ANEXO XII
NORMA DE DESENVOLVIMENTO SEGURO

Normativos relacionados:

Ato normativo	Capítulo / Seção / Artigo
Resolução-GP nº 5/2017	
Portaria nº 3/2021-DIA	

Versionamento:

Versão:	2.0
Data:	22/04/2024
Criada por:	Grupo de Trabalho Técnico (GTT) do CGSI
Aprovada por:	Comitê de Governança de Segurança da Informação (CGSI)
Aprovada em:	22/04/2024

Histórico de mudanças:

Data	Versão	Alterado por	Descrição das alterações
25/07/2023	1.0		
22/04/2024	2.0	GTT do CGSI	Conforme arquivo de registro de alterações (changelog).

1. INTRODUÇÃO

A Norma de Desenvolvimento Seguro complementa a Política de Segurança da Informação (PSI) e estabelece diretrizes para desenvolvimento e manutenção de softwares e sistemas que fazem parte do Poder Judiciário do Estado do Maranhão (PJMA).

Para fins desta norma aplica-se a lista de termos do glossário com suas respectivas definições, conforme descrito no ANEXO I - Glossário da PSI.

A equipe da Coordenadoria de Sistema de Informação (CSI) será representada por servidores(as), terceirizados(as), prestadores(as) de serviço e estagiários(as) lotados(as) na própria Coordenadoria subordinada à Diretoria de Informática e Automação (DIA) do Poder Judiciário do Estado do Maranhão.

Esta norma obedecerá ao escopo definido na Política de Segurança da Informação e às diretrizes detalhadas na Resolução-GP nº 5/2017 - TJMA ou posterior que a substitua, estendendo-se a outras unidades judiciais ou administrativas que estejam envolvidas no desenvolvimento de sistemas ou aplicações no PJMA.

2. OBJETIVOS

Garantir que a segurança da informação seja implementada em todo ciclo de vida de desenvolvimento dos sistemas de informação.

Atender aos princípios e requisitos de segurança da informação para sistemas de informação adquiridos pelo TJMA.

Atender aos princípios e requisitos de segurança da informação para sistemas de informação mantidos e/ou desenvolvidos pela equipe de sistemas do TJMA ou por terceirizados e/ou contratados supervisionados pela equipe de sistemas do TJMA.

Adotar práticas e requisitos de segurança cibernética no desenvolvimento de projetos novos ou em desenvolvimento, tais como ativação do Múltiplo Fator de Autenticação (MFA).

3. DIRETRIZES

Orientações da Norma de Desenvolvimento Seguro.

3.1 Requisitos de Segurança da Aplicação

Ao desenvolver, ou adquirir novos sistemas de informação ou alterar os existentes, a CSI deverá identificar e especificar os requisitos de software por meio de uma avaliação de risco. Nesse processo, deverão ser avaliados, no mínimo, os seguintes itens:

I - riscos relacionados ao acesso não autorizado ao ambiente de desenvolvimento;

II - riscos relacionados a mudanças não autorizadas no ambiente de desenvolvimento;

III - vulnerabilidades técnicas dos sistemas de TIC utilizados no PJMA, incluindo relatórios e um processo de entrada, atribuição, correção e teste da correção das vulnerabilidades;

IV - riscos que uma nova tecnologia pode trazer caso seja utilizada no PJMA.

3.2 Requisitos de Segurança Relacionados às Redes Públicas

A Diretoria de Informática e Automação (DIA) será responsável pela definição dos controles de segurança relacionados às informações em serviços de aplicativos que trafegam pelas redes públicas, incluindo:

I - a descrição dos sistemas de autenticação a serem utilizados;

II - a descrição de como assegurar a confidencialidade e integridade das informações;

III - a descrição de como garantir o não repúdio das ações.

