Tribunal Regional Eleitoral - RJ
Diretoria Geral
Secretaria de Administração
Coordenadoria de Gestão Documental, Informação e Memória

INSTRUÇÃO NORMATIVA DG TRE-RJ Nº 06, DE 03 DE JULHO DE 2023.

Dispõe sobre as regras e os procedimentos para Desenvolvimento Seguro de Software no Tribunal Regional Eleitoral do Rio de Janeiro.

A DIRETORA-GERAL DO TRIBUNAL REGIONAL ELEITORAL DO RIO DE JANEIRO, no uso das atribuições que lhe são conferidas pelo **art. 19, I, da Resolução TSE n.º 23.644, de 1º de julho de (https://www.tse.jus.br/legislacao/compilada/res/2021/resolucao-no-23-644-de-1o-de-julho-de-2021)**
2021 (Política de Segurança da Informação da Justiça Eleitoral) (https://www.tse.jus.br/legislacao/compilada/res/2021/resolucao-no-23-644-de-1o-de-julho-de-2021),

CONSIDERANDO a **Resolução CNJ nº 396, de 7 de junho de 2021 (https://atos.cnj.jus.br/atos/detalhar/3975)**, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);

CONSIDERANDO o **art. 9º, II, j, da Resolução TSE nº 23.644/2021, que institui a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral (https://www.tse.jus.br/legislacao/compilada/res/2021/resolucao-no-23-644-de-1o-de-julho-de-2021)**;

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 segurança da informação previstas no modelo CIS Controls V.8;

CONSIDERANDO a necessidade de implementar controles para o tratamento de dados pessoais, de acordo com a **Lei nº 13.709, de 14 de agosto de 2018 (LGPD) (https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm)**;

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 de Janeiro; e

CONSIDERANDO, ainda, o disposto no processo SEI n.º 2023.0.000019275-6,

RESOLVE:

CAPÍTULO I

DISPOSIÇÕES PRELIMINARES

Art. 1º Fica instituída a norma de Desenvolvimento Seguro de Software, com intuito de estabelecer padrões de segurança no desenvolvimento de software.

Art. 2º Esta norma integra a Política de Segurança de Informação da Justiça Eleitoral, estabelecida pela **Resolução TSE nº 23.644/2021 (https://www.tse.jus.br/legislacao/compilada/res/2021/resolucao-no-23-644-de-1o-de-julho-de-2021)**.

Art. 3º Para os efeitos desta Instrução Normativa, aplicam-se os termos e definições conceituados na **Portaria DG/TSE nº 444, de 8 de julho de 2021 (https://www.tse.jus.br/legislacao/compilada/prt/2021/portaria-no-444-de-08-de-julho-de-2021)**.

CAPÍTULO II

DISPOSIÇÕES GERAIS

Art. 4º O processo para desenvolvimento seguro de software deve contemplar processo de análise e resposta a vulnerabilidades, integrando a segurança no processo de desenvolvimento e obedecendo às seguintes fases:

I - recebimento de notificação de vulnerabilidades;
II - classificação das vulnerabilidades quanto à 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. 5º O modelo de desenvolvimento seguro deverá considerar:

I - o princípio do privilégio mínimo;
II - a proteção de dados durante o tratamento, em trânsito e em repouso;
III - a defesa em profundidade;
IV - a mediação completa com a não confiança nas entradas dos usuários;
V - a minimização da superfície de ataque;
VI - a criação de padrões seguros;
VII - a autenticidade e a integridade (assinatura de código);
VIII - a necessidade de falhar com segurança (manuseio de mensagem de erro);
IX - a utilização de kit de desenvolvimento de software (SDK) confiável.

Art. 6º Os dados de teste devem ser criteriosamente selecionados e controlados, além de mantidos em segurança.

Parágrafo único. Sempre que possível, não serão utilizados dados reais em testes.

