PODER JUDICIÁRIO
DO ESTADO DE RORAIMA

Plano de Gestão de Riscos de TI

Secretaria de Tecnologia da Informação - STI

Boa Vista , Abril de 2025 | Versão 2.0

COMPOSIÇÃO

Desembargador Leonardo Cupello
Presidente

Desembargador Almiro Padilha
Vice – Presidente

Desembargador Erick Linhares
Corregedor - Geral de Justiça

Desembargadora Elaine Bianchi
Ouvidora – Geral

Desembargadora Tânia Vasconcelos
Diretora da Escola Judicial de Roraima

SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO

Secretário de Tecnologia da Informação

Sormany Brilhante

Subsecretários

Allef Weyller Batista Esbell

Carlos Roberto Albuquerque Dias da Silva

José de Nazaré Reis dos Santos

Henrique Acquati Negreiros

Paulo Adriano Brito Oliveira

Targino Carvalho Peixoto

Chefes de Setor

Amanda Cavalcante Sanguanini

Amaro da Rocha e Silva Júnior

Carlos Vinicius da Silva Souza

Cinara da Conceição Araújo

Crispim José de Melo Neto

George Wilson Lima Rodrigues

Marco Aurélio Carvalho Feitosa

Saimon Palácio Pereira

pg

SUMÁRIO

HISTÓRICO DE VERSÕES

Versão	Data	Autor	Notas da Revisão
1.0	2020	Tatiana Brasil Brandão	Elaboração
1.1	2020	Tatiana Brasil Brandão	Inclusão dos artefatos, definição do processo, adequação do passo a passo, objetivos do processo
2.0	2025	Tatiana Brasil Brandão	Reformulação

1. INTRODUÇÃO

O Plano de Gestão de Riscos da Secretaria de Tecnologia da Informação - STI do Tribunal de Justiça do Estado de Roraima está alinhado com as diretrizes estabelecidas pela norma ABNT NBR 27005:2019 e pela Resolução TJRR/TP N.º 8, de 21 de fevereiro de 2024, que formalizou a Política de Gestão de Riscos e faz parte como um dos mecanismos do Programa de Integridade e Compliance do Tribunal.

2. OBJETIVOS ESPECÍFICOS

- O objetivo deste plano é identificar e apontar passos necessários, de acordo com práticas listadas em literatura e conhecimento prático, para a Gestão de Riscos de TIC no Tribunal de Justiça de Roraima - TJRR.

3. GESTÃO DE RISCOS

A gestão de riscos visa identificar, avaliar e reduzir continuamente os riscos relacionados a TI dentro dos níveis de tolerância definidos pela Alta gestão da organização.

3.1 GESTOR DE RISCO DA TI

Gestor de riscos da TI é representado pelo Secretário de Tecnologia da Informação, que possui a responsabilidade de escolher os processos de trabalho e fornecer informações essenciais sobre os riscos durante as etapas subsequentes da metodologia. Além disso, é encarregado de supervisionar o processo como um todo e comunicar-se com as partes interessadas.

Suas atribuições compreendem:
I - realizar a escolha dos processos de trabalho que devam ter os riscos gerenciados e tratados, tendo em vista a dimensão dos prejuízos que possam causar;
II - propor os níveis aceitáveis de exposição ao risco, de modo a consolidar a tolerância ao risco das unidades e dos serviços auxiliares; e
III - definir as ações de tratamento a serem implementadas, bem como o prazo de implementação e avaliação dos resultados obtidos.

A aplicação da metodologia conduzirá à formulação de planos de ação destinados ao tratamento dos riscos priorizados. Estes planos incluirão atividades, para as quais é essencial designar um gestor responsável, diferentemente do gestor de riscos que monitora todo o processo, este gestor não terá a responsabilidade pelo risco, mas apenas pelas atividades a ele designada.

3.2 PROCESSOS GESTÃO DE RISCOS DE TI

Aplicação sistemática de políticas, procedimentos e práticas de gestão para as atividades de comunicação, consulta, estabelecimento do contexto, identificação, análise, avaliação, tratamento, monitoramento e análise crítica dos riscos.

