TRIBUNAL REGIONAL ELEITORAL DE GOIÁS
PRAÇA CIVIA, 300 - Bairro CENTRO - CEP 74003-010 - Goiânia - GO - www.tre-go.jus.br

PORTARIA DG Nº 216, DE 27 DE OUTUBRO DE 2024.

O **DIRETOR-GERAL DO TRIBUNAL REGIONAL ELEITORAL DE GOIÁS**, no uso de suas atribuições legais e regimentais e considerando a Resolução CNJ nº 370, de 28 de janeiro de 2021, que estabelece a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD), a Resolução CNJ nº 396, de 07 de junho de 2021, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ), a Lei nº 13.709, de 14 de agosto de 2018, que dispõe sobre Lei Geral de Proteção de Dados (LGPD), a Resolução TSE nº 23.644, de 1º de julho de 2021, que institui a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral, RESOLVE:

Art. 1º Fica instituída a Norma de Desenvolvimento Seguro de Sistemas, em consonância com as Políticas de Segurança da Informação do Tribunal Regional Eleitoral de Goiás e do Tribunal Superior Eleitoral.

Art. 2º Para os efeitos da Política de Segurança da Informação do TRE-GO e das normas a ela subordinadas, aplicam-se os termos e definições conceituados no Anexo VIII da Portaria CNJ nº 162/2021.

CAPITULO I

DA ARQUITETURA E DOS PADRÕES DE DESENVOLVIMENTO DE SISTEMAS

Art. 3º Os sistemas devem ser desenvolvidos unicamente por meio de linguagens de codificação, bibliotecas, frameworks, ferramentas e demais soluções de desenvolvimento definidas pela unidade de desenvolvimento de sistemas da Secretaria de Tecnologia da Informação.

Art. 4º Devem ser adotados repositórios padronizados de armazenamento de dados para o desenvolvimento de sistemas, que permitam minimamente:

I - o controle de versionamento de códigos-fonte e de toda a documentação associada, tais como casos de uso, workflows, casos de testes, diagramas e relatórios; e

II - o versionamento de artefatos de desenvolvimento, tais como arquivos compilados, bibliotecas, contêineres, snapshots, pacotes de instalação, executáveis e binários.

§1º Os repositórios devem ser mantidos de forma centralizada em ambiente controlado, de modo a garantir a confidencialidade, a integridade e a disponibilidade dos códigos e artefatos neles armazenados.

§2º Os gestores da área de negócio serão os responsáveis para permitir acesso de usuários aos sistemas e às bases de dados do sistema e no desenvolvimento de softwares.

§3º Devem ser mantidos acordos de confidencialidade para desenvolvedores ou usuários que necessitem acessar os códigos desenvolvidos ou sob custódia do TRE-GO, mesmo

que de forma temporária.

Art. 5º A utilização de recursos criptográficos é obrigatória e deverá ser resultado da análise dos requisitos de segurança da aplicação associada à análise de riscos de segurança cibernética.

Art. 6º Os sistemas de informação deverão atender aos seguintes requisitos:

I – ser portáveis e interoperáveis;

II – ser disponíveis para dispositivos móveis e responsivos;

III – possuir documentação atualizada;

IV – oferecer suporte para assinatura baseado em certificação digital emitido por Autoridade Certificadora;

V – utilizar, preferencialmente, sistemas de informação já desenvolvidos, disseminados e experimentados no âmbito do Poder Judiciário.

VI – utilizar, sempre que possível, Repositório Nacional para disseminação de boas práticas e compartilhamento de soluções colaborativas de TIC.

Parágrafo único. A transmissão eletrônica de credenciais de acesso aos sistemas de informação, deverá sempre ser realizada de forma criptografada.

Capítulo II

DOS AMBIENTES DE EXECUÇÃO DOS SISTEMAS

Art. 7º Os sistemas do Tribunal devem contar com ambientes de execução diferenciados para o desenvolvimento, testes, homologação e produção.

Parágrafo único. Sistemas fornecidos por terceiros, com ou sem ônus para o Tribunal, deverão contar, obrigatoriamente, com os ambientes de teste, homologação e produção, além de atender à infraestrutura existente de forma segura.

Art. 8º Os ambientes de desenvolvimento, testes e homologação devem, na medida do possível, reproduzir o ambiente de produção, para fins de redução de vulnerabilidades de segurança.

Art. 9º Os sistemas devem ser devidamente testados e homologados em seus ambientes de execução apropriados, antes da sua liberação para a produção.

Capítulo III

DO PROJETO DE SISTEMAS

Art. 10. O sistema a ser desenvolvido deve especificar os requisitos de segurança relativos à confidencialidade, integridade, disponibilidade, autenticidade, não-repúdio, e de privacidade dos dados por ele tratados.

