

**TRIBUNAL REGIONAL ELEITORAL DO RIO GRANDE DO NORTE  
GABINETE DA PRESIDÊNCIA****PORTARIA N° 240/2023 - GP**

Dispõe sobre o Desenvolvimento Seguro de Sistemas 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 definir processos de continuidade de serviços de TI, em caso de eventos de causas naturais, acidentais, tecnológicas ou humanas;

CONSIDERANDO a Res. CNJ 396/2021, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);

CONSIDERANDO a Res. TSE 23.344/2021, que institui a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral;

CONSIDERANDO a portaria DG/TSE 444/2021, que dispõe sobre a instituição da norma de termos e definições relativa à Política de Segurança da Informação do Tribunal Superior Eleitoral;

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

CONSIDERANDO a necessidade de implementar controles para o tratamento de dados pessoais de acordo com a lei 13.709/2018 (LGPD);

CONSIDERANDO as boas práticas na gestão da continuidade de negócios previstas nas normas ABNT ISO/IEC 22303 e 22313;

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 C desenvolvimento seguro de sistemas do TRE/RN, complementar à Política de Segurança da Informação, com intuito de estabelecer padrões de segurança no desenvolvimento de software, observará as disposições contidas nesta portaria.

### CAPÍTULO II DAS DEFINIÇÕES

Art. 2º Para os efeitos da presente norma, aplicam-se os termos e definições conceituados na Portaria TSE nº 444, de 8 de julho de 2021.

### CAPÍTULO III DA ANÁLISE DE VULNERABILIDADES

Art. 3º O processo para desenvolvimento seguro de software deve se iniciar com o processo de análise e resposta a vulnerabilidades, integrando a segurança no processo de desenvolvimento, obedecendo as seguintes fases:

- I - Recebimento de notificação de vulnerabilidades;
- II - Classificação das vulnerabilidades quanto a gravidade para priorização;
- III - Análise de riscos das vulnerabilidades;
- IV - Correção das vulnerabilidades;
- V - Notificação da correção das vulnerabilidades; e
- VI - Análise da causa raiz das vulnerabilidades.

Art. 4º O modelo de desenvolvimento seguro deverá considerar o princípio de privilégio mínimo e de mediação completa que tratam, respectivamente, de atribuir acesso mínimo ao usuário para a realização dos trabalhos.

Art. 5º Deverá ser implementado modelo de gerenciamento de ameaças que conte com o registro e acompanhamento de problemas de segurança, seus efeitos e impactos, devendo ser priorizados de acordo com a severidade de sua classificação.

§ 1º O registro de problemas deverá contemplar pelo menos as seguintes categorias:

- I – Falsificação (Spoofing): capacidade de se passar por outra pessoa, processo ou sistema;
- II – Alteração (Tampering): capacidade de alterar informação sem autorização;
- III – Repúdio (Repudiation): evitar responsabilidade por uma ação;
- IV – Divulgação de Informação (Information Disclosure): obter acesso a informação sem autorização;
- V – Negação de Serviço (Denial of Service): causar interferência ou mal funcionamento de um sistema ou serviço; e
- VI – Elevação de privilégio (Elevation of privilege): obter controle não autorizado sobre um sistema ou processo.

§ 2º A classificação da severidade se dará da seguinte forma:

- I – Altíssimo: para incidentes que exijam resposta imediata em razão de indisponibilidade de algum serviço;



II – Alto: para incidentes que tenham o potencial de configurar a hipótese prevista no inciso I; e

III – Baixo: para incidentes de baixo impacto ou poder destrutivo.

Art. 6º Para garantir segurança no processo de desenvolvimento deve-se, dentro das possibilidades, seguir as seguintes diretrizes:

- I – Manter treinamento contínuo dos desenvolvedores;
- II – Usar bibliotecas seguras;
- III – Utilizar ferramentas de análise de código para analisar padrões de configuração seguras e convenções;
- IV – Utilizar ferramentas de teste dinâmico de código visando encontrar vulnerabilidades; e
- V - Realizar pen-test manual.

