TRIBUNAL REGIONAL ELEITORAL DO ACRE

PORTARIA DIRETORIA-GERAL Nº 60/2023 PRESI/DG/GADG

Dispõe sobre o Processo para Desenvolvimento Seguro de Software no âmbito do Tribunal Regional Eleitoral do Acre.

A Diretoria-Geral da Secretaria do Tribunal Regional Eleitoral do Acre, no uso das suas atribuições regimentais, nos termos do art. 28, V, do Regimento Interno da Secretaria,

CONSIDERANDO a necessidade de definir processos relacionados à segurança e ao ciclo de vida de software, visando ao desenvolvimento seguro de aplicações e implementação de medidas de segurança aderentes à LGPD (Lei n. 13.709/2018);

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

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

CONSIDERANDO a Portaria DG/TSE n. 444/2021, que dispõe sobre a instituição da norma de termos e definições relativa à Política de Segurança da Informação da Justiça Eleitoral;

CONSIDERANDO as boas práticas em segurança da informação previstas nas normas ABNT ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 e no modelo CIS Controls versão 8,

RESOLVE:

CAPÍTULO I - DISPOSIÇÕES PRELIMINARES

Art. 1º Fica instituída, no âmbito do Tribunal Regional Eleitoral do Acre, a norma de Desenvolvimento Seguro de Software, em consonância com a Política de Segurança de Informação da Justiça Eleitoral, estabelecida pela Resolução TSE n. 23.644/2021 e pela Resolução TRE-AC n 1.776/2022, com intuito de estabelecer padrões de segurança no desenvolvimento de software.

Art. 2º Esta norma complementa a Política de Segurança de Informação.

CAPÍTULO II - DAS DEFINIÇÕES

Art. 3º Para os efeitos da Política de Segurança da Informação do TSE e das normas a ela subordinadas, aplicam-se os termos e definições conceituados na Portaria TSE nº 444, de 8 de julho de 2021.

CAPÍTULO III - DA ARQUITETURA E DOS PADRÕES DE DESENVOLVIMENTO DE SOFTWARE

Art. 4º Os softwares devem ser desenvolvidos unicamente por meio de linguagens de codificação, bibliotecas, frameworks, ferramentas e demais soluções de desenvolvimento previamente aprovadas pela unidade responsável pelas definições de arquitetura de desenvolvimento de software da STI.

Art. 5º Devem ser adotados repositórios padronizados de armazenamento de dados para o desenvolvimento de software 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 Devem ser mantidos acordos de confidencialidade para desenvolvedores ou demais interessados que necessitem acessar os códigos desenvolvidos ou sob custódia do TSE, mesmo que de forma temporária.

Art. 6º APIs, webservices e soluções semelhantes devem ser publicadas e controladas por ferramentas de gerenciamento de APIs.

Parágrafo único. A ferramenta deverá possuir ao menos as seguintes funcionalidades:

I - publicação de instruções de uso das APIs;

II - acompanhamento gráfico do perfil de utilização das APIs (frequência de acesso, endereços IP de origem, usuários que realizam acesso); e

III - controles de utilização das APIs, tais como frequência de utilização, cota máxima de utilização por período, controles de acesso por usuário, endereço IP de origem e outros.

Art. 7º A criação e aprovação dos modelos de dados para o desenvolvimento de software, sob incumbência da unidade responsável pela modelagem de dados da STI, deve contemplar controles efetivos com intuito de conferir segurança na disponibilização e processamento dos dados.

Art. 8º Devem ser utilizados recursos de criptografia no desenvolvimento e implantação de softwares de informação para assegurar, entre outros:

§ 1º A confidencialidade, integridade e a autenticidade de informações sensíveis ou críticas que se encontrem armazenadas em bases de dados ou sistemas de arquivo ou que sejam objeto de transmissão eletrônica.

§ 2º O não repúdio, como forma de comprovar a ocorrência de um evento ou ação e sua associação à entidade originária.

Art. 9º A identificação da necessidade da utilização de recursos criptográficos deverá ser resultado da análise dos requisitos de segurança da aplicação associada à análise de ameaças.

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

Art. 10º A unidade responsável pela Gestão de Segurança de Tecnologia da Informação da STI publicará um Procedimento de Uso de Recursos Criptográficos indicando quais são os recursos de criptografia aprovados para utilização, contemplando, ao menos, algoritmos para criptografia simétrica, assimétrica e cálculo de resumos criptográficos (hashes).

