria de Informática

VERSÃO	**DATA**	**DESCRIÇÃO**
1.0	15/09/2023	Elaboração da minuta do PGRTIC.
1.1	xx/xx/xxxx	Revisão de conteúdo.
2.0	20/10/2023	Modificações na estrutura e no conteúdo da minuta do PGRTIC.

Elaborado por:	Título do Documento:	Versão:	Revisão:
SECRETARIA DE INFORMÁTICA	**PLANO DE GESTÃO DE RISCOS DE TIC – PGRTIC**	**2**	**0**
Aprovado por:	Processo:	Data:	
SECRETARIA DE INFORMÁTICA	**N/D**	**20/10/2023**	

APRESENTAÇÃO

O presente Plano de Gestão de Riscos de Tecnologia da Informação – PGRTIC é um marco que reforça nosso compromisso em garantir a segurança, a inovação e a eficiência em um ambiente cada vez mais digital. É com grande entusiasmo e responsabilidade que iniciamos uma nova etapa em nossa jornada de aprimoramento da Tecnologia da Informação no âmbito do Poder Judiciário.

Em um mundo em constante transformação, a Tecnologia da Informação desempenha um papel crucial em nossa missão de assegurar que a justiça seja acessível, eficaz e eficiente. A digitalização de processos e o uso de sistemas avançados se tornaram indispensáveis para melhorar a experiência de todos os envolvidos no processo judicial, desde magistrados e servidores até os cidadãos que buscam nossos serviços.

No entanto, a crescente dependência da tecnologia traz consigo desafios significativos em relação à segurança, à privacidade e à continuidade dos serviços. É por isso que a introdução deste Plano de Gestão de Riscos de TIC é um passo crucial.

Este Plano não é apenas um conjunto de diretrizes, também é um compromisso concreto com a segurança e com a resiliência da nossa infraestrutura. Detalha como identificaremos, avaliaremos e daremos tratamento adequado aos riscos específicos de nossa área, garantindo que nossos sistemas funcionem de maneira confiável, que os dados estejam protegidos e que possamos responder de modo proativo e eficaz a eventos inesperados.

Nossa missão é clara: muito além de meramente conduzir o planejamento e a execução das ações relacionadas à aplicação de Tecnologias da Informação, a de proporcionar uma experiência digital segura e eficiente a todos os envolvidos no exercício jurisdicional. Ao lançar este Plano de Gestão de Riscos de TIC, estamos reforçando nosso compromisso em cumprir essa missão, mantendo a confiança de nossos stakeholders, protegendo dados e informações, e assegurando a plena continuidade de nossos serviços.

Cumpre salientar que o Plano de Gestão de Riscos de TIC sofrerá alterações no transcorrer do tempo, para sua adaptação ao grau de maturidade alcançado e às novas práticas adotadas. Portanto, a elaboração deste Plano é dinâmica, destinando-se a contribuir para o alcance dos objetivos finalísticos da Secretaria de Informática.

Agradecemos a todos que trabalham incansavelmente para tornar nossa visão realidade. Somente unindo nossos esforços seremos capazes de enfrentar os desafios do mundo digital e assegurar que a justiça prevaleça, independentemente das adversidades.

MARCIO GÓES DO NASCIMENTO

SECRETÁRIO DE INFORMÁTICA

SUMÁRIO

1. INTRODUÇÃO

O fortalecimento da governança, incluso dentre os macrodesafios do Plano Estratégico 2021-2026 do Tribunal de Justiça do Estado do Pará, prevê a adequação da gestão de riscos operacionais, dos controles internos administrativos e do processo de governança corporativa, para que tais processos funcionem de acordo com o planejado. Além disso, faz recomendações para a melhoria das operações, em termos de economicidade, eficiência e desempenho geral da instituição.

Neste contexto, a perspectiva de riscos é de suma importância no processo de tomada de decisões racionais e fundamentadas, capturando a identidade estratégica e os objetivos do Poder Judiciário Estadual, criando e protegendo valor, melhorando o desempenho e contribuindo para o aumento na capacidade do TJPA em lidar com eventos inesperados que possam afetar negativamente os objetivos perseguidos.