Art. 11. Em caso de celebração de convênios/acordos ou contração de desenvolvimento de sistemas de informação, no instrumento contratual deverá constar cláusula que determine o depósito da documentação e afins pertinentes à tecnologia de concepção, manutenção e atualização, bem como, quando cabível, do código-fonte junto a autoridade brasileira que controla a propriedade intelectual de softwares para garantia da continuidade.

Capítulo IV

DA CODIFICAÇÃO DOS SISTEMAS

Art. 12. O processo de desenvolvimento de sistemas do TRE-GO deve considerar os procedimentos para desenvolvimento seguro, definidos conjuntamente pelas unidades responsáveis pela gestão de segurança de TI e desenvolvimento de software do TRE-GO, de acordo com as tecnologias empregadas na codificação, com vistas à garantia da integridade, confidencialidade e disponibilidade dos sistemas e seus dados.

Capítulo V

DO AMBIENTE DE COMPILAÇÃO E IMPLANTAÇÃO DE SOFTWARE

Art. 13. Todos os componentes e bibliotecas de terceiros, utilizados no desenvolvimento de sistemas do TRE-GO, devem ser mantidos em repositório centralizado.

Parágrafo único. O processo de desenvolvimento de sistemas deve considerar, preferencialmente, o uso de bibliotecas já existentes e disponíveis no repositório, com o intuito de reduzir a ocorrência de possíveis riscos no uso de bibliotecas de terceiros que estejam vulneráveis a ataques.

Capítulo VI

DA GESTÃO DE IDENTIDADES, AUTENTICAÇÃO E CERTIFICAÇÃO DIGITAL

Art. 14. Os sistemas devem ser disponibilizados por meio de mecanismos que garantam sua identidade, assim como a criptografia do tráfego de informações entre o ambiente do Tribunal e os clientes desses sistemas.

Parágrafo único. Quando utilizados certificados digitais, suas informações devem ser mantidas em repositório seguro, controlado, de preferência por meio do uso de solução de gerenciamento centralizada, para fim de gestão de seus ciclos de vida.

Capítulo VII

DO INVENTÁRIO DE SISTEMAS

Art. 15. Todos os sistemas, desenvolvidos internamente ou de propriedade do TRE-GO, devem ser claramente identificados e inventariados, contendo informações relevantes para o gerenciamento e manutenção da segurança dos dados institucionais.

Art. 16. Todas as informações sobre os ativos de sistema devem ser reunidas de forma integrada, preferencialmente por meio de base de gerência de ativos centralizada.

Capítulo VIII

DA CAPACITAÇÃO DE DESENVOLVEDORES

Art. 17. O programa de capacitação contínua deverá ser estabelecido pela equipe de desenvolvimento de software e contemplará os princípios gerais de segurança, práticas padrão de segurança de aplicações e proteção de dados pessoais.

Parágrafo único. A capacitação deverá ser realizada, pelo menos uma vez ao ano, para promover a segurança e construir uma cultura de segurança entre os desenvolvedores.

Capítulo IX

DA PROTEÇÃO DE DADOS PESSOAIS

Art. 18. O processo de desenvolvimento seguro de software, no que concerne às boas práticas de proteção de dados, deverá estar alinhado aos conceitos de:

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, por meio de uma abordagem; e

II – Privacy By Default: o software será disponibilizado com todas as salvaguardas relacionadas à proteção de dados estabelecidas no item anterior, adotando uma configuração mais restrita possível no que se refere à exposição, visualização e coleta de dados.

Art. 19. Os softwares ou componentes, que façam tratamento de dados pessoais, deverão seguir os requisitos da Lei nº 13.709/2018, Lei Geral de Proteção de Dados (LGPD), atendendo, pelo menos, aos princípios de finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas.

Art. 20. As vulnerabilidades com dados pessoais, quanto às suas correções, terão prioridade sobre as demais.

Capítulo X

DISPOSIÇÕES FINAIS

Art. 21. Os casos omissos serão resolvidos pelo Comitê Gestor de Segurança da Informação deste Tribunal.

Art. 22. Caberá à Secretaria de Tecnologia da Informação propor a atualização desta Portaria no prazo máximo de 3 (três) anos ou, antes disso, sempre que se fizer necessário.

Art. 23. A Secretaria de Tecnologia da Informação deverá expedir instruções de trabalho a fim de regulamentar padrões e regras complementares a esta Portaria.

Art. 24. Esta portaria entra em vigor na data de sua assinatura.

LEONARDO SAPIÊNCIA SANTOS

Diretor-Geral

Documento assinado eletronicamente por **LEONARDO SAPIÊNCIA SANTOS**, **DIRETOR-GERAL**, em 27/10/2024, às 16:44, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei4.tre-go.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0960844** e o código CRC **18726650**.