#### CAPÍTULO IV DO INVENTÁRIO DE SOFTWARES

Art. 7º Os softwares desenvolvidos internamente e por de terceiros, incluindo os seus componentes, deverão ter gestores técnicos definidos quando da sua utilização;

Art. 8º Os gestores técnicos dos softwares serão responsáveis por:

- I - Manter atualizados;
- II - Atualizar inventários mensalmente;
- III - Avaliar os riscos de segurança e propor ações de combate; e
- IV - Realizar as atualizações críticas de alto risco em até 14 dias, a partir da identificação da falha.

#### CAPÍTULO V DO USO DE COMPONENTES

Art. 9º O uso de componentes de software de terceiros somente será permitido se estiverem atualizados e forem adquiridos de fontes confiáveis, além de certificar-se de que suas distribuições estejam em desenvolvimento e manutenção ativos e tenham um histórico de correção de vulnerabilidades divulgadas;

Art. 10. Antes do seu uso deverão passar por análise de vulnerabilidades e consulta em bancos de dados de vulnerabilidades disponíveis na Internet como o NIST - National Vulnerability Database (NVD)

Art. 11. Para análise de riscos de componentes de terceiros deve-se rigorosamente considerar:

- I - Selecionar produtos que estejam estabelecidos no mercado e que possuam segurança comprovada;
- II - Manter inventário automático ou individualizado atualizado;
- III - Avaliar o risco dos principais componentes da arquitetura;
- IV - Mitigar ou aceitar os riscos avaliados; e
- V - Monitorar os riscos.

#### CAPÍTULO VI DA INFRAESTRUTURA



Art. 12. Os ambientes de Sistemas de Produção e Não Produção deverão ser especificados e mantidos separados.

Art. 13. O repositório de informações e código fontes deverá ser segregado e ter política rígida de acesso com rastreamento de ações realizadas.

## CAPÍTULO VII DA CAPACITAÇÃO DE DESENVOLVEDORES

Art. 14. A equipe de desenvolvimento de software deverá ter um programa de treinamento para desenvolvimento seguro estabelecido que contemple princípios gerais de segurança, práticas padrão de segurança de aplicações e proteção de dados pessoais.

Parágrafo único. O treinamento deverá ser realizado pelo menos uma vez ao ano para promover a segurança dentro da equipe e construir uma cultura de segurança entre os desenvolvedores.

## CAPÍTULO VIII DA PROTEÇÃO DE DADOS PESSOAIS

Art. 15. Os softwares ou componentes que fazem tratamento de dados pessoais deverão seguir os requisitos da Lei nº 13.709/2018 e atender a pelo menos os seguintes princípios:

I - Finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

II - Adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

III - Necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

IV - Livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

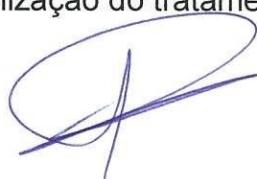
V - Qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

VI - Transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

VII - Segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

VIII - Prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

IX - Não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; e



X - Responsabilizaçāo e prestaçāc de contas: demonstração, pelo agente, da acoçāc de medicas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteçāc de dados pessoais e, inclusive, da eficácia dessas medidas.

Art. 16. O processc de desenvolvimento de seguro de software deverá estar alinhado com os padrões da indústria:

I - Privacy By Design: assegura que a proteção de dados pessoais deverá ser estabelecida desde a concepção do software ou componente compreendendo todo o ciclo de vida, devendo a equipe realizar uma abordagem proativa na proteção de dados pessoais; e

II – Privacy By Default: o software deverá resguardar a exposição de dados pessoais salvaguardando a privacidade, sendo o mais restritivo possível tanto na exposição/visualização de dados pessoais quanto na coleta;

Art. 17. As vulnerabilidades com cados pessoais terão prioridade sobre as demais, para as suas correções.

## CAPÍTULO V DAS DISPOSIÇÔES FINAIS

Art. 18. Esta portaria ceverá ser revisada a cada 12 meses.

Art. 19. Os casos omissos e eventuais dúvidas quanto à aplicação desta norma serão dirimidos pe a Comissâc Permanente de Segurança da Informação deste Tribunal.

Art. 20. Esta Portaria entra em vigor na data ce sua publicação e sua implementação iniciará imediatamente e ceverá estar totalmente implantada no prazo de 24 (vinte e quatro) meses a cortar desta data.

Natal/RN, 12 de dezembro de 2023.

  
Desembargador **Cornélio Alves**  
Presidente