Ademais, as incertezas constituem riscos e oportunidades com capacidade para destruir ou agregar valor. A principal finalidade da Gestão de Riscos de TIC é garantir a eficiência e a eficácia organizacional, integrando o processo de gerenciamento de riscos à governança e à gestão, de modo que esteja incorporada à cultura institucional.

Portanto, o presente Plano de Gestão de Riscos de TIC – PGRTIC foi concebido com o intuito de especificar a abordagem, os componentes de gestão (procedimentos, práticas, atribuição de responsabilidades, sequência e planos de ação) e os recursos a serem empregados no gerenciamento dos riscos de TIC, estabelecendo as métricas e os critérios para os processos de análise e avaliação, orientando estratégias de resposta/tratamento dos riscos e internalizando tais práticas nas atividades conduzidas pelas equipes técnicas da Secretaria de Informática do TJPA.

Por fim, este PGRTIC também consiste na descrição documentada da construção e da manutenção da estrutura necessária para a implantação, para o suporte e para o gerenciamento de riscos no âmbito da Secretaria de Informática do TJPA, incluindo a definição:

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 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 **PLANO DE GESTÃO DE RISCOS DO TJPA (versão 1.2, de 06/12/2019)**, elaborado pelo Núcleo Estratégico de Governança de Auditoria e Risco da Secretaria de Auditoria Interna – SEAUD, 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 organizacionais 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 Informática 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 Informática;

VIII. **Considerar a importância dos fatores humanos e culturais:** o processo de Gestão de Riscos de TIC deverá reconhecer as capacidades, 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 Plano de Gestão de Riscos de TIC. 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 riscos de TIC aos quais a Organização pode estar exposta;

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

d) Apoiar as lideranças da Secretaria de Informática na definição e revisão de seu apetite e tolerância aos riscos, bem como das métricas para sua avaliação em âmbito corporativo;

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 Informática 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 todas as subunidades da Secretaria de Informática do TJPA, abrangendo as áreas de planejamento e gestão, de governança, de infraestrutura, de aplicações, de segurança da informação, e de atendimento a usuários.

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 do órgão com a sociedade e se estabelece 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;

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 Informática.

Com a finalidade de, periodicamente, serem reavaliados os riscos no ambiente de TI, o processo de Gestão de Riscos de TIC deverá ser aplicado no início de cada Gestão, mas 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, documentos estes encontrados no sítio da internet: https://www.tjpa.jus.br/PortalExterno/hotsite/planejamento-estrategico/instrumentos.xhtml?idPagina=669281;

c) **Plano de Gestão de Risco do TJPA**, versão 1.2, 06/12/2019, 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 31010:2012**, 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 Informática do TJPA, criada pela Lei 6.850/2006 de 02/05/2006, 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 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 Informática:

I. **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;

II. **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;

III. **COORDENADORIA DE SUPORTE TÉCNICO – CST:** 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.

Fazem parte de estrutura de governança de TIC:

IV. **COMITÊ DE GOVERNANÇA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO – CGOVTIC:** de caráter estratégico, deliberativo e multidisciplinar, instituído pela Portaria 3127/2023-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);

V. **COMITÊ DE GESTÃO DE TECNOLOGIA DA INFORMAÇÃO – CGESTIC:** instituído pela Portaria 2585/2023-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 Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD 2021-2026);

VI. **COMITÊ DE GOVERNANÇA DE SEGURANÇA DA INFORMAÇÃO – CGSI:** instituído pela Portaria 847/2023-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 Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD 2021-2026).

2.2. CONTEXTUALIZAÇÃO

Abordar o diagnóstico do processo de Gestão de Riscos de Tecnologia da Informação e Comunicação – PGRTIC, no âmbito da Secretaria de Informática do TJPA e 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. O processo de Gestão de Riscos de TIC, embora instituído desde 2019, permanece incipiente, caracterizado por sua baixa aplicabilidade e pela falta de revisão periódica.

