



TRIBUNAL REGIONAL ELEITORAL DO RIO GRANDE DO NORTE
SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO E ELEIÇÕES

PLANO DE GESTÃO DE RISCOS DE TECNOLOGIA DA INFORMAÇÃO

(Versão 2.0)

Abril/2026

SUMÁRIO

1. INTRODUÇÃO	3
2. CONCEITOS E DEFINIÇÕES	4
3. DOCUMENTOS DE REFERÊNCIA	4
4. METODOLOGIA	4
5. FORMAS E FERRAMENTAS PARA ANÁLISE DE RISCOS	5
5.1. Gerenciamento de projetos	6
5.2. Gerenciamento de ativos de tecnologia da informação	6
5.3. Gerenciamento de contratações	7
5.4. Análise de riscos de Segurança da Informação	8
5.5. Gestão e Governança	8
5.6. Eleitoral	9
6. PROCESSO PARA GESTÃO DE RISCOS	10

1. INTRODUÇÃO

O Plano de Gestão de Riscos de Tecnologia da Informação é um instrumento complementar de diagnóstico, planejamento e gestão dos riscos, fundamental para a continuidade dos processos internos da Secretaria de Tecnologia da Informação e Eleições.

A Resolução nº 370/2021 do CNJ, que estabelece a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD), para o período 2021 a 2026, instituiu no art. 37 que “Cada órgão deverá elaborar Plano de Gestão de Riscos de TIC, com foco na continuidade de negócios, manutenção dos serviços e alinhado ao plano institucional de gestão de riscos, objetivando mitigar as ameaças mapeadas para atuar de forma preditiva e preventiva às possíveis incertezas.”

O plano segue a Resolução TRE-RN nº 17/2017, que instituiu a Política de Gestão de Riscos da Justiça Eleitoral do Rio Grande do Norte e considera pontos particulares de Tecnologia da Informação, além de planejar quais processos devem ser gerenciados sob a metodologia do Tribunal.

Como artefato importante no planejamento estratégico da Secretaria de Tecnologia da Informação e Eleições do TRE-RN, o plano de gestão de riscos de TI guiará os gestores e suas equipes na identificação, análise, registro, comunicação e tratamento de riscos que permeiam as ações, projetos e os processos da Secretaria.

São premissas do plano:

- transparência
- relevância
- previsibilidade e auxílio na tomada de decisão
- redução de custos com ações corretivas
- aumento da satisfação dos usuários
- revisão e melhoria contínua
- inovação

- sustentabilidade
- conformidade
- auditabilidade

2. CONCEITOS E DEFINIÇÕES

Para um melhor entendimento deste plano, serão utilizados os conceitos e definições compilados no item 4 da Resolução TRE-RN nº 17/2017, que instituiu a **Política de Gestão de Riscos da Justiça Eleitoral do Rio Grande do Norte**.

3. DOCUMENTOS DE REFERÊNCIA

- Resolução TRE-RN nº 17/2017;
- Norma ABNT NBR ISO 31000:2009;
- Resolução CNJ 370/2021;
- Resolução CNJ 396/2021;
- Portaria CNJ 162/2021;

4. METODOLOGIA

A base metodológica utilizada segue as etapas preconizadas no **Manual do Processo de Gestão de Riscos da Justiça Eleitoral do Rio Grande do Norte** (anexo da Resolução nº 17/2017-TRE/RN):

- Planejar o Gerenciamento dos Riscos
- Identificar os riscos;
- Realizar a Análise Qualitativa dos riscos;
- Realizar a Análise Quantitativa dos riscos;
- Planejar as Respostas aos Riscos;
- Monitorar e Controlar os Riscos.

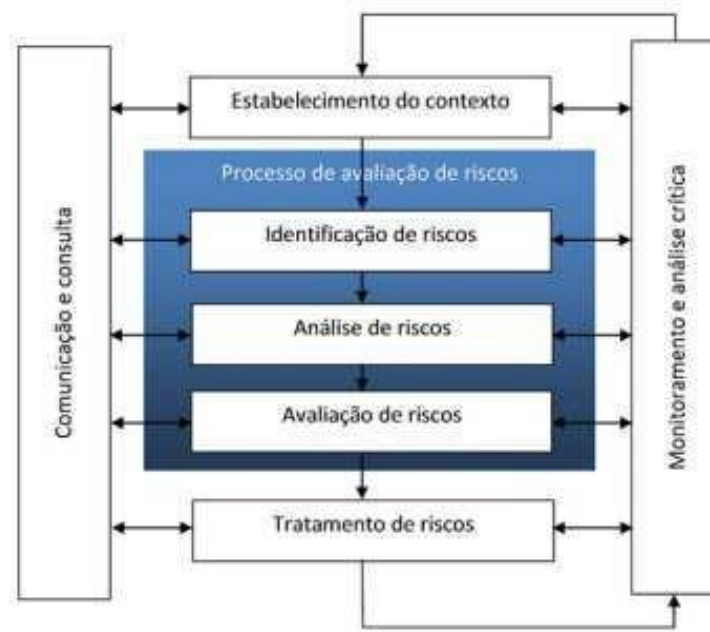


Figura 1 – Processo de gestão de riscos

5. FORMAS E FERRAMENTAS PARA ANÁLISE DE RISCOS

Conforme o contexto onde a análise de riscos será realizada, poderá haver uma variação do uso da base metodológica descrita no item anterior, bem como diferentes formas e ferramentas de se chegar a identificação do valor do risco e formas de mitigação.