Parágrafo único. Os sistemas eleitorais podem adotar padrões de criptografia específicos, também previstos no procedimento a que se refere o *caput* deste artigo, de acordo com as peculiaridades necessárias ao seu processo de desenvolvimento ou por força de legislação eleitoral que assim o requeira.

Art. 11. Devem ser estabelecidas arquiteturas de referência para as diferentes linguagens de desenvolvimento de software, que incluam os controles mínimos de segurança aplicáveis.

CAPÍTULO IV - DOS AMBIENTES DE EXECUÇÃO DOS SOFTWARES

Art. 12. Os softwares do Tribunal devem contar com ambientes de execução diferenciados para o desenvolvimento, testes, homologação e produção.

Parágrafo único. Softwares fornecidos por terceiros, com ou sem ônus para o Tribunal, deverão contar obrigatoriamente com os ambientes de teste, homologação e produção.

Art. 13. Os ambientes de desenvolvimento, testes e homologação devem reproduzir o mais fielmente possível o ambiente de produção, para fins de redução de vulnerabilidades de segurança, com exceção das características de dimensionamento dos ambientes.

Art. 14. Cabe exclusivamente à unidade responsável pela infraestrutura de TI da STI, o controle sobre o dimensionamento e o acesso aos ambientes de execução de softwares.

Art. 15. Os softwares devem ser devidamente testados e homologados em seus ambientes de execução apropriados, antes da sua liberação para a produção, de acordo com o processo de liberação de softwares definido pela STI.

Art. 16. A infraestrutura dos ambientes de execução dos sistemas deve conter mecanismos que garantam o acesso seguro, observando-se, no mínimo, os seguintes controles:

I - somente a unidade responsável pela infraestrutura dos ambientes de produção da STI deve possuir acesso direto aos ambientes de produção dos sistemas, exceto por determinação da STI, após análise e aprovação de justificativa fundamentada;

II - O acesso aos ambientes de desenvolvimento, testes e homologação é permitido somente à equipe de infraestrutura e à equipe de desenvolvimento do sistema que esteja sendo construído ou testado; e

III - A unidade responsável pela infraestrutura de TI da STI poderá, após análise, conceder o direito de acesso remoto aos ambientes de desenvolvimento, teste e homologação do sistema aos seus desenvolvedores ou interessados, desde que seja solicitado com as devidas justificativas.

Parágrafo único. Toda e qualquer concessão de permissão de acesso aos ambientes deve ser precedida de assinatura de acordos de confidencialidade.

CAPÍTULO V - DO PROJETO DE SOFTWARES

Art. 17. Devem ser especificados os requisitos de segurança relativos ao software a ser desenvolvido, quanto à confidencialidade, integridade, disponibilidade, autenticidade, não-repúdio, e de privacidade dos dados por ele tratados.

§ 1º Todos os requisitos e especificações devem ser analisados e revisados quanto ao aspecto da segurança da informação, antes e durante a codificação, de acordo com as definições de desenvolvimento seguro aprovadas para cada tecnologia de codificação empregada.

§ 2º A análise de segurança dos requisitos e especificações do sistema deve direcionar as ações de verificação e testes de segurança necessárias ao longo do processo de desenvolvimento do sistema.

Art. 18. Os sistemas desenvolvidos por terceiros por meio de demanda formalizada pelo Tribunal, bem como sua documentação e artefatos, devem ser submetidos à verificação de segurança pelo TRE-AC, de acordo com critérios de avaliação definidos pela unidade responsável pela gestão da segurança de TI do TRE-AC.

CAPÍTULO VI - DA CODIFICAÇÃO DOS SOFTWARES

Art. 19. O processo de desenvolvimento de software do TRE-AC deve considerar os procedimentos para desenvolvimento seguro definidos conjuntamente pela unidade responsável pela gestão de segurança de TI do TRE-AC e pelas unidades de desenvolvimento, de acordo com as tecnologias empregadas na codificação, com vistas à garantia da integridade, confidencialidade e disponibilidade dos sistemas e seus dados.

Parágrafo único. Os procedimentos para desenvolvimento seguro serão publicados por meio da unidade responsável pela gestão de segurança de TI do TRE-AC, em guias especializadas.