Primeiramente, as deficiências no gerenciamento do processo de Gestão de Riscos de TIC é alarmante. A organização carece de uma estrutura formal e sólida para identificar, analisar, avaliar e dar tratamento adequado aos riscos associados à tecnologia da informação. Isso acaba por criar um ambiente propenso a vulnerabilidades e ameaças, as quais podem impactar negativamente as operações e a segurança dos dados.

Ademais, uma das questões mais preocupantes é a completa ausência de Gerenciamento de Processos. Sequer existe um mapeamento dos processos associados ao domínio de TIC, dificultando o entendimento das atividades, a identificação dos pontos críticos e dos riscos. Sem essa visibilidade, a organização está exposta a riscos que podem passar despercebidos.

A ausência de atribuição clara e formal de papéis e responsabilidades é outro desafio significativo. Não existe clareza quanto a quem deve ser responsável por identificar, avaliar e tratar os riscos de TIC. Essa lacuna na estrutura de governança torna o processo de Gestão de Riscos de TIC ineficaz e fragmentado, podendo resultar na falta de responsabilidade e de prestação de contas.

A deficiência de equipe especializada é um problema adicional. A tecnologia da informação está em constante evolução, e é essencial contar com profissionais qualificados para compreender e lidar com os riscos associados. A necessidade de capacitação se torna evidente, pois a falta de conhecimento pode levar a decisões inadequadas e estratégias de gerenciamento de riscos ineficazes.

3. ESTRUTURA DE GESTÃO DE RISCOS DE TIC

3.1. ESTRUTURA

Conforme orientações contidas na Norma ABNT NBR ISO 31000:2018, 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 defesa definida no **PLANO DE GESTÃO DE RISCOS DO TJPA (versão 1.2, 06/12/2019)**, elaborado pelo Núcleo Estratégico de Governança de Auditoria e Risco da Secretaria de Auditoria Interna – SEAUD, a estrutura de governança da Gestão de Riscos de TIC fica composta da seguinte forma:

I. **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 Informática – SECINFO;

II. **SEGUNDA LINHA:** de natureza tática, deverá ser exercida pelo Grupo Estratégico de Governança de TIC – GEGTIC, 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;

III. **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 SECINFO.

Mais detalhadamente, a estrutura de governança do gerenciamento de riscos da Secretaria de Informática será constituída pelas seguintes instâncias:

Os **Comitês de Gestão da Área de TIC – CGesTIC/PJPA, de Governança de TIC – CGovTIC/PJPA e de Governança da Segurança da Informação – CGSI/PJPA** são as instâncias deliberativas da política e do processo de Gestão de Riscos de TIC.

O **Grupo Estratégico de Governança de TIC – GEGTIC da Secretaria de Informática**, 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.

Os **Núcleos de Gestão de Riscos – NGR** são instâncias de orientação e supervisão operacional das atividades de gestão de riscos desempenhadas pela primeira linha de defesa, instituídas nas unidades administrativas da SECINFO. Cada Núcleo de Gestão de Riscos será composto pelos respectivos Coordenadores de cada subunidade e por servidores por estes designados, em quantitativo necessário para resguardar o cumprimento regular de suas competências.

O **Núcleo Estratégico de Governança de Auditoria e Risco da 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.

