TRIBUNAL REGIONAL ELEITORAL DO RIO GRANDE DO NORTE
GABINETE DA PRESIDÊNCIA

PORTARIA N.° 232/2023 – GP

Dispõe sobre as regras e os procedimentos para gestão de riscos de segurança da informação do Tribunal Regional Eleitoral do Rio Grande do Norte.

O DESEMBARGADOR-PRESIDENTE DO TRIBUNAL REGIONAL ELEITORAL DO RIO GRANDE DO NORTE, no uso das atribuições que lhe são conferidas pelo artigo 20, inciso XIX, da Resolução nº 09/2012 - TRE/RN, e

CONSIDERANDO a necessidade de apoiar a gestão dos riscos de segurança da informação do TRE/RN, cuja avaliação periódica é condição para implementação e operação do SGSI – Sistema de Gestão de Segurança da Informação;

CONSIDERANDO a Resolução CNJ n.º 370/2021, que estabelece a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD);

CONSIDERANDO a Resolução CNJ nº 396/2021, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);

CONSIDERANDO a Resolução TRE/RN nº 110/2023, que institui a Política de Segurança da Informação (PSI) no âmbito do Tribunal Regional Eleitoral do Rio Grande do Norte;

CONSIDERANDO a Portaria DG/TSE nº 444/2021, que dispõe sobre a instituição da norma de termos e definições relativas à Política de Segurança da Informação do Tribunal Superior Eleitoral;

CONSIDERANDO as boas práticas em segurança das informações previstas nas normas ABNT ISO/IEC 27001 e ABNT NBR ISO/IEC 27002;

CONSIDERANDO as boas práticas em gestão de riscos de segurança cibernéticos na norma ABNT ISO/IEC 27005 versão 2019 baseada no Processo de Gestão de Riscos estabelecido na ISO 31:000:2018;

CONSIDERANDO a necessidade de gerenciar os riscos que envolvem o tratamento de dados pessoais, de acordo com a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados); e

CONSIDERANDO que a segurança da informação e a proteção de dados pessoais são condições essenciais para a prestação dos serviços

jurisdicionais e administrativos do Tribunal Regional Eleitoral do Rio Grande do Norte, e tendo em vista o que consta no Processo PAE nº 10.487/2023;

RESOLVE:

CAPÍTULO I
DISPOSIÇÕES PRELIMINARES

Art. 1º A Gestão de Riscos de Segurança da Informação, adotada pelo Tribunal Regional Eleitoral do Rio Grande do Norte, observará as disposições contidas nesta norma.

Art. 2º Esta norma integra a Política de Segurança de Informação da Justiça Eleitoral do TRE/RN.

Art. 3º Entende-se por risco de segurança da informação todo evento que possa afetar a integridade, a confidencialidade, a disponibilidade ou a autenticidade da informação e dos dados pessoais custodiados pela Justiça Eleitoral do Rio Grande do Norte.

Art. 4º A Gestão de Riscos de Segurança da Informação é orientada pela Política de Gestão de Riscos deste Tribunal, instituída pela Resolução TRE/RN nº 17/2017.

Art. 5º Deverão ser analisados os riscos de segurança da informação, antes da implementação, aquisição ou contratação:

I - dos ativos de tecnologia da informação;

II - dos processos de trabalho executados no Tribunal.

CAPÍTULO II
DAS DEFINIÇÕES GERAIS E CONCEITOS TÉCNICOS

Art. 6º Para efeitos desta norma consideram-se os termos e definições relativos à Política de Segurança da Informação do Tribunal Superior Eleitoral previstos na Portaria DG/TSE nº 444/2021, além dos seguintes:

I - Contexto Externo - Conjunto de circunstâncias a que o risco de segurança da informação está associado, com perspectiva focada na sociedade.

II - Contexto Interno - Conjunto de circunstâncias a que o risco de segurança da informação está associado, com perspectiva focada apenas no ambiente interno da instituição.

III - Proprietário do Risco - unidade responsável pelo ativo ou processo de negócio a que o risco se refere.

Art. 7º Esta norma segue as diretrizes da norma ABNT ISO/IEC 27005:2019, na implementação e na operação do Sistema de Gestão de Segurança da Informação.

Art. 8º Considere-se, no que couber, a Política de Gestão de Riscos do TRE-RN, de acordo com a Resolução TRE/RN nº 17/2017.