Art. 20. Os procedimentos de codificação segura dos sistemas devem considerar, no mínimo, os seguintes controles de segurança:

I - O desenvolvimento deve ser auxiliado por interfaces, ferramentas ou procedimentos que garantam a codificação segura do sistema;

II - O sistema deve utilizar camada de persistência segura para acesso ao banco de dados, de modo a evitar ataques contra a integridade, a confidencialidade e a disponibilidade dos dados;

III - Os dados de entrada do sistema devem ser submetidos à validação ou sanitização, antes da sua inserção à base de dados;

IV - Os dados de saída do sistema devem ser codificados de forma a garantir a integridade e a confidencialidade das informações, quando seus requisitos assim o requererem;

V - A ocorrência de exceções e erros na execução dos sistemas em ambiente de produção deve ser tratada com a apresentação de mensagens de erro na tela dos usuários que não apresentem códigos ou textos que revelem detalhes técnicos sobre os erros. Tais detalhes devem ser apresentados exclusivamente no registro do evento no log do sistema; e

VI - Os sistemas não devem conter senhas, chaves de criptografia, credenciais ou informações pessoais como CPF, nome, e-mail, título de eleitor ou outros dados sensíveis diretamente escritos em seus códigos-fonte.

CAPÍTULO VII - DO AMBIENTE DE COMPILAÇÃO E IMPLANTAÇÃO DE SOFTWARE

Art. 21. Devem ser definidos e documentados procedimentos de compilação de software de acordo com as linguagens de programação utilizadas.

§ 1º A definição do processo de compilação deve ser disponibilizada em um local centralizado e acessível às ferramentas e profissionais envolvidos com o processo de desenvolvimento.

§ 2º As ferramentas utilizadas no processo de compilação devem contar com manutenção ativa de seus fabricantes ou comunidades de desenvolvimento, devem ser configuradas segundo as boas práticas de segurança por eles recomendadas e devem ser submetidas a um processo periódico de aplicação de correções de segurança disponibilizadas, como patches, hotfixes, entre outros métodos.

§ 3º As ferramentas utilizadas no processo de compilação devem prover mecanismos de verificação de integridade dos artefatos gerados (tais como hashes ou assinaturas).

§ 4º Verificações de segurança automatizadas devem ser integradas ao processo de implantação de software, tais como a Análise Estática de Código Fonte (SAST).

§ 5º Os resultados das verificações de segurança automatizadas deverão compor os critérios de aceitação para a implantação dos sistemas em ambiente de produção.

Art. 22. Todos os componentes e bibliotecas de terceiros utilizados no desenvolvimento de sistemas do TRE-AC devem ser mantidos em repositório centralizado.

§ 1º Os componentes e bibliotecas de terceiros devem ser submetidos à verificação de vulnerabilidade periodicamente ou sempre que necessária sua avaliação, de preferência de forma automatizada.

§ 2º Nos casos em que o componente a ser verificado integra sistema classificado como de alta criticidade, a verificação deve incluir uma análise manual detalhada, para a garantia de uma maior eficácia na realização dos testes.

§ 3º O processo de desenvolvimento de sistemas deve considerar preferencialmente o uso de bibliotecas já existentes e disponíveis no repositório, com o intuito de se reduzir a ocorrência de possíveis riscos no uso de bibliotecas de terceiros que estejam vulneráveis a ataques.

Art. 23 Devem ser definidos e documentados procedimentos de implantação de software nos ambientes de desenvolvimento, homologação e produção.

§ 1º A definição do processo de implantação deve ser disponibilizada em um local centralizado e acessível a ferramentas e profissionais envolvidos com o processo de desenvolvimento.

§ 2º As ferramentas utilizadas no processo de implantação devem contar com manutenção ativa de seus fabricantes ou comunidades de desenvolvimento, devem ser configuradas segundo as boas práticas de segurança recomendadas e devem ser submetidas a um processo periódico de aplicação de correções de segurança para ela disponibilizadas como patches, hotfixes, entre outros métodos.

§ 3º Os procedimentos de implantação devem ser automatizados em todos os estágios, de forma a eliminar a possibilidade de erros em função de sua execução manual.