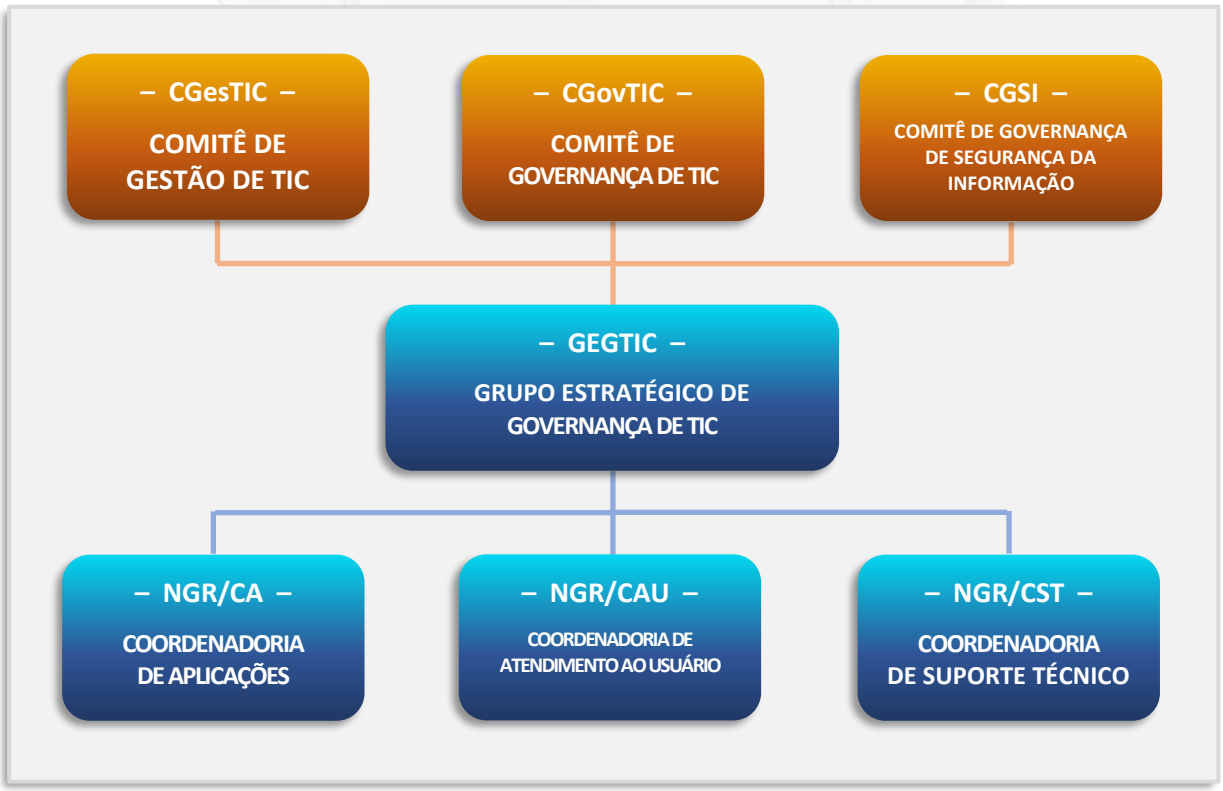


Figura 1 – Estrutura de governança do gerenciamento de riscos de TIC.

3.2. COMPETÊNCIAS E RESPONSABILIDADES

Compete ao **Comitê de Governança de TIC – CGovTIC/PJPA**, ao **Comitê de Gestão da Área de TIC – CGesTIC/PJPA** e ao **Comitê de Governança da Segurança da Informação – CGSI/PJPA**, com relação à Gestão de Riscos de TIC, no âmbito de suas atribuições:

a) Promover a revisão periódica e a atualização da Política de Gestão de Riscos de TI;

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

c) Operacionalizar, no âmbito das unidades da Secretaria de Informática, 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 Informática**, com relação à gestão de riscos de TIC:

m) Coordenar o processo e acompanhar a execução das atividades relacionadas à Gestão de Riscos de TIC;

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

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

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

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

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

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

t) Aperfeiçoar o processo de decisão baseado em riscos;

u) Atender às requisições do Núcleo Estratégico de Governança de Auditoria e Risco da SEAUD e dos Comitês de Governança de TIC – CGovTIC, de Gestão da Área de TIC – CGesTIC, e de Governança da Segurança da Informação – CGSI;

v) Subsidiar a Secretaria 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;

w) 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;

x) Avaliar e divulgar as melhores práticas de gestão de riscos para utilização no âmbito da Secretaria de Informática;

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

z) Elaborar e manter atualizado o Manual de Gestão de Riscos de TIC do TJPA;

aa) Zelar pelo estrito cumprimento da Política de Gestão de Riscos do TJPA;

