TRIBUNAL REGIONAL ELEITORAL DO PIAUI

Portaria Presidência Nº 551/2025 TRE/PRESI/DG/ASSDG, de 28 de novembro de 2025

Dispõe sobre as regras e os procedimentos para gestão de riscos de segurança da informação no âmbito do Tribunal Regional Eleitoral do Piauí.

O PRESIDENTE DO TRIBUNAL REGIONAL ELEITORAL DO PIAUÍ, no uso de suas atribuições legais e regimentais,

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

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

CONSIDERANDO a Resolução TSE nº 23.644/2021, que institui a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral;

CONSIDERANDO a Resolução TRE-PI nº 448/2022, que adota no âmbito do Tribunal Regional Eleitoral do Piauí, a Política de Segurança da Informação da Justiça Eleitoral, estabelecida pela Resolução TSE nº 23.644/2021;

CONSIDERANDO a Resolução TRE-PI nº 503/2025 que institui a Política de Gestão de Riscos Corporativos no âmbito do Tribunal Regional Eleitoral do Piauí;

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

CONSIDERANDO as boas práticas em gestão de riscos de segurança da informação previstas na norma ABNT ISO/IEC 27005;

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

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 Piauí; e

CONSIDERANDO a Decisão 1741 (0002580363) proferida no Processo SEI 0016134-80.2025.6.18.8000;

RESOLVE:

CAPÍTULO I

DISPOSIÇÕES PRELIMINARES

Art. 1º. Fica instituída a Portaria para a Gestão de Riscos de Segurança da Informação.

Art. 2º. Esta norma integra a Política de Segurança de Informação da Justiça Eleitoral, estabelecida pela Resolução TSE nº 23.644/2021 e adotada pela Resolução TRE-PI nº 448/2022.

Art. 3º. Considere-se, no que couber, a Política de Gestão de Riscos do TRE-PI, de acordo com a Resolução TRE-PI nº 503/2025.

Art. 4º. São considerados gestores de riscos os responsáveis pelas unidades organizacionais do TRE-PI, o gestor de segurança da informação, o encarregado de dados pessoais e o gestor de continuidade de negócios ou continuidade de serviços essenciais de TI.

Art. 5º. Esta norma segue as diretrizes da norma ABNT ISO/IEC 27005:2019, na implementação e na operação do SGSI (Sistema de Gestão de Segurança da Informação).

Art. 6º. Todos 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 II

DAS DEFINIÇÕES GERAIS

Art. 7º. Para efeitos desta norma consideram-se os termos e definições seguintes:

I - Ameaça: causa potencial de um incidente indesejado que pode resultar em dano para um sistema ou organização;

II - Atividades críticas: atividades precípuas da Justiça Eleitoral cuja interrupção ocasiona severos transtornos, como, por exemplo, perda de prazos administrativos e judiciais, dano à imagem institucional, prejuízo ao Erário, entre outros;

III - Ativo de informação: patrimônio composto por todos os dados e informações gerados, adquiridos, utilizados ou armazenados pela Justiça Eleitoral;

IV - Ativo: qualquer bem, tangível ou intangível, que tenha valor para a organização;

V - Autenticidade: propriedade que garante que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade;

VI - Confidencialidade: propriedade da informação que garante que ela não será disponibilizada ou divulgada a indivíduos, entidades ou processos sem a devida autorização;

VII – Contexto Externo: Conjunto de circunstâncias a que o risco de segurança da informação está associado, com perspectiva focada na sociedade;

VIII – Contexto Interno: Conjunto de circunstâncias a que o risco de

segurança da informação está associado, com perspectiva focada apenas no ambiente interno da instituição;

IX - Continuidade de negócios: capacidade estratégica e tática de um órgão ou entidade de planejar e responder a incidentes e interrupções de negócios, minimizando seus impactos e recuperando perdas de ativos da informação das atividades críticas, de forma a manter suas operações em um nível aceitável, previamente definido;

X - Disponibilidade: propriedade da informação que garante que ela será acessível e utilizável sempre que demandada;

XI - Gestão de Segurança da Informação: ações e métodos que visam à integração das atividades de gestão de riscos, gestão de continuidade de negócios, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e segurança organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando à tecnologia da informação;

XII - Informação: conjunto de dados, textos, imagens, métodos, sistemas ou quaisquer formas de representação dotadas de significado em determinado contexto, independentemente do suporte em que resida ou da forma pela qual seja veiculado;