Os Processos de riscos de TIC são determinados pela norma ABNT NBR 27005:2019 e pela Resolução TJRR/TP N.º 8, de 21 de fevereiro de 2024 compreendido pelas seguintes fases:

I – Estabelecimento do contexto – etapa em que são identificados os objetivos relacionados ao processo organizacional e definidos os fatores externo e interno que podem afetar o alcance dos objetivos/resultados (pessoas, sistemas informatizados, estruturas organizacionais, legislação, recursos, stakeholders etc.) e os critérios de riscos a serem levados em consideração ao gerenciar riscos;

Compõem os critérios de risco:

- Escala de probabilidade: define como a probabilidade será medida. A probabilidade está associada às chances de um evento ocorrer;
- Escala e impacto: define natureza e tipos de consequências e como elas serão medidas nas diversas áreas. Para definir o nível do impacto, é necessário primeiro considerar as dimensões do objetivo do processo de trabalho avaliado;
- Matriz impacto X Probabilidade: define como o nível de risco deve ser determinado;
- Apetite a risco: é o nível em que um risco se torna aceitável ou inaceitável;

- Matriz de classificação de riscos: define como os riscos serão classificados quanto à significância;
- Diretrizes para priorização e tratamento: determina como os riscos serão priorizados; e
- Definição da eficácia dos controles: estabelece critérios objetivos para análise dos controles implementados e para cálculo do risco residual.

II - Identificação de Riscos - etapa em que são identificados possíveis riscos para os objetivos associados aos processos organizacionais. O propósito da identificação de risco é determinar o que pode causar uma perda e deixar claro como, onde e o por que a perda pode acontecer. A identificação de risco devem incluir os riscos cujas fontes estejam ou não sob controle da organização, mesmo que a fonte ou a causa dos riscos não seja evidente.

III - Análise de riscos - etapa que se refere ao desenvolvimento da compreensão sobre o risco e à determinação do nível do risco, que é determinado pela Matriz Probabilidade x Impacto.

- Escala de probabilidade: cada evento de risco deve ser atribuído o grau de probabilidade de ocorrências de risco.

Grau	Probabilidade	Descrição
1	MUITO BAIXA	Sem histórico de ocorrência. O evento poderá ocorrer em situação extraordinária
2	BAIXA	Sem histórico de ocorrência, mas com a possibilidade de o evento acontecer
3	MÉDIA	Há histórico de ocorrência, porém com frequência reduzida
4	ALTA	Há histórico de ocorrência, com alta frequência
5	MUITO ALTA	Há histórico de ocorrência. As circunstâncias apontam evidências de novas ocorrências

Figura 1: escala de probabilidade adotada pelo TJRR

- Escala de impacto: cada evento de risco deve ser atribuído o grau de impacto de ocorrências de risco.

Grau	Impacto	Descrição
1	INSIGNIFICANTE	Não afeta os objetivos / Impactoinsignificante nos objetivos
2	POUCO RELEVANTE	Torna duvidoso seu atingimento / Impacto mínimo nos objetivos
3	RELEVANTE	Torna incerto seu atingimento / Impacto mediano nos objetivos
4	MUITO RELEVANTE	Torna improvável seu atingimento / Impacto significativo nos objetivos
5	CATASTRÓFICO	Capaz de impedir o alcance dos objetivos / Impacto máximo nos objetivos

