DIÁRIO DA JUSTIÇA ELETRÔNICO

DO TRIBUNAL REGIONAL ELEITORAL DO AMAPÁ

Ano: 2023, nº 48

Disponibilização: quarta-feira, 15 de março de 2023
Publicação: quinta-feira, 16 de março de 2023

Tribunal Regional Eleitoral do Amapá

Desembargador João Guilherme Lages Mendes
Presidente

Desembargador Carmo Antônio de Souza
Vice-Presidente e Corregedor

Dr. Francisco Valentim Maia
Diretor-Geral

Avenida Mendonça Júnior, 1502 - Centro
Macapá/AP
CEP: 68900-914

Contato
(96) 3198 - 7541
sejud@tre-ap.jus.br

SUMÁRIO

ATOS DA PRESIDÊNCIA

PORTARIAS

PORTARIA PRESIDÊNCIA Nº 27/2023 TRE-AP/PRES/ASPRES

Portaria Presidência Nº 27/2023 TRE-AP/PRES/ASPRES

Dispõe sobre as regras e os procedimentos para Desenvolvimento e Implantação Segura de *Software* no Tribunal Regional Eleitoral do Amapá.

O PRESIDENTE do Tribunal Regional Eleitoral Amapá (TRE-AP), no uso de suas atribuições legais e regimentais,

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

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

CONSIDERANDO a portaria da Diretoria Geral do TSE nº 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 as boas práticas em segurança da informação previstas nas normas da Associação Brasileira de Normas Técnicas (ABNT), ABNT ISO/IEC 27001 e ABNT NBR ISO/IEC 27002;

CONSIDERANDO as boas práticas em segurança da informação previstas no modelo *Center for Internet Security* (CIS) *Controls* V.8;

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

CONSIDERANDO a Resolução do Tribunal Regional Eleitoral do Amapá (TRE-AP) nº 570/2022, que dispõe sobre a Política de Segurança da Informação (PSI) no âmbito do Tribunal Regional Eleitoral do Amapá;

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

CONSIDERANDO a Portaria TRE-AP 120/2021, que instituiu a Política Organizacional de Desenvolvimento e Implantação de Softwares no âmbito do TRE-AP ;

CONSIDERANDO a Portaria TRE-AP 11/2022, que dispõe sobre a Governança e a Gestão Negocial das Soluções de Tecnologia;

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 Amapá (TRE-AP);

RESOLVE:

CAPÍTULO I

DISPOSIÇÕES PRELIMINARES

Art. 1º. Instituir a portaria complementar da Política de Segurança da Informação para Desenvolvimento e Implantação Segura de *Software* no Tribunal Regional Eleitoral do Amapá (TRE-AP), com intuito de estabelecer padrões de segurança no desenvolvimento e implantação de *software*.

Art. 2º Esta portaria integra a Política de Segurança de Informação do TRE-AP, estabelecida pela Resolução TRE-AP nº 570/2022.

CAPÍTULO II

DAS DEFINIÇÕES

Art. 3º Para os efeitos da Política de Segurança da Informação do TRE-AP, aplicam-se os termos e definições conceituados na Portaria TRE-AP nº 25/2023.

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 (*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. 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 *pen-test* manual a nível código.

CAPÍTULO IX

DO INVENTÁRIO DE *SOFTWARES*

Art. 8º Os *softwares* desenvolvidos internamente e por terceiros, incluindo os seus componentes, deverão ter gestores negociais e técnicos definidos quando da sua utilização, conforme previsto nas Portarias TRE-AP nº 11/2022 e nº 120/2021.

Art. 9º Os gestores técnicos dos *softwares* serão responsáveis:

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 de forma automática ou em até 14 dias.

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;

Parágrafo único. Antes do seu uso, deverão passar por análise de vulnerabilidades e consulta em bancos de dados de vulnerabilidades disponíveis na internet como o *National Vulnerability Database* (NVD) do *National Institute of Standards and Technology* (NIST).

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 VI

DA INFRAESTRUTURA

Art. 12. 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. 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 de acesso com rastreamento de ações realizadas.