Art. 24. A realização de testes dinâmicos em aplicações e de testes de intrusão deverá ser feita observando-se a classificação dos sistemas, de acordo com procedimento definido pela unidade responsável pela gestão da segurança de TI do TRE-AC, observando-se também os critérios de grau de sigilo, de criticidade das informações tratadas e o processo de modelagem de ameaças adotado pelo TRE-AC, contando com o apoio de ferramentas especializadas, e deve considerar os seguintes controles:

I - todas as falhas encontradas, bem como as correções e evidências do teste devem ser registradas de forma centralizada e reportadas às equipes responsáveis pelo projeto de desenvolvimento e correção;

II - preferencialmente, deve ser realizada análise de riscos sobre as falhas encontradas e não corrigidas;

III - adicionalmente, na realização de verificação de segurança em aplicações críticas, devem ser realizados testes complementares envolvendo técnicas exploratórias sobre os controles de segurança da aplicação, como metodologia de autenticação, criptografia utilizada, controle de acessos e outros controles de segurança.

CAPÍTULO VIII - DA GESTÃO DE IDENTIDADES, AUTENTICAÇÃO E CERTIFICAÇÃO DIGITAL

Art. 25. A autenticação de usuários nos sistemas do Tribunal deve ser realizada por meio de soluções de gestão de identidades e de autenticação padronizadas para o acesso dos usuários aos sistemas, não sendo permitido o armazenamento de quaisquer credenciais advindas de soluções de autenticação distintas das homologadas pela unidade responsável pelas definições de arquitetura de desenvolvimento de software da STI.

§ 1º As soluções de gestão de identidades e de autenticação devem prever a implementação de controles efetivos de segurança, tais como:

I - uso de duplo fator de autenticação (2FA);

II - suporte à utilização de certificação digital e tokens;

III - funções de identificação de robôs, tais como captcha;

IV - gestão de políticas de senhas;

V - gestão de direitos de acesso; e

VI - registros das atividades (logs) de criação, modificação e exclusão de credenciais, bem como de autenticação.

§ 1º As funcionalidades de autorização de acesso dos usuários aos sistemas devem ser implementadas preferencialmente por meio de perfis de direitos de acesso, em oposição a direitos de acesso atribuídos de forma individual.

§ 2º Os sistemas que necessitem ser expostos para acesso externo ao TRE-AC, devem possuir controles específicos de segurança no acesso que complementam o uso simples de credenciais baseadas em usuário e senha, tais como o uso obrigatório de duplo fator de autenticação ou o uso de certificação digital.

§ 3º A unidade responsável pela gestão da segurança de TI do TRE-AC publicará procedimento divulgando quais são as soluções de gestão de identidades e autenticação homologadas para utilização pelos sistemas e aplicações do Tribunal, indicando os cenários em que podem ser utilizadas.

§ 4º O procedimento de que trata o parágrafo anterior será revisado com periodicidade mínima anual ou quando houver fato novo que exija sua revisão.

§ 5º As credenciais de acesso aos bancos de dados e aos sistemas devem possuir direitos de acesso mínimos necessários para suas funções.

Art. 26. Os sistemas expostos externamente ao TRE-AC devem ser disponibilizados por meio de mecanismos que garantam a identidade do sistema, 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 IX - DOS REGISTROS DE LOG DOS SISTEMAS

Art. 27. Os registros de logs dos sistemas devem ser armazenados por meio de solução centralizada e padronizada de gerenciamento de eventos.

Art. 28. Os projetos de desenvolvimento dos sistemas devem prever mecanismos para a geração e armazenamento dos logs, conforme definições da unidade responsável pela segurança de TI do TRE-AC, sendo necessário que o sistema mantenha uma base de logs local, a qual deve prever a sua replicação em base centralizada.

Art. 29. Os sistemas desenvolvidos pelo TRE-AC devem gerar registros sobre sua utilização, com especificação de data e hora da ocorrência em milissegundos, tais como:

I - autenticação de usuários, com sucesso ou falha;

II - alteração de perfil do usuário;

III - erros e exceções sem tratamento nos sistemas;

IV - acesso a dados sensíveis para alteração;

V - acesso a dados sensíveis para leitura;

VI - negação de acesso a páginas ou funções;

VII - usuário autenticado executando a ação;

VIII - nome do servidor do sistema (se aplicável);

IX - IP e número da porta de origem da máquina cliente do sistema (se aplicável);

X - tipo da ação; e

XI - tipo de erro.

