SUMÁRIO

1. INTRODUÇÃO

O objetivo desta Política é esclarecer como a DTI realiza o desenvolvimento de seus sistemas e servir como guia de boas práticas a serem adotadas por analistas, desenvolvedores e todos os colaboradores que operam os sistemas, tornando o processo de concepção e uso dos mesmos mais confiável, auditável, estável e protegido contra ameaças, a fim de atender aos conceitos de qualidade de software.

A prática de desenvolvimento seguro na DTI se baseia, dentro do aplicável, no Guia de Codificação Segura da OWASP, nas práticas do Ciclo de Vida de Desenvolvimento de Software Seguro (SDLC), segregação de ambientes, bem como, em uma estrutura de gestão ágil (SCRUM) de auto-organização das equipes em direção a um objetivo comum.

2. OBJETIVO

Estabelecer políticas de desenvolvimento seguro, agregando práticas destinadas a inclusão de atributos de segurança em projetos de software, a serem desenvolvidos por times dinâmicos e ágeis.

3. ABRANGÊNCIA

Esta Política se aplica a todos os colaboradores de tecnologia da informação, sejam servidores, contratados, trabalhadores temporários, terceirizados ou estagiários, que estejam de algum modo envolvidos nos processos de desenvolvimento de sistemas e aplicações da DTI.

4. REFERÊNCIAS

Plano Diretor de Tecnologia da Informação PDTI (2024-2026);

Política Corporativa de Segurança da Informação do TCE-AL;

Política de Controle de Acesso Lógico e Físico;

Política de Gestão de Backup e Recuperação de Dados;

Política de Gestão de Riscos de TI;

Política de Governança de TI;

Política de Privacidade e Proteção de Dados Pessoais do TCE-AL;

Política de Tecnologia da Informação do TCE-AL;

Procedimento Operacional de Gestão de Incidentes e Requisições;

Procedimento Operacional de Gestão de Mudanças;

Processo de Gestão e Análise de Vulnerabilidades de TI;

Manual de Classificação e Tratamento de Informações Sigilosas;

Manual de Gerenciamento de Permissões de Acesso;

Norma ABNT ISO/IEC 20000:2018 para Gerenciamento de Serviços de TI;

Norma ABNT ISO/IEC 27001:2022 para Gestão da Segurança da Informação, Segurança Cibernética e Proteção à Privacidade;

Norma ABNT ISO/IEC 29134:2017 - Tecnologia da Informação - Técnicas de Segurança, Avaliação de Impacto de Privacidade;

Norma ABNT NBR ISO/IEC 27005:2023 - Gestão de Riscos de TI;

Norma ABNT NBR 14724: 2011 – Informação e Documentação – Apresentação Trabalhos Acadêmicos.

Norma ABNT ISO/IEC 12207:2017 para Engenharia de Sistemas e Software – Processos do Ciclo de Vida do Software;

Norma ABNT ISO/IEC 15504:2008 – Melhoria de Processos de Software;

Norma ABNT NBR 13596 – Avaliação de Produto de Software – Características de Qualidade e Diretrizes para o seu Uso;

5. CONCEITOS E DEFINIÇÕES

Para fins de compreensão dos termos utilizados neste processo serão aplicados os seguintes conceitos e definições:

Ameaça: conjunto de fatores externos ou causa potencial de incidente indesejado que podem resultar em dano para um sistema;

Análise dinâmica: tipo de teste que verifica o comportamento externo do software em busca de anomalias ou vulnerabilidades, por meio de interações com o software em execução;

Análise estática: tipo de teste de software que verifica sua lógica interna em busca de falhas ou vulnerabilidades, por meio da verificação do código-fonte ou dos binários;

Ativos de informação: sistemas de informação, meios de armazenamento, transmissão e processamento, bem como locais onde se encontram esses meios e as pessoas que a eles têm acesso;

Ativo de software: item de solução de Tecnologia da Informação constituído por software;

Avaliação de conformidade em segurança da informação: exame sistemático do grau de atendimento aos requisitos relativos à segurança da informação com base em legislações específicas;