Art. 7º Será utilizado processo de modelagem de ameaças, a fim de identificar possíveis ameaças e implementar proteções contra elas.

Art. 8º Para garantir segurança no processo de desenvolvimento deve-se obedecer às seguintes diretrizes:

I - manter treinamento continuo dos desenvolvedores;
II - usar bibliotecas seguras;
III - realizar análises de código, de forma manual ou automatizada, para analisar padrões de configuração segura e convenções;
IV - utilizar ferramentas de teste dinâmico de código visando encontrar vulnerabilidades;
V - realizar testes de penetração.

CAPÍTULO III

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 de cada componente;

IV - mitigar ou aceitar os riscos avaliados;
V - monitorar os riscos.

CAPÍTULO IV

DA INFRAESTRUTURA

Art. 12. Os componentes da infraestrutura de aplicações serão configurados seguindo modelospadrão submetidos a processo de hardening, para que funcionem corretamente e com a segurança necessária.

Parágrafo único. Os modelos-padrão serão definidos com a utilização, sempre que possível, de modelos predefinidos por fornecedores ou organizações independentes de cibersegurança e
observarão a Política de Segurança da Informação da Justiça Eleitoral e suas normas complementares.

Art. 13. Os ambientes de sistemas de produção e não produção deverão ser especificados e mantidos separados.

Art. 14. O repositório de informações e códigos-fonte deverá ser segregado e ter políticas rígidas de acesso com rastreamento de ações realizadas.

CAPÍTULO V

DA CAPACITAÇÃO DE DESENVOLVEDORES

Art. 15. A equipe de desenvolvimento de software deverá estabelecer um programa de treinamento para desenvolvimento seguro que contemple princípios gerais de segurança, práticas padrão de segurança de aplicações e proteção de dados pessoais.

Parágrafo único. Deve ser realizado ao menos um treinamento por ano, para promover a segurança dentro da equipe e construir uma cultura de segurança entre os desenvolvedores.

CAPÍTULO VI

DA PROTEÇÃO DE DADOS PESSOAIS

Art. 16. Os softwares ou componentes que façam tratamento de dados pessoais deverão seguir os princípios e requisitos da **Lei nº 13.709/2018 (https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm)**, no que couber.

Art. 17. O processo de desenvolvimento seguro de software deverá estar alinhado com os seguintes 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, onde a equipe deverá realizar uma abordagem proativa na proteção de dados pessoais;
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.

CAPÍTULO VII

DISPOSIÇÕES FINAIS

Art. 18. Os casos omissos serão resolvidos pela Diretoria-Geral, ouvida, se necessário, a Comissão de Segurança da Informação.

Art. 19. Essa norma deve ser revisada a cada 3 (três) anos, ou antes, se necessário, pela Assessoria de Segurança da Informação, juntamente com a Secretaria de Tecnologia da Informação, e encaminhada para nova apreciação da Comissão de Segurança da Informação.

Art. 20. Esta norma entra em vigor na data de sua publicação e sua implementação se fará no prazo de 18 (dezoito) meses a contar desta data.

ELINE IRIS RABELLO GARCIA DA SILVA
Diretora-Geral

Este texto não substitui o publicado no **DJE TRE-RJ nº 165, de 05/07/2023, p. 6 (https://dje.tse.jus.br/dje/pdf/v1/edicao/104814#page=6)**

FICHA NORMATIVA

Data de Assinatura: 03/07/2023

Ementa: Dispõe sobre as regras e os procedimentos para Desenvolvimento Seguro de Software no Tribunal Regional Eleitoral do Rio de Janeiro.

Situação: Não consta revogação.

Diretor(a)-Geral: ELINE IRIS RABELLO GARCIA DA SILVA

Data de publicação: DJE TRE-RJ nº 165, de 05/07/2023, p. 6 (https://dje.tse.jus.br/dje/pdf/v1/edicao/104814#page=6)

Alteração: Não consta alteração.