Presidência

PORTARIA PRESIDÊNCIA Nº 290 DE 30 DE JUNHO DE 2026.

Institui a Política de Desenvolvimento Seguro de Aplicações no âmbito do Conselho Nacional de Justiça.

O **PRESIDENTE DO CONSELHO NACIONAL DE JUSTIÇA (CNJ)**, no uso das atribuições constitucionais e regimentais e considerando o contido no processo SEI/CNJ nº 00496/2024,

RESOLVE:

Capítulo I

DAS DISPOSIÇÕES INICIAIS

Art. 1º Fica instituída a Política de Desenvolvimento Seguro de Aplicações, com o intuito de estabelecer padrões de segurança no desenvolvimento de soluções de TIC exclusivamente no âmbito interno do Conselho Nacional de Justiça.

§ 1º Esta norma passa a integrar a Política de Segurança da Informação (PSI) do CNJ, estabelecida pela Portaria Presidência n° 47/2017.

§ 2º Os dispositivos constantes desta Política são obrigatórios para todas as novas soluções que passarem a fazer parte do Portfólio de Soluções de TIC do CNJ. Para as soluções que já estejam em produção, os dispositivos constantes desta Política devem ser aplicados, sempre que possível, nos ciclos regulares de atualização ou, de forma emergencial, caso haja indício do comprometimento de algum elemento que afete os padrões de segurança previstos nesta Portaria.

§ 3º A aplicação dos controles previstos nesta Portaria observará a criticidade da solução, a exposição da aplicação, a sensibilidade dos dados tratados e os riscos associados ao serviço digital, conforme classificação técnica a ser definida pelo Departamento de Tecnologia da Informação e Comunicação (DTI).

Art. 2º Para efeitos desta Portaria, considera-se:

I - ameaça: conjunto de fatores externos ou causa potencial de incidente indesejado que podem resultar em dano para uma aplicação, sistema ou organização;

II - análise dinâmica ou *Dynamic Application Security Testing (DAST)*: tipo de teste que verifica o comportamento externo da aplicação em busca de anomalias ou vulnerabilidades, por meio de interações com o software em execução;

III - análise estática ou *Static Application Security Testing (SAST)*: tipo de teste de aplicação que verifica sua lógica interna em busca de falhas ou vulnerabilidades, por meio da verificação do código-fonte ou dos binários;

IV - confidencialidade: propriedade de que a informação não esteja disponível ou seja revelada a indivíduos, entidades ou processos não autorizados;

V - controles de segurança: medidas adotadas para evitar ou diminuir a probabilidade de exploração de uma vulnerabilidade, tais como, criptografia, funções de *hash*, validação de entrada, balanceamento de carga, trilhas de auditoria, controle de acesso, expiração de sessão, *backups,* etc;

VI - criptografia: disciplina que incorpora os princípios, meios e métodos para a transformação de dados com a finalidade de ocultar o conteúdo semântico e prevenir a utilização não autorizada ou a modificação não detectada;

VII - criticidade: propriedade de que a redução ou perda de funcionalidade de um determinado ativo cause impacto ao negócio de acordo com sua gravidade;

VIII - disponibilidade: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinada aplicação, órgão ou entidade autorizados;

IX - integridade: propriedade de salvaguarda da exatidão e completude da informação;

X - requisitos de segurança: conjunto de necessidades de segurança que a aplicação deve atender, sendo tais necessidades influenciadas fortemente pela política de segurança da informação da organização, compreendendo aspectos funcionais, não funcionais e legais;

XI - trilha de auditoria: registro que apresenta quem acessou uma aplicação e quais operações o usuário executou em um determinado período; e

XII - vulnerabilidade: fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.

Capítulo II

DO DESENVOLVIMENTO SEGURO DE APLICAÇÕES

Seção I

Do ciclo de vida de aplicações

Art. 3º O ciclo de vida de uma aplicação compreende as seguintes fases:

I - concepção: fase que envolve definições iniciais da aplicação;

II - construção e implantação: compreende o projeto, codificação, validação e disponibilização para uso;

III - operação e manutenção: alcança a manutenção e suporte da solução ao longo do tempo;

IV - descontinuação: fase em que é encerrado o uso da aplicação.

Art. 4º O ciclo de vida da aplicação deverá considerar em todas as suas etapas o princípio do privilégio mínimo e de mediação completa que tratam, respectivamente, de atribuir acesso mínimo ao usuário para a realização das suas atividades laborais e verificar a autorização, de todo e qualquer acesso, a um objeto ou recurso.

Parágrafo único. O modelo do caput deverá realizar o tratamento de dados pessoais de acordo com os princípios e requisitos da Lei Geral de Proteção de Dados (LGPD).