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

Compete a cada um dos **Núcleos de Gestão de Riscos – NGR,** no âmbito de suas respectivas unidades e subunidades administrativas:

cc) Dar suporte à identificação, análise e avaliação dos riscos dos processos organizacionais selecionados para a implementação da Gestão de Riscos no âmbito da SECINFO;

dd) Conhecer e adotar a política e os instrumentos de gestão de riscos, promovendo a efetividade dos controles dela decorrentes;

ee) Monitorar a evolução dos níveis de riscos e a efetividade das medidas de controle implementadas;

ff) Construir e propor ao Grupo Estratégico de Governança de TIC – GEGTIC e ao Núcleo Estratégico de Governança de Auditoria e Risco da Secretaria de Auditoria Interna – SEAUD os indicadores de desempenho para a Gestão de Riscos de TIC, alinhados aos indicadores de desempenho da própria SECINFO;

gg) fornecer subsídios para o acompanhamento, o monitoramento e a análise crítica do processo de gestão de riscos em suas áreas de atuação;

hh) Medir o desempenho da Gestão de Riscos de TIC, objetivando sua melhoria contínua;

ii) Reportar ao GEGTIC os riscos que eventualmente extrapolarem sua competência e capacidade para gerenciamento;

jj) Requisitar aos responsáveis pelo gerenciamento de riscos dos processos organizacionais as informações e documentos relacionados à Gestão de Riscos de TIC;

kk) Identificar e consolidar as necessidades de capacitação dos servidores das unidades da Secretaria de Informática, nos temas afetos às disciplinas de Gestão de Riscos, e encaminhar a(s) demanda(s) para aprovação pela Secretaria de Informática e para conhecimento por parte dos Comitês competentes e do Núcleo Estratégico de Governança de Auditoria e Risco da SEAUD;

ll) Atender às requisições do Grupo Estratégico de Governança de TIC – GEGTIC e do Núcleo Estratégico de Governança de Auditoria e Risco da SEAUD;

mm) Estimular a cultura de gestão de riscos em suas equipes e participar de ações de sensibilização e capacitação.

Compete aos servidores **responsáveis pelo gerenciamento dos riscos de TIC** dos processos organizacionais da Secretaria de Informática:

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

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

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

qq) 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;

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

ss) Disponibilizar as informações adequadas quanto à Gestão dos Riscos dos processos sob sua responsabilidade a todos os níveis da Secretaria de Informática e demais partes interessadas;

tt) Notificar seus superiores hierárquicos e o Núcleo de Gestão de Riscos associado sempre que identificar eventuais riscos não mapeados em processos organizacionais fora de sua responsabilidade; e

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

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

Compete ao **Núcleo Estratégico de Governança de Auditoria e Risco da Secretaria de Auditoria Interna – SEAUD**:

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

ww) Realizar auditorias internas baseadas em riscos;

xx) Disponibilizar à Secretaria de Informática, mais especificamente ao GEGTIC, as ferramentas e técnicas utilizadas pela auditoria interna para analisar riscos e controles administrativos na área de TI;

yy) 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 Informática**:

zz) 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	NGR	GEGTIC	COMITÊS	SEAUD
	1ª. LINHA	2ª. LINHA	2ª. LINHA	3ª. LINHA
Definir Plano de Gestão de Riscos	C	R	A	A
Designar membros para o GEGTIC	I	- - - -	A	I
Definir o escopo da avaliação de riscos	R	R	A	I
Analisar o Contexto e identificar ativos de TIC	R	R	A	I
Realizar a identificação e análise dos riscos	R	C	A	I
Realizar a avaliação dos riscos de TIC	R	R	A	I
Realizar a priorização dos riscos de TIC	C	R	A	I
Definir a(s) resposta(s) aos riscos mapeados	R	C	A	I
Validar os riscos mapeados	I	R	A	I
Implementar os planos de tratamento de riscos	C	R	I	I
Identificar e avaliar controles existentes	A	A	C	I
Produzir relatório de análise e avaliação de riscos	C	A	I	I
Aprovar relatório de análise e avaliação de riscos	I	I	A	C
Monitorar o processo de Gestão de Riscos de TIC	R	R	I	I
Coordenar o processo de gerenciamento de riscos	I	R	I	C
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 Informática, priorizando-se o processo de gerenciamento de processos.