CAPÍTULO VII

DA CAPACITAÇÃO DE DESENVOLVEDORES

Art. 15 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. 16. Os *softwares* ou componentes que façam tratamento de dados pessoais deverão seguir os requisitos da lei 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;
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. 17. O processo 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, 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. 18. As vulnerabilidades com dados pessoais, terão prioridade sobre as demais, para as suas correções.
Art. 19. 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
DA IMPLANTAÇÃO DE SOFTWARES
Art. 20. A implantação de Softwares na infraestrutura tecnológica administrada pelo TRE/AP deve ser precedida de avaliação de segurança efetuada pela área técnica responsável pela Seção de Desenvolvimento de Sistemas (SDS), com apoio das áreas de redes, banco de dados e de segurança cibernética do TRE-AP.
Art. 21. A avaliação de Segurança deverá ter como produto um relatório técnico com parecer, que deverá ser armazenado em repositório próprio visando a Gestão da Segurança da Informação.
Art. 22. O Relatório Técnico, fruto da avaliação de segurança, deve conter, no mínimo:
I - Resultado da Análise de Vulnerabilidades do Software, efetuada em software próprio para esse fim.
II - Informação sobre aplicação ou não de técnicas de desenvolvimento seguro na codificação do sistema, descrevendo-as, de forma sucinta, quando estiverem presentes.
III - Informação sobre a linguagem de programação e/ou ferramentas tecnológicas usadas no desenvolvimento do Software, com informações sucintas sobre eventuais fragilidades de segurança nessa linguagem/ferramenta.

IV - Informação sobre como se dará o processo de atualização de segurança do Software durante o seu ciclo de vida, incluindo as responsabilidades.

V - Informação sobre adequação de segurança do Software quanto à proteção dos dados pessoais, com indicação do responsável de negócio pelos dados.

Art. 23. O Parecer, fruto da avaliação de segurança, deve indicar, com base nas informações constantes no Relatório Técnico, se o sistema possui requisitos mínimos de segurança para ser implantado na infraestrutura tecnológica do TRE-AP.

Art. 24. Caberá ao Comitê de Governança de Segurança da Informação a decisão final sobre a implantação ou não de um Software com parecer técnico desfavorável à implantação.

CAPÍTULO X

DA DISPONIBILIZAÇÃO DE SOFTWARES E SERVIÇOS NA INTERNET

Art. 25. Os Softwares disponibilizados na Internet devem, obrigatoriamente, atender aos requisitos previstos na Portaria que estabelece a Política de Uso Aceitável dos Recursos de Tecnologia da Informação e Comunicação (TIC) no Tribunal Regional Eleitoral do Amapá.

capítulo XI

DISPOSIÇÕES FINAIS

Art. 26. Os casos omissos serão resolvidos pela Comitê de Gestão de Tecnologia da Informação e Comunicação (CGTIC) deste Tribunal.

Art. 27. Esta portaria complementar deve ser revisada a cada 12 (doze) meses pela CSC e encaminhada para apreciação do CGTIC.

Art. 28. Esta Política deve ser publicada no portal de intranet do Tribunal.

Art. 29. O descumprimento desta portaria será objeto de apuração pela unidade competente do Tribunal, com a consequente aplicação das penalidades cabíveis a cada caso.

Art. 30. Esta portaria entra em vigor na data de sua publicação e sua implementação deve ser realizada em até 12 (doze) meses.

Documento assinado eletronicamente por JOÃO GUILHERME LAGES MENDES, Presidente, em 13/03/2023, conforme art. 1º, III, "b", da Lei 11.419/2006.

PORTARIA PRESIDÊNCIA Nº 28/2023 TRE-AP/PRES/ASPRES

Portaria Presidência Nº 28/2023 TRE-AP/PRES/ASPRES

Institui a Gestão de Ativos de informação e de processamento relativa à Política de Segurança da Informação do Tribunal Regional Eleitoral de Amapá.

O PRESIDENTE do Tribunal Regional Eleitoral do Amapá, no uso de suas atribuições legais e regimentais,

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

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

CONSIDERANDO a Resolução do Tribunal Regional Eleitoral do Amapá (TRE-AP) 570/2022, que dispõe sobre a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral do Amapá;

CONSIDERANDO a portaria da Diretoria Geral do 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 as boas práticas em segurança da informação previstas nas normas da Associação Brasileira de Normas Técnicas (ABNT), ABNT ISO/IEC 27001 e ABNT NBR ISO/IEC 27002;