3.3 Princípios de Desenvolvimento Seguro

A Diretoria de Informática e Automação (DIA) deverá garantir a proteção integral de todos os componentes dos softwares contra adulteração e/ou acesso não autorizado, gerenciando adequadamente o controle de acesso para proteger os arquivos relacionados ao desenvolvimento. Tal medida inclui a atribuição de permissões específicas a usuários(as) ou grupos de usuários(as), restringindo o acesso apenas a desenvolvedores(as) autorizados(as). Além disso, é fundamental aplicar o princípio do menor privilégio, garantindo que cada desenvolvedor(a) tenha apenas as permissões necessárias para desempenhar suas atividades laborais.

A Coordenadoria de Sistema de Informação (CSI) será responsável por produzir software seguro que tenha vulnerabilidades de segurança mínimas em suas aplicações ou sistemas, considerando as boas práticas de desenvolvimento seguro, tais como a possibilidade de ativação do Múltiplo Fator de Autenticação (MFA) e utilização de Single Sign-On (SSO).

Para análise de segurança do código fonte, a CSI poderá utilizar ferramentas de análise estática para verificar automaticamente o código em busca de vulnerabilidades e conformidade com os padrões de codificação segura. Essas ferramentas deverão ser utilizadas para corrigir práticas de software inseguras documentadas e verificadas continuamente.

A CSI poderá, quando necessário, utilizar bibliotecas e/ou componentes de software de terceiros atualizados e confiáveis, selecionando obrigatoriamente frameworks estabelecidos no mercado e comprovadamente seguros.

A Coordenadoria de Sistema de Informação (CSI) deverá aplicar os princípios de design seguro em arquiteturas de aplicativos, seguindo as melhores práticas do mercado, como o projeto OWASP (Open Web Application Security Project).

A CSI deverá elaborar a modelagem de ameaças, sendo conduzido por pessoas especializadas que avaliam o design da aplicação e medem os riscos de segurança para cada ponto de entrada e nível de acesso.

3.4 Ambiente de Desenvolvimento

As aplicações desenvolvidas pelo PJMA, deverão possuir separação adequada quanto aos sistemas de desenvolvimento, homologação e produção e operação deles em diferentes domínios (por exemplo, em ambientes virtuais ou físicos separados).

As informações sensíveis, como dados pessoais, utilizadas nos ambientes de desenvolvimento e de homologação dos sistemas de informação deverão ser evitadas, substituindo-os, sempre que possível, por dados fictícios ou anonimizados.

3.5 Ambiente de Homologação

As alterações nas aplicações deverão ser validadas formalmente pelos(as) usuários(as) final(is) e pela equipe técnica no ambiente de homologação antes de serem aplicadas no ambiente de produção.

Dados confidenciais, bem como dados que possam estar relacionados a informações pessoais e protegidos pela Lei Geral de Proteção de Dados Pessoais (LGPD), não deverão ser utilizados nos ambientes de desenvolvimento e homologação. As exceções serão aprovadas pelo Comitê Gestor de Proteção de Dados Pessoais (CGPD), cabendo à DIA definir como esses dados serão protegidos.

A DIA é responsável por definir a metodologia, as responsabilidades e o prazo para verificar se todos os requisitos de segurança da informação foram cumpridos e se o sistema é aceitável para entrar em produção.

3.6 Treinamentos

A Diretoria de Informática e Automação (DIA) deverá:

I - certificar-se de que todo o pessoal de desenvolvimento de software receba treinamento para escrever código seguro, incluindo princípios gerais de segurança e práticas padrão de segurança de aplicativos;

II - garantir treinamentos que promovam a segurança dentro da equipe de desenvolvimento e construam uma cultura de segurança entre os desenvolvedores.

A Coordenadoria de Sistema de Informação (CSI) é responsável por definir as habilidades e conhecimentos necessários para o processo de desenvolvimento seguro dos treinamentos propostos.