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 TI 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 Informática.

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 outubro/2024. 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. 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 Plano de Gestão de Riscos institucional.

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 processos de gestão.

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 riscos e no acompanhamento das estratégias de tratamento. Fazem parte do grupo de recursos de TIC que irão apoiar a Gestão de Riscos institucional os seguintes sistemas:

I. **PLATAFORMA TARGET:** plataforma digital voltada para a execução e o controle das ações e resultados de planejamento estratégico, que possibilita assistir tanto o processo de gerenciamento de processos quanto o processo de gerenciamento de riscos;

II. **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 GESTÃO DE RISCOS DE TIC:** as etapas do processo de gestão 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, com o apoio da PLATAFORMA TARGET e de ferramentas complementares;

b) **REGISTROS DE EVENTOS DE RISCO:** o monitoramento contínuo e a análise crítica acerca do processo de Gestão 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 RISCOS:** 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 já identificados.

TREINAMENTO:

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.

A Secretaria de Informática, 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:

d) Técnicas e ferramentas de mapeamento de processos;

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

f) 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).

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.

O treinamento e a capacitação adequados dos servidores desempenham um papel crucial na mitigação de riscos, na proteção dos ativos de TIC e na manutenção da confiança do público. Portanto, investir em programas de treinamento contínuo é um passo essencial na garantia da segurança e eficiência dos sistemas de TIC do judiciário

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 **PLANO DE GESTÃO DE RISCO DO TJPA (VERSÃO 1.2, DE 06/12/2019)** do Núcleo Estratégico de Governança de Auditoria e Risco da Secretaria de Auditoria Interna – SEAUD.

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 é coordenado pelo Grupo Estratégico de Governança de TIC - GEGTIC, tendo na sua execução a participação das demais unidades da Secretaria de Informática por meio dos Núcleos de Gestão de Riscos, 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 Informática, 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 SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO:** 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 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 seu tratamento;

III. **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 manter na base de riscos de TIC. A equipe de planejamento da contratação é responsável por identificar e monitorar os riscos referentes ao processo licitatório (contratação) até etapa de homologação, enquanto o gestor do contrato é responsável por gerenciar os riscos inerentes à execução do contrato;

IV. **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;

V. **RISCOS EM PROCESSOS DE TIC:** riscos identificados nos processos mapeados e/ou instituídos pela Secretaria de Informática 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 Informática do TJPA, de forma gradual, em prazo e extensão a serem definidos pelo **Grupo Estratégico de Governança de TIC – GEGTIC** da própria SECINFO – 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 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 Informática.

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 de gerenciamento de riscos definidos.

4.4. APETITE E TOLERÂNCIA AO RISCO

O apetite ao risco deve expressar a realidade da Secretaria de Informática, e precisa estar embasado nas estratégias que influenciam os comportamentos organizacionais. Para tanto, minimamente, se faz necessário:

I. Um entendimento comum aso riscos de TIC; e

II. Que a SECINFO esteja preparada para as probabilidades e os impactos das ameaças conhecidas/mapeadas;

Importa ressaltar que a Secretaria de Informática deve definir o nível máximo de tolerância aos riscos antes de iniciar/implementar seu processo de Gestão de Riscos.

O desenvolvimento de um apetite a risco se condiciona a uma análise prévia do(a):

III. **PERFIL DE RISCO:** definição dos principais riscos da SECINFO e dos controles para sua mitigação;
IV. **CAPACIDADE DE RISCO:** definição da quantidade de risco que a SECINFO pode absorver.

A Declaração de Apetite ao Risco deve ser feita por meio de documento oficial, contendo de forma clara os limites de tolerância. Esta declaração é de responsabilidade do Comitê de Governança de TIC – CGovTIC e deve orientar o comportamento dos Núcleos de Gestão de Riscos, dos proprietários dos ativos de TIC, dos responsáveis pelo risco, assim como deve orientar os processos de tomada de decisões estratégicas.