Art. 5º As etapas do ciclo de vida da aplicação deverão estar alinhadas com os seguintes princípios de segurança:

I - *Privacy By Design*: assegura que a proteção de dados pessoais deverá ser estabelecida desde a concepção do software até sua descontinuação, quando o gestor negocial, em conjunto com o gestor técnico, deverá realizar uma abordagem proativa na proteção de dados pessoais;

II - *Privacy By Default*: a aplicação deverá resguardar a exposição de dados pessoais salvaguardando a privacidade, sendo o mais restritivo possível tanto na exposição e visualização de dados pessoais quanto na coleta; e

Art. 6º Sempre que aplicável, a aplicação deverá possuir documentação técnica suficiente para sua implantação, operação, manutenção, integração e sustentação, preferencialmente mantida em repositório oficial do CNJ.

Seção II

Da codificação e da compilação das aplicações

Art. 7º O Diretor Técnico do DTI deverá estabelecer arquiteturas de referência para as diferentes linguagens de desenvolvimento de aplicações que incluam controles de Segurança da Informação.

Parágrafo único. Os processos de desenvolvimento de sistemas deverão prever, explicitamente, fase(s) de controle de Segurança da Informação.

Art. 8º Os procedimentos de codificação segura das aplicações devem implementar, no que couber, os seguintes controles de segurança:

I - o desenvolvimento deve ser auxiliado por interfaces, ferramentas ou procedimentos que garantam a codificação segura da aplicação;

II - a aplicação deve utilizar camada de persistência segura para acesso ao banco de dados, de modo a evitar ataques contra a integridade, a confidencialidade, a disponibilidade e a autenticidade das informações;

III - os dados de entrada da aplicação devem ser submetidos à validação ou sanitização, antes da sua inserção em base de dados;

IV - os dados de saída da aplicação devem ser codificados de forma a garantir a integridade, a confidencialidade e a autenticidade das informações, quando seus requisitos assim o requererem;

V - implementação de autenticação multifator;

VI - integração com sistemas de gerenciamento de identidades;

VII - a ocorrência de exceções e erros na execução das aplicações em ambiente de produção deve ser tratada com a apresentação de mensag**ens 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 da a**plicação;

VIII - as aplicações não devem conter senhas, chaves de criptografia, credenciais, segredos estáticos ou outros dados sensíveis diretamente armazenados em seus códigos-fonte ou em qualquer tipo de documentação; e

IX - deve-se documentar, inclusive no código da aplicação, as medidas protetivas aplicadas ao código-fonte, de modo a indicar, precisamente, o procedimento utilizado e suas peculiaridades.

Art. 9º O uso de componentes, bibliotecas, imagens, frameworks ou artefatos de terceiros deverá observar controles de procedência, atualização, licenciamento e vulnerabilidades conhecidas, preferencialmente mediante ferramentas automatizadas de análise de composição de software, inventário de dependências e verificação de segredos.

Art. 10. As aplicações desenvolvidas devem gerar trilhas de auditoria capazes de identificar, no mínimo, as seguintes informações:

I - data e hora do evento;

II - autenticação de usuários, com sucesso ou falha;

III - alteração de perfil do usuário;

IV - erros e exceções sem tratamento nas aplicações;

V - acesso a dados sensíveis para alteração;

VI - acesso a dados sensíveis para leitura;

VII - negação de acesso a páginas ou funções;

VIII - usuário autenticado executando a ação;

IX - nome do servidor da aplicação;

X - endereço IP e número da porta de origem da máquina cliente da aplicação;

XI - tipo da ação; e

XII - tipo de erro.

Art. 11. O Diretor Técnico do DTI deverá definir e designar equipe técnica para documentar 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 prover mecanismos de verificação de integridade dos artefatos gerados (tais como *hashes* ou assinaturas digitais).

§ 3º Verificações de segurança automatizadas devem ser integradas ao processo de desenvolvimento de aplicações, incluída a análise estática.

§ 4º Os resultados das verificações de segurança automatizadas decorrentes da análise estática deverão compor os critérios de aceitação para a implantação das novas aplicações em ambiente de produção.

Seção III

Da infraestrutura de operação e controle das aplicações

Art. 12. Durante as fases do ciclo de vida de construção e implantação, bem como operação e manutenção, a aplicação deve contar com ambientes operacionais de execução diferenciados para produção e demais ambientes (desenvolvimento, teste, homologação, dentre outros).

§ 1º Os ambientes operacionais das aplicações deverão ser especificados e mantidos de forma segregada.

§ 2º Os demais ambientes operacionais não produtivos devem reproduzir o ambiente operacional de produção, com exceção das características de dimensionamento e de dados reais.

§ 3º As aplicações devem ser devidamente testadas e homologadas em seus ambientes operacionais de execução apropriados, antes da sua liberação para produção.

§ 4º Os dados de teste e homologação devem ser criteriosamente selecionados e controlados, além de mantidos em segurança.

§ 5º As mudanças em quaisquer ambientes devem ser controladas, de forma a produzir documentação que irá integrar o ciclo de vida de desenvolvimento das aplicações.