Figura 2: escala de impacto adotada pelo TJRR

ESCALA DE IMPACTO - ANÁLISE COMPLETA							
NÍVEL	GRAU	ESFORÇO DE GESTÃO	REGULAÇÃO	REPUTAÇÃO	NEGOCIOS/SERVIÇOS A SOCIEDADE	INTERVENÇÃO HIERÁRQUICA	ORÇAMENTO
		13%	16%	11%	23%	6%	31%
1	INSIGNIFICANTE	Evento cujo impacto pode ser absorvido por meio de atividades normais	Pouco ou nenhum impacto	Impacto apenas interno / sem impacto	Pouco ou nenhum impacto nas metas	Seria alcançada no funcionamento normal da atividade	< 1%
2	POUCO RELEVANTE	Evento cujas consequências podem ser absorvidas, mas carecem de esforço da gestão para minimizar o	Determina ações de caráter orientativo	Tende a limitar-se às partes envolvidas	Prejudica o alcance das metas do processo	Exigiria a intervenção do Coordenador	> = 1% < 3%
3	RELEVANTE	Evento significativo que pode ser gerenciado em circunstâncias normais	Determina ações de caráter corretivo	Pode chegar à mídia provocando a exposição por um curto período de tempo	Prejudica o alcance dos objetivos estratégicos	Exigiria a intervenção do Secretário	> = 3% < 10%
4	MUITO RELEVANTE	Evento crítico, mas que com a devida gestão pode ser suportado.	Determina ações de caráter pecuniários (multas)	Com algum destaque na mídia nacional, provocando exposição significativa.	Prejudica o alcance da missão da Unidade	Exigiria a intervenção do Secretário-Geral	> = 10% < 25%
5	CATASTRÓFICO	Evento com potencial para levar o negócio ou serviço ao colapso	Determina interrupção das atividades	Com destaque na mídia nacional e internacional, podendo atingir os objetivos estratégicos e a missão	Prejudica o alcance da missão do TJRR	Exigiria a intervenção do Presidente	> = 25%

Figura 3: escala de impacto baseada em categorias adotada pelo TJRR

- Nível de Riscos

A magnitude do risco é chamada de nível de risco que advém da multiplicação do Grau de Probabilidade (GP) pelo Grau de Impacto (GI) atribuído a cada evento de risco identificado.

A este primeiro resultado dá-se o nome de Nível de Risco Inerente (NRI), que quer dizer o nível de risco a que um processo de trabalho está exposto, sem considerar os controles já existentes ou a aplicação de algum tratamento, conforme a fórmula abaixo:

NRI = GP x GI
NRI = nível do risco inerente
GP = grau de probabilidade
GI = grau de impacto

O produto entre o valor do nível do risco inerente e o fator de avaliação dos controles é denominado Nível do Risco Residual (NRR), nos termos abaixo:

NRR = NRI x FC
NRR = nível do risco residual
NRI = nível do risco inerente
FC = fator de avaliação dos controles

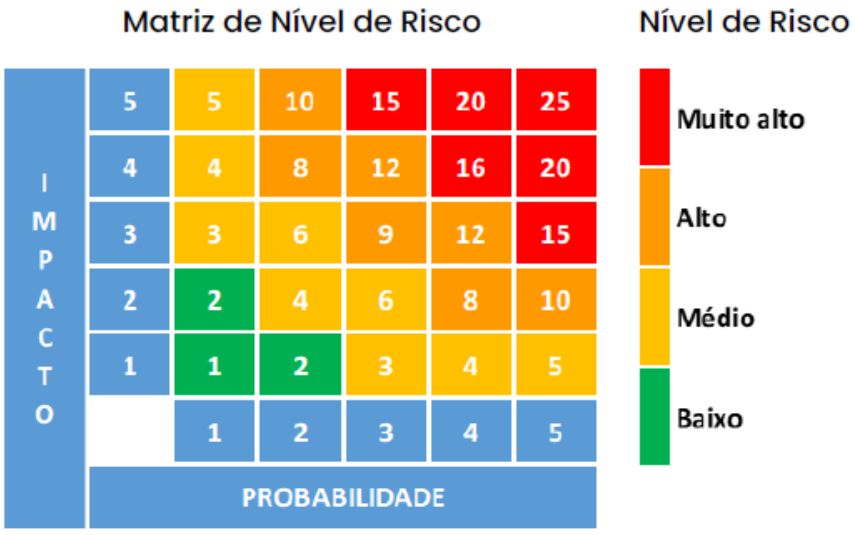

Figura 4: Matriz de nível de risco inerente adotada pelo TJRR

IV – Avaliação de Riscos – etapa em que são estimados os níveis dos riscos identificados, a fim de determinar se o risco é aceitável.

O limite de exposição a riscos representa o nível de risco acima do qual é desejável o tratamento do risco. Espera-se que, com os resultados do tratamento, o nível de risco residual fique abaixo do limite de exposição.