Ciclo de Vida de Desenvolvimento de Software Seguro (SDLC): processo que consiste na inserção de várias atividades e produtos relacionados a segurança na fase de desenvolvimento de software, como modelagem de ameaças, análise estática do código com uso de ferramentas, revisão de código, testes de segurança direcionados e uma revisão final de segurança, minimizando o surgimento de vulnerabilidades;

Codificação Segura OWASP: conjunto de diretrizes que ajudam os desenvolvedores a mitigarem vulnerabilidades comuns de segurança de software;

Confidencialidade: propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados;

Controles de segurança: medidas adotadas para evitar ou diminuir a probabilidade de exploração de uma vulnerabilidade, tais como, criptografia, validação de entrada, balanceamento de carga, trilhas de auditoria, controle de acesso, expiração de sessão, backups, etc.;

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;

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

Disponibilidade: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física, determinado sistema, órgão ou entidade autorizados;

Integridade: propriedade de salvaguarda da exatidão e completude da informação;

Requisitos de segurança: conjunto de necessidades de segurança que o sistema deve atender, sendo tais necessidades influenciadas fortemente pela **Política Corporativa de Segurança da Informação do TCE-AL**, compreendendo aspectos funcionais, não funcionais e legais. Os aspectos funcionais descrevem comportamentos que viabilizam a criação ou a manutenção da segurança e, geralmente, podem ser testados diretamente. Na maioria dos casos, remetem a mecanismos de segurança como, por exemplo, controle de acesso baseado em papéis de usuários (administradores, usuários comuns etc.), autenticação com o uso de credenciais (usuário e senha, certificados digitais etc.), dentre outros. Os aspectos não funcionais descrevem procedimentos necessários para que o sistema permaneça executando as funções adequadamente mesmo quando sob uso indevido como, por exemplo, a validação das entradas de dados e o registro de logs de auditoria com informações suficientes para análise técnicas;

OWASP: comunidade internacional sem fins lucrativos com a missão de ajudar organizações a conceber, desenvolver, adquirir, operar e manter aplicações confiáveis;

Plataforma GitLab: repositório centralizado para código fonte o qual permite os desenvolvedores clonarem a base em suas máquinas locais, fazer alterações no código e, em seguida, as enviar de volta para o repositório central (Controle de versões). O Gitlab registra todas as alterações feitas no código, permitindo que os desenvolvedores acompanhem o histórico de alterações e revertam para versões anteriores, quando necessário;

Plataforma GitHub: serviço de hospedagem de repositório de código aberto usado para hospedar e revisar código, construir software e gerenciar projetos de desenvolvimento;

Plataforma Bitbucket: serviço de repositório e controle de versão onde desenvolvedores e equipes podem hospedar seus projetos de programação e monitorar seus progressos, trabalhando com elementos como sistema de controle, documentação, busca de código e muito mais;

Segurança da informação: ações que objetivam viabilizar e assegurar a disponibilidade, integridade, confidencialidade e autenticidade das informações;

Sistema de informação: conjunto de recursos, meios e procedimentos que junta, armazena, processa e disponibiliza informação relevante para uma organização de modo a torná-la acessível e útil para quem a deseje e possa utilizar;

Single Sign-On (SSO): esquema de autenticação que permite que os usuários façam login uma vez usando um único conjunto de credenciais e acessem várias aplicações durante a mesma sessão;

Trilha de auditoria: registro que apresenta quem acessou um sistema de informação e quais operações o usuário executou em um determinado período;

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

6. PRINCÍPIOS, DIRETRIZES E REQUISITOS

Dentro das diretrizes e regras gerais da segurança da informação definidas nas **Políticas Corporativa de Segurança da Informação** e **Privacidade e Proteção de Dados Pessoais do TCE-AL** os sistemas e aplicações desenvolvidos, criados ou implantados no ambiente da DTI devem seguir um Ciclo de Vida de Desenvolvimento Seguro e o Guia de Desenvolvimento Seguro da OWASP padronizado e estabelecido na política em tela.