A CSI deverá editar procedimentos baseados em boas práticas de desenvolvimento seguro para os sistemas de informações, tanto para a elaboração de novos sistemas quanto para a manutenção dos sistemas existentes, bem como definirá as normas mínimas de segurança que deverão ser cumpridas.

Os mesmos princípios de desenvolvimento seguro serão aplicados para sistemas de informação mantidos e/ou desenvolvidos por terceirizados(as) e/ou contratados(as) supervisionados(as) pela Coordenadoria de Sistema de Informação (CSI).

3.7 Repositórios

Os códigos-fonte deverão ser hospedados em repositórios internos cedidos pelo PJMA. Os repositórios remotos, como GitHub, GitLab ou Bitbucket só deverão

ser utilizados caso sejam devidamente autorizados pela Diretoria de Informática e Automação (DIA).

O acesso aos repositórios deverá ser protegido por autenticação de dois fatores (2FA) e outras medidas de segurança, como utilização de senhas fortes.

Dependendo da sensibilidade do código ou de outros arquivos relacionados ao desenvolvimento, a CSI poderá criptografá-los para impedir o acesso não autorizado, que poderá ser alcançado por meio de criptografia de disco, criptografia de arquivo ou criptografia de transporte, seguindo as diretrizes do ANEXO IX - Norma de Gestão de Criptografia e Gerenciamento de Chaves da PSI.

3.8 Controle de Versão (Versionamento)

A Coordenadoria de Sistema de Informação (CSI) poderá utilizar o sistema de controle de versão (numeração, datas, etc.) e aplicar nos ambientes de desenvolvimento, homologação e/ou produção. Este sistema permite que várias pessoas trabalhem em conjunto, rastreiem as alterações feitas no código ao longo do tempo e revertam para versões anteriores, caso seja necessário.

Todos os sistemas de informação próprios e de terceiros, terão suas diversas versões disponibilizadas em ciclos de desenvolvimento, homologação e/ou produção, denominados de lançamentos (releases). Os lançamentos serão disponibilizados em intervalos fixos mínimos de 30 (trinta) dias na maioria dos casos, podendo ocorrer em intervalos menores caso haja necessidade expressa da administração.

Toda e qualquer alteração não emergencial nos sistemas de informação deverá ser incluída no próximo lançamento, de acordo com a capacidade operacional da DIA e seguindo ordem de priorização definida pela CSI.

A cada ciclo de desenvolvimento, a Diretoria de Informática e Automação informará sua capacidade operacional, a fim de suportar a priorização de suas demandas e determinada pelos seguintes fatores:

I - número de homem/horas disponíveis para cada lançamento;

II - demandas emergenciais impostas por alterações legais ou normativas, pelo Conselho Nacional de Justiça (CNJ) ou pela equipe técnica da DIA;

III - projetos definidos no Planejamento Estratégico do TJMA;

IV - correção emergencial de erros críticos dos sistemas de informação em uso;

V - projetos definidos como prioritários pela DIA ou pela Presidência do Tribunal de Justiça do Maranhão.

A Diretoria de Informática e Automação (DIA) categoriza os sistemas de informação em uso no Poder Judiciário do Estado do Maranhão (PJMA) em:

I – operacionais;

II – táticos;

III – estratégicos.

3.9 Cópias de Segurança

Os sistemas de informações do PJMA deverão possuir cópias de segurança (backup) regulares dos arquivos relacionados ao desenvolvimento para prevenir perdas de dados em casos de incidentes de segurança da informação, tais como, falhas de hardware, desastres naturais ou ataques cibernéticos. As cópias de segurança deverão ser armazenadas em locais seguros e testadas regularmente para garantir sua integridade e capacidade de recuperação, seguindo as diretrizes do ANEXO VIII - Norma de Cópias de Segurança da Informação da PSI.

3.10 Controle de Alterações

As alterações no desenvolvimento e nas manutenções dos sistemas de informação do PJMA deverão ser realizadas em conformidade com o disposto na PORTARIA-DIA nº 3/2021 ou em posterior que a substitua.