A definição do apetite passa pelo entendimento dos Planejamentos Estratégicos, das metas estabelecidas, dos processos envolvidos, das partes interessadas e da cultura da Secretaria de Informática no que se refere aos riscos suportados.

Somente a partir do entendimento da cultura de risco e dos valores da instituição, pode ser iniciado o processo de identificação do Apetite ao Risco.

É imprescindível que o apetite esteja alinhado ao Planejamento Estratégico da Secretaria de Informática, uma vez que precisa ser definido no nível estratégico da organização. Entretanto, a Gestão dos Riscos de TIC deve se dar em todos os níveis, sem distinção.

A Declaração de Apetite ao Risco deve comunicar os seguintes pontos:

a) **VALORES CORPORATIVOS:** quais riscos a organização está disposta a assumir e quais devem ser evitados?

b) **ESTRATÉGIA:** quais riscos são inerentes à estratégia?

c) **STAKEHOLDERS:** quanto e quais tipos de riscos podem assumir?

d) **CAPACIDADE:** quanto risco a organização pode absorver?

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 Informática 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)												
		OUT/2023	NOV/2023	DEZ/2023	JAN/2024	FEV/2024	MAR/2024	ABR/2024	MAI/2024	JUN/2024	JUL/2024	AGO/2024	SET/2024	OUT/2024
1.	Definir Plano de Gestão de Riscos	●												
2.	Designar membros para o GEGTIC		●											
3.	Mapear os processos organizacionais de TIC			●	●	●	●	●	●					
4.	Definir o escopo da avaliação de riscos			●										
5.	Analisar o Contexto e identificar ativos de TIC			●	●									
6.	Realizar a identificação e análise dos riscos					●	●	●						
7.	Realizar a avaliação dos riscos de TIC						●	●						
8.	Realizar a priorização dos riscos de TIC							●	●					
9.	Definir a(s) resposta(s) aos riscos mapeados						●	●	●	●				
10.	Validar os riscos mapeados								●	●				
11.	Implementar os planos de tratamento de riscos							●	●	●	●			
12.	Identificar e avaliar controles existentes								●	●	●			
13.	Produzir relatório de análise e avaliação de riscos											●		
14.	Aprovar relatório de análise e avaliação de riscos											●		
15.	Monitorar o processo de Gestão de Riscos de TIC			●	●	●	●	●	●	●	●	●	●	●
16.	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 organização 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 Informática. 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. **NÚCLEOS DE GESTÃO DE RISCOS DE TIC – NGR:** 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 Informática e monitora os riscos classificados como “Extremos”, “Altos” e “Médios”.

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 “Extremos”, “Altos” e “Médios”. 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 dos Núcleos de Gestão de Riscos – NGR 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, critérios de aversão ao risco e recursos disponíveis. Ao selecionar tais opções, a organização 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 o tratamento dos riscos. 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 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, irão avaliá-las e aprová-las.

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) se mostra cada vez mais estratégica para o Tribunal de Justiça do Estado do Pará, 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 ou o impacto de efetivamente ocorrerem.

Além das etapas descritas acima, o plano de gestão de riscos pode incluir as seguintes recomendações:

a) Implementação de um sistema de registro de riscos;

b) Realização de exercícios de simulação de incidentes;

c) Divulgação do plano de gestão de riscos 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 **PLANO DE GESTÃO DE RISCO DO TJPA (versão 1.2, de 06/12/2019)**, elaborado pelo Núcleo Estratégico de Governança de Auditoria e Risco da Secretaria de Auditoria Interna – SEAUD.

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.
Ativo de TIC	para efeitos do processo de Gestão de Riscos, compreende os serviços tecnológicos ofertados e os sistemas computacionais geridos pela SECINFO.
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.
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;
Organização estendida	compreende as organizações que operam de forma interdependentes dentro e fora do âmbito da Secretaria de Informática 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.
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	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.
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.