V – Tratamento de Riscos – etapa em que são definidas as respostas aos riscos, de forma a adequar seus níveis ao apetite estabelecido para os processos organizacionais, além da escolha das medidas de controle associadas a essas respostas.

As opções de tratamento de riscos são:

- Evitar o risco: atuar com o objetivo de impedir o início ou provocar a descontinuação das atividades que geram os riscos, ao intervir diretamente em suas causas (fonte de risco), o que elimina a possibilidade de ocorrência do risco;
- Compartilhar o risco: reduzir a probabilidade ou o impacto dos riscos pela transferência ou compartilhamento com outra parte interessada, de uma porção do risco, por exemplo, com a contratação de um seguro;
- Mitigar o risco: adotar medidas para reduzir o impacto ou a probabilidade de ocorrência do risco;
- Aceitar o risco: aceitar ou tolerar o risco sem que nenhuma ação específica seja tomada, pois ou o nível do risco é considerado baixo ou a capacidade da organização para tratar o risco é limitada ou o custo é desproporcional ao benefício.

VI - Aceitação de Riscos - etapa em que se aceita ou tolera o risco sem que nenhuma ação específica seja tomada, pois ou o nível do risco é considerado baixo ou a capacidade da organização para tratar o risco é limitada ou o custo é desproporcional ao benefício.

A elaboração e a implementação do Plano de Tratamento de Riscos deve levar em consideração:

- A eficácia das ações já existentes.
- As restrições organizacionais, técnicas e estruturais.
- Os requisitos legais.
- A análise custo/benefício.
- As ações a serem realizadas.
- Os responsáveis.
- As prioridades.
- Os prazos de execução.

VII - Comunicação e Consulta do Risco - etapa que ocorre durante todo o processo de gerenciamento de riscos e é responsável pela integração de todas as instâncias envolvidas.

VII - Monitoramento do Risco - etapa que ocorre durante todo o processo de gerenciamento de riscos onde os riscos são monitorados e analisados criticamente, a fim de se identificar, o mais rapidamente possível, eventuais mudanças de contexto da organização e de se manter uma visão geral dos riscos.