Art. 9º São considerados gestores de riscos os responsáveis pelas unidades organizacionais do TRE-RN, o gestor de segurança da informação e os gestores responsáveis pelos serviços essenciais de TIC.

Art. 10. Os novos sistemas de informação, sejam estes desenvolvidos internamente, obtidos de outras instituições ou adquiridos de fornecedor externo, deverão passar por análise de riscos de segurança da informação antes de sua implementação.

CAPÍTULO III
DA DEFINIÇÃO DO CONTEXTO DO RISCO

Art. 11. Para a definição do escopo devem ser considerados os fatores humanos, tecnológicos, organizacionais e de imagem da Justiça Eleitoral, além da:

I - Identificação dos ativos de informação;
II - Identificação das ameaças;
III - Identificação das vulnerabilidades;
IV - Proteção de dados pessoais, de acordo com a LGPD;
V - Identificação das partes interessadas.

CAPÍTULO V
DO PROCESSO DE AVALIAÇÃO DO RISCO

Art. 12. O processo de avaliação do risco deve seguir os seguintes passos:

I - Identificação: Reconhecimento do contexto, dos ativos, das ameaças e das vulnerabilidades, dos controles existentes, no que tange à integridade, a disponibilidade e a confidencialidade da informação, independente da fonte ou causa do risco estar ou não sob o controle da organização.

II - Análise: A análise do risco deve levar em conta a criticidade dos ativos de informação, a extensão das vulnerabilidades conhecidas e dos incidentes anteriores registrados.

III - Avaliação: A avaliação do risco se dará pela comparação da tabela de impacto x probabilidade com o apetite ao risco estabelecido pela organização, definindo as medidas de tratamento aplicáveis.

Art. 13. Para a análise qualitativa do risco, considera-se o apetite ao risco o grau máximo de 12 (médio), em escala de 25 pontos.

CAPÍTULO V
DO TRATAMENTO DO RISCO

Art. 14. O tratamento do risco elaborado após criteriosa avaliação, deverá atuar para modificar, reter, compartilhar ou evitar os riscos, por meio de controles e ações adequados.

CAPÍTULO VI
DA ACEITAÇÃO DO RISCO

Art. 15. A aceitação do risco residual, o qual esteja além do limite do apetite ao risco definido, deverá ser feito por autoridade, após análise e parecer do Comitê Gestor de Segurança da Informação.

CAPÍTULO VII
DA COMUNICAÇÃO E CONSULTA DO RISCO

Art.16. Os riscos deverão ser comunicados e compartilhados entre as partes interessadas.

CAPÍTULO VIII
DO MONITORAMENTO E ANÁLISE CRÍTICA DO RISCO

Art. 17. O monitoramento e análise crítica dos riscos em segurança da informação deverá ser efetuada pelo gestor de segurança da informação e pelo Comitê Gestor de TIC, por meio de subsídios a serem encaminhados pelas áreas proprietárias do risco.

Art. 18. Os riscos elencados devem ser reavaliados com periodicidade mínima anual.

Art.19. Os riscos de segurança da informação devem ser monitorados, preferencialmente, por meio de solução informatizada de GRC (governança, risco e conformidade), permitindo o acesso às partes interessadas e à alta administração.

Parágrafo Único. Na impossibilidade de adoção de sistema informatizado para monitoramento dos riscos devem ser adotados controles manuais, cujo controle ficará a cargo do Comitê Gestor de TIC .

CAPÍTULO IX
DISPOSIÇÕES FINAIS

Art. 20. A Seção de Segurança da Informação e o Gestor de Segurança da Informação apoiarão as demais unidades organizacionais quando da elaboração da análise de riscos de segurança da informação.

Art. 21. Os casos omissos serão resolvidos pelo Comitê Gestor de Segurança da Informação ou pelo Comitê Gestor de Proteção de Dados Pessoais, de acordo com o tipo de risco elencado.

Art. 22. Qualquer descumprimento desta norma deve ser imediatamente comunicado e registrado pelo Gestor de Segurança da Informação, com consequente adoção das providências cabíveis.

Art. 23. Esta norma complementar deverá ser revisada a cada 24 meses e encaminhada para nova apreciação do Comitê Gestor de Segurança da Informação.

Art. 24. Esta Portaria entra em vigor na data de sua publicação e sua implementação inicia-se imediatamente.

Natal/RN, 12 de dezembro de 2023.

Desembargador **Cornélio Alves**
Presidente