A metodologia em vigor classifica os riscos em:

- Operacionais
- De aquisição
- De Orçamento
- De Imagem
- Organizacionais
- Estratégicos
- De Segurança da informação
- De partes interessadas
- De Integridade

Na STIE, foram identificados 6 contextos ou áreas temáticas com características a

considerar no levantamento e gerenciamento de riscos:

- Riscos no gerenciamento de projetos
- Riscos no gerenciamento de ativos (hardware e software)
- Riscos no gerenciamento de contratações (aquisições)
- Riscos de Segurança da Informação
- Riscos de Gestão e Governança
- Riscos Eleitorais

O tratamento dos riscos deve sempre considerar medidas preventivas, bem como de contingência.

O monitoramento contínuo deve ocorrer para validação das medidas previstas para mitigação dos riscos e retroalimentar o processo.

De forma a se garantir o aprimoramento contínuo, é crucial o informe de ocorrência dos riscos para se avaliar as medidas previstas e revisar periodicamente a análise e tratamento.

5.1- Gerenciamento de projetos

Riscos no gerenciamento de projetos devem considerar:

- ciclo de vida e artefatos
- melhores práticas
- ferramentas e continuidade
- formas de gerenciamento
- responsabilidades
- mudanças na equipe
- repriorização
- contratempos
- custos
- impacto na descontinuidade
- mudanças no projeto

5.2 - Gerenciamento de ativos de tecnologia da informação

Os ativos de TI compreendem itens de hardware, software e pessoas.

Os riscos relativos aos ativos de tecnologia da informação dizem respeito às atividades relacionadas à forma com a qual uma instituição lida com os riscos que seus ativos podem sofrer.

No levantamento de riscos nessa área, devem ser considerados:

- a correta identificação do ativo
- seu ciclo de vida
- acesso / segurança
- manutenção
- descarte
- impacto na descontinuidade
- interrupção técnica programada / indisponibilidade
- mudanças
- danos
- acidentes
- contratempos
- atualização

5.3 - Gerenciamento de contratações

Nas contratações, deve-se considerar, entre outros itens:

- indisponibilidade orçamentária: não contratação imediata, atraso no cronograma
- atraso no trâmite processual: atraso na contratação da solução, atraso no cronograma
- impugnação improcedente: interrupção do processo de contratação, atraso no cronograma, frustração da contratação
- licitação frustrada (deserta/fracassada): interrupção do processo de contratação, atraso no cronograma, frustração da contratação
- licitação anulada: interrupção do processo de contratação, atraso no cronograma, frustração da contratação

- solução considerada inadequada pela área demandante: insatisfação do usuários dos serviços de TIC, não utilização da solução, necessidade de nova avaliação de solução
- não cumprimento do prazo de entrega: atraso na instalação/implementação da solução
- entrega de solução incompatível (especificações): ineficácia na execução dos serviços prestados pelo órgão
- descrição correta dos itens
- economicidade
- soluções de contingência
- indisponibilidade de atualização
- possibilidade de substitutos
- compatibilidade
- sustentabilidade
- acessibilidade

5.4 - Análise de riscos de Segurança da Informação

A análise de riscos na área de segurança da informação deve levar em consideração as constantes ameaças, cujas demandas exigem monitoramento ininterrupto por meio de ferramentas próprias.

O principal objetivo é permitir que o órgão faça uma análise preditiva de todos os processos e situações que ocorrem ou possam ocorrer eventualmente.

Além dessas perspectivas, é crucial considerar o aspecto humano, de forma a se evitar brechas que se aproveitam da engenharia social. Deriva-se, portanto, a necessidade de frequente aperfeiçoamento e divulgação do tema entre o público interno e externo por meio de ações de conscientização e sensibilização.

5.5 - Gestão e Governança

No levantamento de riscos nessa área, devem ser considerados:

- alinhamento estratégico
- conformidade

- avaliação de satisfação
- revisão de instrumentos
- estabelecimento de indicadores e metas
- responsabilidades
- repriorização
- contratempos
- economia
- impacto na descontinuidade
- pedidos de mudanças

5.6 - Eleitoral

O contexto eleitoral possui diversas variáveis a considerar, sobretudo:

- mudanças normativas
- treinamento
- responsabilidades
- mudanças na equipe
- repriorização
- plano de contingência
- prazos eleitorais
- inovação

6 PROCESSO PARA GESTÃO DE RISCOS

Com base na modelagem dos processos de trabalho, foram determinados quais devem ser submetidos à gestão de riscos:

ID	Classe do Risco	Processo	Unidade Responsável	Situação Atual	Validade da análise de risco do processo	Prazo para revisar ou realizar a análise de risco
1	Operacional	Planejamento Orçamentário e das Contratações de TIC do TRE/RN (mudança do nome)	GAPSTIE	A Revisar	2019 (Processo revisado em abr/2026)	Junho/2026
2	Operacional	Gerenciamento de Incidentes de TIC (versão 1.1)	SSI/COINF	Revisado SEI Nº 6844/2020 Análise de risco aprovada pelo CGRISCO em 26.09.2025	Setembro/2027.	Julho/2027
3	Operacional	Gerenciamento de Cópias de Segurança (backup) e de Restauração de Dados.	SRI/COINF	A Revisar SEI Nº 3554/2024 Análise de risco aprovada pelo CGRISCO em 03.05.2023	Março/2025	Junho/2026
4	Operacional	Solicitação de demandas de sistemas	COSIS	A Revisar SEI Nº 3551/2024 Análise de risco aprovada pelo e CGRISCO em 03.05.2023	Março/2025	Julho/2026
5	Estratégico	Atividades da SSAE no zoneamento	SSAE/COELE	A Revisar SEI nº	Março/2025	Dezembro/2026

ID	Classe do Risco	Processo	Unidade Responsável	Situação Atual	Validade da análise de risco do processo	Prazo para revisar ou realizar a análise de risco
		SEI 03557/2024 (processo da análise de riscos está na SSAE/COELE)		03557/2024 Análise de risco aprovada pelo CGRISCO em 03.05.2023		
6	Operacional	Gerenciamento de escopo e requisitos	COSIS	A Revisar SEI nº 03582/2024 Análise de risco aprovada pelo CGRISCO em 10.11.2021	Novembro/2023	Julho/2026
7	Estratégico	Preparação e treinamento nos sistemas eleitorais	SSAE/COELE	Revisado SEI nº 7048/2024 Análise de risco aprovada pelo CGRISCO em 10.11.2021	Novembro/2023	Junho/2026
8	Estratégico	Urnas eletrônicas - Manutenção preventiva	SUE/COELE	Revisado SEI nº 03583/2024 Análise de risco aprovada pelo COGESTIC em 12.06.2025 e CGRISCO em 26.09.2025	Setembro/2027	Julho/2027
9	Estratégico	Elaboração do Plano Integrado de Eleições (PIELEI)	COELE	A iniciar	-	Julho/2027
10	Operacional	Elaboração e Gestão do Plano de Capacitação de TIC	GAPSTIE	Revisado SEI 3593/2024	Novembro/2025	Mai/2026

ID	Classe do Risco	Processo	Unidade Responsável	Situação Atual	Validade da análise de risco do processo	Prazo para revisar ou realizar a análise de risco
				Análise de risco aprovada pelo CGRISCO em 28.11.2023		
11	Estratégico	Urnas Eletrônicas - Manutenção corretiva durante o período eleitoral	SUE/COELE	Revisado SEI nº 03587/2024 Análise de risco aprovada pelo COGESTIC em 12.06.2025 e CGRISCO em 26.09.2025	Setembro/2027	-
12	Operacional	Gerenciamento da Central de Serviços de TIC	SMI/COINF	A Revisar SEI nº 3968/2024 Análise de risco aprovada pelo CGRISCO em 28.11.2023	Novembro/2025	Agosto/2026
13	Operacional	Gerenciamento da Rede de Comunicação de Dados	SRI/COINF	A Revisar SEI nº 3581/2024 Análise de risco aprovada pelo CGRISCO em 03.05.2023	Março/2025	Agosto/2026
14	Operacional	Gerenciamento da Base de Usuários	SSI/COINF	A Revisar SEI 595/2024 Análise de risco aprovada pelo COGESTIC em janeiro/2024	Aguardando aprovação pelo CGRISCO	-
15	Operacional	Gerenciamento da Base de	SMI/COINF	Aguardando aprovação	Encaminhar para aprovação	Mai/2026 (encaminhar)

ID	Classe do Risco	Processo	Unidade Responsável	Situação Atual	Validade da análise de risco do processo	Prazo para revisar ou realizar a análise de risco
		Conhecimento de TIC		SEI 595/2024 Análise de risco aprovada pelo COGESTIC em janeiro/2024	pelo CGRISCO, após ajustes pela unidade técnica	
16	Operacional	Gerenciamento de Problemas de TIC	SMI/COINF	A Iniciar	-	Agosto/2026
17	Operacional	Gerenciamento de Capacidade de TIC	SRI/COINF	Aguardando aprovação Análise de risco aprovada pelo COGESTIC em outubro/2025	Encaminhar para aprovação pelo CGRISCO	Abril/2026 (encaminhar)
18	Operacional	Gerenciamento de Controle de Acesso Lógico	SRI/COINF	A Iniciar	-	Agosto/2026
19	Operacional	Gerenciamento de Disponibilidade de TIC	SRI/COINF	Aguardando aprovação Análise de risco aprovada pelo COGESTIC em novembro/2025	Encaminhar para aprovação pelo CGRISCO	Abril/2026 (encaminhar)
20	Operacional	Recebimento de Ativos de TIC	SMI/COINF	Aguardando aprovação Análise de risco aprovada pelo COGESTIC em maio/2025	Aguardando aprovação pelo CGRISCO	-