FLUXOGRAMA DO PROCESSO DE AVALIAÇÃO DE RISCOS

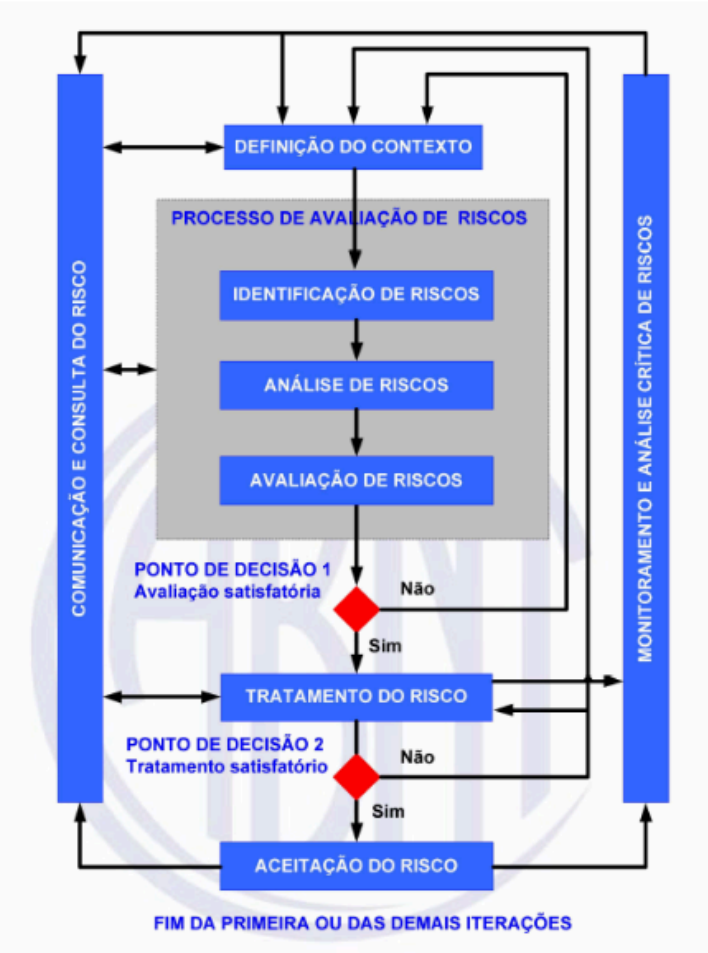

Figura 5: O processo de Gestão de Riscos de TIC - Fonte: ABNT NBR 27005:2019

4. MODELOS DE DOCUMENTOS

Escopo da Gestão de Riscos

Processo de Trabalho:	Elaborado por (Equipe): Data:
Objetivo do Processo de Trabalho:	Analisado por: Data:
Descrição das etapas do Processo/Projeto:	Referências documentais:
Partes Interessadas	

Análise dos ambientes interno e externo

AMBIENTE INTERNO

Forças:	***Fraquezas:***
S	W
O	T
Oportunidades:	***Ameaças:***

AMBIENTE EXTERNO

Riscos relacionados

ID	ETAPA	EVENTO DE RISCOS	CAUSAS	CONSEQUÊNCIAS

Mapa de Riscos - Análise Completa

ANÁLISE DOS RISCOS - NRR			
CONTROLES EXISTENTES preventivos	CONTROLES EXISTENTES contingenciais	FATOR DE CONTROLE	CLASSIFICAÇÃO DE NRR

Mapa de Riscos - Análise Completa

AVALIAÇÃO E TRATAMENTO						
RESPOSTA	AÇÃO DE MITIGAÇÃO/MELHORIA preventiva/contingencial	RESPONSÁVEL	PREVISÃO DE INÍCIO	PREVISÃO DE TÉRMINO	QUEM DEVE SER COMUNICADO(A)	FREQUÊNCIA DE COMUNICAÇÃO

Plano de Ação para o Tratamento dos Riscos

Ordem de Criticidade	Evento de Risco	Gestor do Risco	Controle		Ação	Responsável pela Ação	Início previsto	Previsão de Término	% de Conclusão	Data real de conclusão
				1						
				2						
				3						
				4						
				5						
				6						
				7						
				8						
				9						
				10						
				1						
				2						
				3						
				4						
				5						

Plano de comunicação

COMUNICAÇÃO E CONSULTA				
UNIDADE A SER COMUNICADA	RESPONSÁVEL PELA COMUNICAÇÃO	MÉTODO DE COMUNICAÇÃO	OBJETO DA COMUNICAÇÃO	FREQUÊNCIA

Controle dos Registros

REGISTRO E RELATO		
AUTORIDADE RESPONSÁVEL / PARTE INTERESSADA	DECISÃO TOMADA	PROCESSO SEI

Monitoramento

MONITORAMENTO							
NÍVEL DE RISCO RESIDUAL	RESPONSÁVEL PELA MITIGAÇÃO DO RISCO	CONTROLE EM IMPLEMENTAÇÃO	DATA DE INÍCIO	DATA DE FIM	STATUS DE IMPLEMENTAÇÃO DOS CONTROLES	EXPECTATIVA DE NÍVEL DE RISCO APÓS OS CONTROLES	OCORRÊNCIA

5. CONCLUSÃO

A crescente demanda por serviços públicos de qualidade, agilidade e transparência exige que as organizações públicas adotem estratégias eficazes. Nesse contexto, a gestão de riscos se destaca como um diferencial estratégico, ao contribuir para o aprimoramento das operações e o atendimento às expectativas da sociedade.

Sua principal função é reduzir perdas e impactos negativos, além de identificar oportunidades para viabilizar projetos e alcançar resultados sustentáveis. Para isso, é fundamental que as organizações estejam preparadas para diagnosticar, priorizar, tratar e monitorar riscos, considerando as constantes mudanças no ambiente interno e externo.

Embora sempre haja um grau de risco residual, devido à escassez de recursos e à incerteza inerente às atividades, a gestão eficaz desses riscos reduz surpresas e prejuízos.