Art. 13. A infraestrutura dos ambientes de execução das aplicações deve conter mecanismos que garantam o acesso seguro, observando-se as seguintes regras:

I - somente as unidades responsáveis pela infraestrutura de TIC do ambiente tecnológico do CNJ devem possuir acesso direto aos ambientes de produção, exceto se houver determinação do Diretor Técnico do DTI mediante justificativa fundamentada;

II - o acesso aos demais ambientes operacionais não produtivos será permitido somente à equipe de infraestrutura e à equipe de desenvolvimento da aplicação que esteja sendo construída ou testada; e

III - mediante justificativa fundamentada e autorização do Diretor Técnico do DTI, outros interessados poderão ter acesso temporário aos ambientes operacionais tratados no inciso II.

Parágrafo único. Toda e qualquer nova concessão de permissão de acesso ao ambiente operacional de produção deverá ser precedida de assinatura de acordos de confidencialidade, exceto para os servidores do CNJ que já atuarem nas unidades responsáveis pela infraestrutura de TIC do ambiente tecnológico do CNJ.

Art. 14. A análise dinâmica, os testes automatizados de segurança e, quando cabível, os testes de intrusão serão realizados conforme critérios de risco, criticidade, exposição da aplicação e disponibilidade operacional da unidade gestora de Segurança da Informação.

Parágrafo único. Os resultados das verificações de segurança aplicáveis deverão compor, conforme matriz de risco definida pelo DTI, os critérios de aceitação para implantação das aplicações em ambiente de produção.

Art. 15. Todos os componentes, inclusive os de terceiros, utilizados no desenvolvimento de aplicações devem ser mantidos em repositório centralizado, de modo a garantir a confidencialidade, a integridade, a disponibilidade e a autenticidade dos códigos e artefatos neles armazenados.

§ 1º A equipe de desenvolvimento da aplicação deverá realizar 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.

§ 2º A equipe de desenvolvimento da aplicação deverá providenciar o versionamento de artefatos de desenvolvimento, tais como arquivos compilados, bibliotecas, contêineres, *snapshots*, pacotes de instalação, executáveis e binários, de acordo com o estabelecido no art. 4º da Portaria Presidência nº 47/2017.

Seção IV

Da gestão das vulnerabilidades

Art. 16. O processo de gestão de vulnerabilidades deverá conter as seguintes fases:

I - recebimento de notificação de vulnerabilidades;

II - classificação das vulnerabilidades quanto à gravidade para priorização;

III - análise de riscos das vulnerabilidades;

IV - correção das vulnerabilidades;

V - notificação da correção das vulnerabilidades; e

VI - análise da causa raiz das vulnerabilidades.

Parágrafo único. As vulnerabilidades serão identificadas de acordo com os seguintes níveis de gravidade:

I - alta: para as que exijam resposta imediata em razão do alto impacto ou do alto poder destrutivo;

II - média: para as que tenham o potencial de configurar a hipótese prevista no inciso I; e

III - baixa: para as de baixo impacto ou de baixo poder destrutivo.

Art. 17. O Gestor Negocial, após análise técnica da unidade gestora de Segurança da Informação, irá avaliar a gravidade da vulnerabilidade e analisar seus riscos frente às ameaças para o negócio, podendo determinar a suspensão cautelar da aplicação, interrompendo o seu funcionamento em ambiente de produção.

§ 1º As vulnerabilidades de gravidade alta, independentemente da criticidade da aplicação, deverão ser imediatamente corrigidas pelas unidades responsáveis pela infraestrutura de TIC e pela equipe de desenvolvimento da aplicação.

§ 2º As vulnerabilidades de gravidade média ou baixa deverão ser corrigidas de acordo com o resultado da priorização da fase análise de riscos das vulnerabilidades, tendo em vista a criticidade da aplicação.

§ 3º O Diretor Técnico do DTI poderá atribuir prazos máximos para a correção das vulnerabilidades altas, médias e baixas, dependendo da priorização de demandas e carga das equipes responsáveis pelas correções.

Capítulo III

DAS DISPOSIÇÕES FINAIS

Art. 18. As situações não previstas nesta Portaria deverão ser resolvidas pelo Comitê de Governança de Segurança da Informação do CNJ juntamente com o Diretor Técnico do DTI.

Art. 19. A inobservância dos dispositivos constantes desta Política pode acarretar, isolada ou cumulativamente, nos termos da lei, sanções administrativas, civis ou penais, assegurados aos envolvidos o contraditório e a ampla defesa.

Art. 20. A Política de Desenvolvimento Seguro de Aplicações deverá ser revisada bianualmente ou quando necessário.

Art. 21. Esta Portaria entra em vigor 90 (noventa) dias após sua publicação.

Ministro **Edson Fachin**

PORTARIA PRESIDÊNCIA Nº 291 DE 30 DE JUNHO DE 2026.

Altera a Portaria Presidência nº 65/2021, que designa os integrantes dos Comitês Estaduais Judiciais de Enfrentamento à Exploração do Trabalho em Condição Análoga à de Escravo e ao Tráfico de Pessoas.

O **PRESIDENTE DO CONSELHO NACIONAL DE JUSTIÇA (CNJ)**, no uso de suas atribuições legais e regimentais e considerando o contido no processo SEI/CNJ nº 10019/2020,

RESOLVE:

Art. 1º A Portaria Presidência nº 65/2021 passa a vigorar com a seguinte alteração:

"Art. 1º .....