Desembargador ERIVAN LOPES
Presidente do TRE/PI

PORTARIA PRESIDÊNCIA Nº 158/2023 TRE/PRESI/DG/ASSDG, DE 14 DE ABRIL DE 2023

Dispõe sobre as regras e os procedimentos para Desenvolvimento Seguro de Software 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 definir normativo para estabelecer diretrizes para o desenvolvimento seguro no âmbito do TRE-PI;

CONSIDERANDO a necessidade de implementar controles para o tratamento de dados pessoais, de acordo com a Lei nº 13.709/2018 (LGPD);

CONSIDERANDO a Resolução nº 396, de 7 de junho de 2021, do Conselho Nacional de Justiça, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);

CONSIDERANDO a Resolução nº 23.644, de 1º de julho de 2021, do Tribunal Superior Eleitoral, que institui a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral;

CONSIDERANDO a Resolução nº 448, de 24 de maio de 2022, que adota a PSI da Justiça Eleitoral estabelecida pela Resolução nº 23.644/2021, de 1º de julho de 2021, do Tribunal Superior Eleitoral;

CONSIDERANDO as boas práticas em segurança da informação previstas nas normas ABNT ISO /IEC 27001:2013 e ABNT NBR ISO/IEC 27002:2013;

CONSIDERANDO as boas práticas em segurança da informação previstas no modelo *CIS Controls V.8.;*

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;

RESOLVE:

CAPÍTULO I

DAS DISPOSIÇÕES PRELIMINARES

Art. 1º Fica instituída a norma complementar da Política de Segurança da Informação para 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 do TRE-PI, estabelecida pela Resolução nº 448, de 24 de maio de 2022.

CAPÍTULO II

DAS DEFINIÇÕES

Art. 3º Para efeitos desta norma consideram-se os termos e definições a seguir:

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, danos à imagem institucional, prejuízo ao erário, entre outros;

III - Atividades precípuas: conjunto de procedimentos e tarefas que utilizam recursos tecnológicos, humanos e materiais, inerentes à atividade-fim da Justiça Eleitoral;

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

V - Ativo de processamento: patrimônio composto por todos os elementos de hardware, software e infraestrutura de comunicação necessários à execução das atividades precípuas da Justiça Eleitoral;
VI - Ativo: qualquer bem, tangível ou intangível, que tenha valor para a organização;
VII - 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;
VIII - Ciclo de vida da informação: ciclo formado pelas fases de produção, recepção, organização, uso, disseminação e destinação;
IX - Confidencialidade: propriedade da informação que garante que ela não será disponibilizada ou divulgada a indivíduos, entidades ou processos sem a devida autorização;
XX - Disponibilidade: propriedade da informação que garante que ela será acessível e utilizável sempre que demandada;
XI - 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;
XII - Integridade: propriedade que garante que a informação mantém todas as características originais estabelecidas pelo proprietário;
XIII - Irretratabilidade (ou não repúdio): garantia de que a pessoa se responsabilize por ter assinado ou criado a informação;
XIV - 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;
XV - Recurso: além da própria informação, é todo o meio direto ou indireto utilizado para o seu tratamento, tráfego e armazenamento;
XVI - 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;
XVII - Risco: potencial associado à exploração de vulnerabilidades de um ativo de informação por ameaças, com impacto negativo no negócio da organização;
XVIII - 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;
XIX - 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;
XX - Tratamento da informação: recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação, inclusive as sigilosas;
XXI - Usuário: aquele que utiliza, de forma autorizada, recursos inerentes às atividades precípuas da Justiça Eleitoral;
XXII - Vulnerabilidade: fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.

CAPÍTULO III
DA ANÁLISE DE VULNERABILIDADES

Art. 4º O processo para desenvolvimento seguro de software deve 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 Vulnerabilidade;

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 o princípio de privilégio mínimo e de mediação completa que tratam, respectivamente, de atribuir acesso mínimo ao usuário para a realização dos trabalhos e nunca confiar nas entradas checando-se todo acesso a todo objeto.

Art. 6º Deverá ser implementado modelo de gerenciamento de ameaças que contemple 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 - Adulteração de dados (*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, conforme definido no Plano de Gestão de Riscos de TI vigente, considerando o impacto de uma vulnerabilidade gerar incidentes, que venham causar:

I - indisponibilidade de serviço

II - violação de privacidade;

III - perda de dados;

IV - dano a imagem do Tribunal;

V - qualquer outro tipo de vulnerabilidade que possa prejudicar o desenvolvimento das atividades regulares do Tribunal.

Art. 7º 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 *pentest* manual a nível código.

CAPÍTULO IV

DO INVENTÁRIO DE SOFTWARES

Art. 8º Os softwares desenvolvidos internamente e por terceiros, incluindo os seus componentes, deverão ter gestores definidos quando da sua utilização;

Art. 9º Os gestores 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 - Providenciar e acompanhar as atualizações críticas de alto risco de forma automática ou em até 14 dias.
Parágrafo único. Na impossibilidade de cumprimento do prazo estabelecido no inciso IV, o software ou componente deverá ser desativado imediatamente.
CAPÍTULO V
DO USO DE COMPONENTES
Art. 10. 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. 11. 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. 12. 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 VI
DA INFRAESTRUTURA
Art. 13. O processo de desenvolvimento seguro de software deverá possuir elementos de sua infraestrutura padronizada seguindo rigoroso Modelo Seguro de Configuração para componentes de infraestrutura de aplicações que estabeleçam a funcionalidade mínima e que possuam imagens padrão que passaram por processo de ?*hardening*?.
Art. 14. Os ambientes de Sistemas de Produção e Não Produção deverão ser especificados e mantidos separados.
Art. 15. O repositório de informações e código fontes deverá ser segregado e terem políticas rígidas de acesso com rastreamento de ações realizadas.
CAPÍTULO VII
DA CAPACITAÇÃO DE DESENVOLVEDORES
Art. 16. 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. 17. Os softwares ou componentes que façam tratamento de dados pessoais deverão seguir os requisitos da Lei nº 13.709, de 14 de agosto de 2018 (LGPD), 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;
X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.
Art. 18. O processo de desenvolvimento de seguro de software deverá estar alinhado com os padrões da indústria:
I - *Privacy By Design*: assegura a proteção de dados pessoais deverá ser estabelecida desde a concepção do software ou componentes compreendendo todo o ciclo de vida, onde a equipe deverá 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. 19. As vulnerabilidades com dados pessoais, terão prioridade sobre as demais, para as suas correções.
Art. 20. Os componentes de terceiros que manuseiam dados pessoais devem passar por análise adicional sendo inventariado e validado em sua conformidade com a proteção de dados pessoais, além de passar por testes de invasão específicos.
CAPÍTULO IX
DAS DISPOSIÇÕES FINAIS
Art. 21. Os casos omissos serão resolvidos pela Diretoria Geral, subsidiada pela Comissão de Segurança da Informação deste Tribunal.
Art. 22. A revisão deste normativo ocorrerá sempre que se fizer necessário ou conveniente para este Tribunal, não excedendo o período máximo de 3 (três) anos.
Art. 23. O descumprimento desta política será objeto de apuração pela unidade competente do Tribunal e consequente aplicação das penalidades cabíveis a cada caso.
Art. 24. Esta Portaria entra em vigor na data de sua publicação.
Desembargador ERIVAN LOPES
Presidente do TRE-PI