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

PLANO DE GESTÃO DE RISCOS DE TECNOLOGIA DA INFORMAÇÃO

Agosto/2023

COMPOSIÇÃO DO PLENO DO

TRIBUNAL REGIONAL ELEITORAL DO RIO GRANDE DO NORTE

Desembargador Cornélio Alves
Presidente

Desembargador Expedito Ferreira
Vice-Presidente e Corregedor Regional Eleitoral

Juiz Fábio Luiz de Oliveira Bezerra

Juíza Maria Neíze de Andrade Fernandes

Juíza Ticiana Maria Delgado Nobre

Juiz Fernando de Araújo Jales Costa

Juiz Daniel Cabral Mariz Maia

Gilberto Barroso de Carvalho Júnior
Procurador Regional Eleitoral

Sumário

Introdução
Conceitos e definições
Documentos de Referência
Metodologia
Formas e Ferramentas para Análise de Riscos
Processos para gestão de riscos

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

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**.

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;

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.

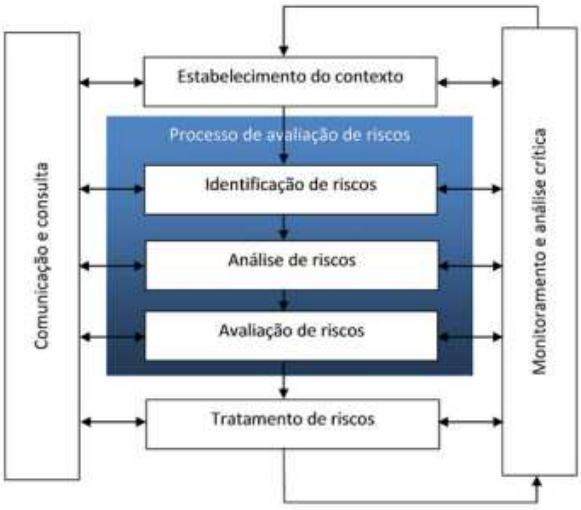

Figura 1 – Processo de gestão de riscos

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

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

Processos para gestão de riscos

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

Id	Processo	Situação	Histórico	Instituído em/ Previsão
01	Elaboração e Gestão do Plano de Contratações de Soluções de TIC	Em revisão	Enviado PAE 11709/2019 para EPOR. Em análise pelo GAPSTIE	2019
02	Gerenciamento de Incidentes de TIC	Em vigor	Enviado PAE 6844/2020 para EPOR. Aprovado pelo CGR em 15/09/2021. Em análise pelo EPOR, da revisão realizada em 2023 pela SSI/COINF/STIE. Aguardando a SSI realizar os ajustes da revisão, solicitados pelo EPOR.	2020
03	Gerenciamento de Cópias de Segurança (backup) e de Restauração de Dados	Em vigor	Enviado PAE 6844/2020 para EPOR. Aprovado pelo CGR em 03/05/2023.	2020
04	Solicitação de demandas de sistemas	Em vigor	Enviado PAE 6844/2020 para EPOR. Aprovado pelo CGR em 03/05/2023.	2020

05	Atividades da SSAE no rezoneamento	Em vigor	Enviado PAE 6844/2020 para EPOR. Aprovado pelo CGR em 03/05/2023.	2020
06	Gerenciamento de escopo e requisitos	Em revisão	Enviado PAE 7830/2021 para EPOR. Em análise pela SDS/COSIS	2021
07	Preparação e treinamento nos sistemas eleitorais	Em revisão	Enviado PAE 7830/2021 para EPOR. Em análise pela SUE/COELE	2021
08	Urnas eletrônicas - Manutenção preventiva	Em vigor	Enviado PAE 7830/2021 para EPOR. Aprovado pelo CGR em 03/05/2023	2021
09	Gerenciamento de cópias de segurança (Backup) e de restauração de dados	Em vigor	Enviado PAE 6844/2020 para EPOR. Aprovado pelo CGR em 03/05/2023.	2021
10	Elaboração do Plano Integrado de Eleições (PIELEI)	Não analisados os riscos	Aguardando a conclusão da revisão do processo do PIELEI para realizar a análise de riscos.	2021
11	Elaboração e Gestão do Plano de Capacitação de TIC	Validado pelo COGESTIC	Enviado PAE 4556/2023 para EPOR. Em análise pelo EPOR.	2022
12	Urnas Eletrônicas - Manutenção corretiva durante o período eleitoral	Em vigor	Enviado PAE 1983/2022 para EPOR. Aprovada pelo CGR em 03/05/2023.	2022
13	Gerenciamento da Central de	Validado	Enviado PAE 3632/2023 para	

	Serviços de TIC	pelo COGESTIC	EPOR. Aguardando aprovação pelo CGR.	2022
14	Gerenciamento da Rede de Comunicação de Dados	Em vigor	Enviado PAE 7830/2021 para EPOR. Aprovada pelo CGR em 03/05/2023.	2022
15	Gerenciamento da Base de Usuários	Não analisados os riscos	Reagendado para 31/07/2023	2023
16	Gerenciamento da Base de Conhecimento	Não analisados os riscos	Reagendado para 31/07	2023
17	Gerenciamento de Problemas de TIC	Não analisados os riscos	-	2024
18	Gerenciamento de Capacidade de TIC	Não analisados os riscos	-	2025
19	Gerenciamento de Controle de Acesso Lógico	Não analisados os riscos	-	2025
20	Gerenciamento de Disponibilidade de TIC	Não analisados os riscos	-	2026