O Diretor de Informática e Automação poderá, a seu critério, autorizar alterações emergenciais no desenvolvimento e na manutenção dos sistemas de informação do PJMA.

3.10.1 Alterações Emergenciais

Considera-se como “erro emergencial” qualquer comportamento anômalo ou díspar gerado pelo sistema que impeça, de forma imperativa, sua utilização, comprometendo a capacidade operacional de uma atividade crítica ou área do PJMA. Caso exista uma operação alternativa no sistema de informação ou no setor que possa mitigar o erro em questão, este não será considerado emergencial.

Quando necessário, poderão ser criadas versões intermediárias dos sistemas antes da resolução do problema emergencial.

3.11 Propriedade Intelectual

O uso não autorizado de software ou sistema de informação de propriedade intelectual do PJMA, como reprodução, modificação, distribuição ou qualquer outra forma de uso das aplicações sem permissão expressa da Diretoria de Informática e Automação (DIA), é proibido.

4. NOVOS SISTEMAS DE INFORMAÇÃO

A implementação de novos sistemas de informação, seja por aquisição, doação ou desenvolvimento interno, estará condicionada à análise prévia de viabilidade técnica, realizada por 02 (dois) servidores efetivos da Diretoria de Informática e Automação (DIA).

A análise deverá resultar em um Relatório de Diagnóstico de Sistema, elaborado e assinado pelos 02 (dois) servidores efetivos da DIA. O relatório analisará a adequação do sistema proposto ao ambiente computacional do PJMA, recomendando a continuidade ou cancelamento do processo de implementação, considerando questões relacionadas à segurança da informação e privacidade de dados pessoais.

A Coordenadoria de Sistemas de Informação deverá emitir parecer técnico sobre a aquisição ou desenvolvimento de novos sistemas, assim como para a realização de manutenções evolutivas e corretivas em sistemas já existentes, necessárias para cumprimento de atos administrativos.

5. PAPÉIS E RESPONSABILIDADES

Papéis e responsabilidades no contexto desta norma.

5.1 Diretoria de Informática e Automação

Compete exclusivamente à Diretoria de Informática e Automação (DIA):

I – gerir os softwares e sistemas de informação do PJMA;

II – homologar sistemas de informação para uso nas atividades jurisdicionais e administrativas;

III – desenvolver ou adquirir sistemas de informação, buscando dar celeridade às atividades jurisdicionais ou administrativas;

IV – realizar atividades de perícia e auditoria das operações nos sistemas de informação;

V – estabelecer políticas de homologação de softwares e sistemas;

VI – implementar mecanismos de controle de licenças de uso e bloqueio de instalações de softwares não licenciados ou não homologados;

VII – aplicar políticas de controle de alterações das configurações dos sistemas;

VIII - definir os meses de liberação dos lançamentos (releases), seguindo os ciclos estabelecidos.

IX - divulgar amplamente informações sobre as novas versões lançadas, mantendo um histórico das alterações realizadas nos últimos de 02 (dois) anos.

5.2 Comitê Gestor de Proteção de Dados Pessoais

É responsabilidade do Comitê Gestor de Proteção de Dados Pessoais (CGPD):

I - aprovar o uso de dados confidenciais e dados pessoais protegidos pela Lei Geral de Proteção de Dados Pessoais (LGPD) nos ambientes de desenvolvimento e homologação.

6. INFRAÇÕES E PENALIDADES

Infrações e penalidades serão aplicadas conforme previsto na Política de Segurança da Informação.

7. REVISÕES

Esta norma será alterada mediante necessidade de atualização, com apreciação e aprovação do Comitê de Governança de Segurança da Informação (CGSI).

8. APROVAÇÃO

A norma foi aprovada pelo Comitê de Governança de Segurança da Informação (CGSI), revogando-se todas as disposições em contrário.