XIII - Integridade: propriedade que garante que a informação mantém todas as características originais estabelecidas pelo proprietário;

XIV - Irretratabilidade (ou não repúdio): garantia de que a pessoa se responsabilize por ter assinado ou criado a informação;

XV - Proprietário do ativo de informação: refere-se à parte interessada do órgão ou entidade, indivíduo legalmente instituído por sua posição e/ou cargo, o qual é responsável primário pela viabilidade e sobrevivência dos ativos de informação;

XVI - Proprietário do Risco: Unidade Organizacional responsável pelo ativo ou processo de negócio a que o risco se refere;

XVII - Recurso: além da própria informação, é todo o meio direto ou indireto utilizado para o seu tratamento, tráfego e armazenamento;

XVIII - Recursos de Tecnologia da Informação: são o conjunto de bens e serviços de tecnologia da informação que constituem a infraestrutura tecnológica de suporte automatizado ao ciclo da informação, que envolve as atividades de produção, coleta, tratamento, armazenamento, transmissão, recepção, comunicação e disseminação;

XIX - Risco: potencial associado à exploração de vulnerabilidades de um ativo de informação por ameaças, com impacto negativo no negócio da organização;

XX - Segurança da informação: abrange aspectos físicos, tecnológicos e humanos da organização e orienta-se pelos princípios da autenticidade, da confidencialidade, da integridade, da disponibilidade e da irretratabilidade da informação, entre outras propriedades;

XXI - Tecnologia da Informação e Comunicação (TIC): ativo estratégico que suporta processos institucionais, por meio da conjugação de recursos, processos e técnicas utilizados para obter, processar, armazenar, fazer uso e disseminar informações;

XXII- Tratamento da informação: recepção, produção, reprodução,

utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação, inclusive as sigilosas; e

XXIII - Vulnerabilidade: fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.

CAPÍTULO III

DA DEFINIÇÃO DO CONTEXTO DO RISCO

Art. 8º. Para a definição dos contextos externos e internos 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; e

V - Identificação das partes interessadas.

CAPÍTULO IV

DO PROCESSO DE AVALIAÇÃO DO RISCO

Art. 9º. 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 a 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; e

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

Parágrafo único. Caso a análise dos riscos seja quantitativa, caberá à Comissão de Segurança da Informação o aceite do risco no caso concreto.

CAPÍTULO V

DO TRATAMENTO DO RISCO

Art. 11. 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. 12. 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 pela Comissão de Segurança da Informação.

CAPÍTULO VII
DA COMUNICAÇÃO E CONSULTA DO RISCO

Art. 13. Os riscos deverão ser comunicados e compartilhados entre as partes interessadas.

CAPÍTULO VI
DO MONITORAMENTO E ANÁLISE CRÍTICA DO RISCO

Art. 14. O monitoramento e análise crítica dos riscos em segurança da informação deverá ser efetuada pelo Gestor de Segurança da Informação e pela Comissão de Segurança da Informação, por meio de subsídios a serem encaminhados pelas áreas proprietárias do risco.

Art. 15. Os riscos elencados devem ser reavaliados com periodicidade mínima anual.

Art. 16. 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 Gestor de Segurança da Informação.

CAPÍTULO VII
DISPOSIÇÕES FINAIS

Art. 17. O responsável pela área responsável pela Segurança Cibernética e o Gestor de Segurança da Informação apoiarão as demais unidades organizacionais quando da elaboração da análise de riscos de segurança da informação.

Art. 18. Os casos omissos serão resolvidos pela Comissão de Segurança da Informação ou pelo Comitê Gestor de Proteção de Dados Pessoais, de

acordo com o tipo do risco elencado.

Art. 19. Qualquer descumprimento desta norma deve ser imediatamente comunicado e registrado pelo Gestor de Segurança da Informação, com consequente adoção das providências cabíveis.

Art. 20. Esta norma complementar deverá ser revisada a cada 12 (doze) meses pelo Gestor de Segurança da Informação e encaminhada para nova apreciação da Comissão de Segurança da Informação.

Art. 21. Esta Portaria entra em vigor na data de sua publicação e sua implementação inicia-se imediatamente.

Desembargador SEBASTIÃO RIBEIRO MARTINS

Presidente do TRE-PI

Documento assinado eletronicamente por **Sebastião Ribeiro Martins**, **Presidente**, em 28/11/2025, às 19:32, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.tre-pi.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0002580366** e o código CRC **B2C8C640**.