CAPÍTULO X - DO CICLO DE VIDA DOS SISTEMAS

Art. 30. Deve ser observado o procedimento para manutenção do ciclo de vida dos sistemas desenvolvidos ou de propriedade do TRE-AC, envolvendo a inclusão de regras para o descarte, descontinuação e transição segura de sistemas e base de dados previstas na Política de Segurança da Informação.

§ 1º Para fins de transparência e obediência à Política de Gestão Documental (Resolução TRE-AC n. 1.755/2022), o descarte deverá estar previsto na Tabela de Temporalidade, seguindo os trâmites internos de gestão documental para o descarte seguro dos dados e documentos, com registro no Sistema Eletrônico de Informações - SEI e publicação de edital de descarte no portal do Tribunal.

§ 2º Qualquer informação orgânica/arquivística armazenada em sistemas, bancos e bases de dados deverá ser avaliada e autorizada pela Comissão Permanente de Avaliação de Documentos (CPAD) antes do descarte, conforme a Política de Gestão Documental (Resolução TRE-AC n. 1.755/2022).

Art. 31. O procedimento para manutenção do ciclo de vida dos sistemas deve considerar, no mínimo, os seguintes controles:

I - os sistemas e suas bases de dados que foram substituídos ou legados devem ser retirados do ambiente de produção e preservados por meio de procedimento de armazenamento, de acordo com as regras definidas na Política de Backup de Informações (Instrução Normativa TRE-AC n. 35/2018), salvo por motivação legal ou por determinação da Secretaria de Tecnologia da Informação;

II - as bases de dados de sistemas legados que não mais realizem transações, porém necessitem disponibilizar os seus dados para consulta, devem preferencialmente ser disponibilizadas por meio de soluções de descoberta e disponibilização de dados;

III - os ambientes de desenvolvimento, homologação e testes devem ser desativados quando não mais houver evolução no sistema, quando o sistema for retirado do ambiente de produção ou quando formalmente solicitado pelo gestor do sistema;

IV - as unidades gestoras dos sistemas devem ser consultadas periodicamente quanto à necessidade de manutenção dos sistemas em produção.

CAPÍTULO XI - DA ANÁLISE DE VULNERABILIDADES

Art. 32. 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. 33. 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. 34. 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. 35. 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 de código.

CAPÍTULO XII - DO INVENTÁRIO DE SOFTWARES

Art. 36. Os softwares desenvolvidos internamente e por terceiros, incluindo os seus componentes, deverão ter gestores definidos quando da sua utilização;

Art. 37. Os gestores dos softwares serão responsáveis por:

I - Solicitar, acompanhar e gerenciar a atualização dos softwares, sempre que necessário;

II - Solicitar, acompanhar e gerenciar a atualização dos inventários, sempre que necessário;

III - Avaliar os riscos de segurança e propor ações de combate; e

IV - Solicitar, acompanhar e gerenciar as atualizações críticas de alto risco com a urgência que o caso requer.

CAPÍTULO XIII - DO USO DE COMPONENTES

Art. 38. 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. 39. 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 NIST (National Institute of Standards and Technology);

Art. 40. Para análise de riscos de componentes de terceiros deve-se 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 XIV - DA CAPACITAÇÃO DE DESENVOLVEDORES

Art. 41. 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 XV - DA PROTEÇÃO DE DADOS PESSOAIS

Art. 42. Os softwares ou componentes que façam tratamento de dados pessoais deverão seguir os requisitos da Lei n. 13.709/2018 (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. 43. O processo de desenvolvimento seguro de software deverá estar alinhado com os padrões da indústria:

I - Privacy By Design: assegura a proteção de dados pessoais devendo 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. 44. As vulnerabilidades com dados pessoais terão prioridade sobre as demais, para as suas correções.

Art. 45. 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 XVI - DISPOSIÇÕES FINAIS

Art. 46. Os casos omissos serão tratados pela Comissão de Segurança da Informação - CSI.

Art. 47. O conteúdo desta norma será revisado a cada 2 (dois) anos ou sempre que se fizer necessário.

Rio Branco, 14 de julho de 2023.

Documento assinado eletronicamente por **ROSANA MAGALHÃES DA SILVA**, **Diretora-Geral**, em 14/07/2023, às 10:27, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.tre-ac.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0598663** e o código CRC **C6402A67**.

0000799-97.2022.6.01.8000 0598663v3