Os sistemas e aplicações devem receber manutenção frequente e é exigido que passem por atualizações periódicas para lidar com possíveis vulnerabilidades. Esses processos deverão ocorrer em intervalos planejados e coordenados pelos envolvidos nas áreas de TI da DTI, junto com fornecedores, fábrica de software e prestadores de serviços, onde aplicável, ou quando existir a necessidade/recomendação de atualização.

Cabe salientar que existe segregação de ambientes na infraestrutura de TI da DTI (Desenvolvimento, Homologação/Teste, Produção e, em algumas situações, o ambiente Pré Produtivo), separação de funções e controles de acesso entre o pessoal designado para os respectivos ambientes. São utilizados servidores, bases de dados e redes diferentes para garantir que não haja contaminação de dados.

O conteúdo da política em tela está estruturado em torno de princípios, diretrizes, requisitos e recomendações de boas práticas a serem seguidas em cada um dos tópicos listado abaixo:

6.1. REQUISITOS DE SEGURANÇA DA APLICAÇÃO

Ao desenvolver, ou adquirir novos sistemas de informação ou alterar os existentes, a DTI deverá identificar e especificar os requisitos de software por meio de uma avaliação de risco, incluindo no mínimo, os seguintes itens:

a) riscos relacionados a mudanças e aos acessos não autorizados aos ambientes (desenvolvimento, homologação/teste, produção);

b) vulnerabilidades técnicas dos sistemas utilizados na DTI, incluindo relatórios e um processo de entrada, atribuição, correção e teste da correção das vulnerabilidades;
c) riscos que uma nova tecnologia pode trazer caso seja utilizada na DTI.

6.2. PRINCÍPIOS DE DESENVOLVIMENTO SEGURO

A Diretoria de Tecnologia e Informática (DTI) e todo os eu corpo técnico envolvido 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 ao devidamente autorizados(as). Além disso, é fundamental aplicar o princípio do menor privilégio, garantindo que todos tenha apenas as permissões necessárias para desempenhar suas atividades técnicas.

Produzir software seguro que tenha vulnerabilidades de segurança mínimas em suas aplicações ou sistemas, considerando as boas práticas de desenvolvimento seguro, tal como a utilização de Single Sign-On (SSO).

Aplicar ferramentas de análise estática e dinâmica, dentro do aplicável, para verificar automaticamente o código em busca de vulnerabilidades e conformidade com os padrões de codificação segura com foco principal na correção de práticas de software inseguras.

6.3. AMBIENTE DE DESENVOLVIMENTO

Os sistemas e aplicações desenvolvidas pela DTI, deverão possuir separação adequada quanto aos sistemas de desenvolvimento, homologação/teste 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/teste dos sistemas de informação deverão ser evitadas, substituindo-os, sempre que possível, por dados fictícios ou anonimizados.

6.4. AMBIENTE DE HOMOLOGAÇÃO/TESTE

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

Dados confidenciais, bem como dados que possam estar relacionados a informações pessoais e protegidos conforme diretrizes definas nas **Políticas Corporativa de Segurança da Informação** e **Privacidade e Proteção de Dados Pessoais do TCE-AL**, não deverão ser utilizados nos ambientes de desenvolvimento e homologação/teste. Na existência de particularidades e exceções deverão ocorrer aprovação conjunta do **Núcleo de Segurança da Informação e Diretoria DTI**.

Ademais, o **Núcleo de Segurança da Informação e Diretoria DTI,** com total apoio do corpo técnico, são responsáveis 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.

6.5. TREINAMENTOS

Habilidades, atitudes e conhecimentos necessários para o processo de desenvolvimento seguro de software deve ser promovido na DTI através capacitações especializadas na escrita de código seguro. Tais capacitações são necessárias para promoção da cultura de segurança dentro das equipes técnicas de desenvolvimento e sustentação de aplicações.

Da mesma forma, normas, procedimentos e instruções de trabalho baseados em boas práticas de desenvolvimento seguro para os sistemas de informação, tanto para a elaboração de novos quanto para manutenção dos existentes devem ser escritos e modelados pelo Escritório de Processos da DTI.

Cabe ressaltar que os mesmos princípios e normativos de desenvolvimento seguro aplicados no desenvolvimento interno serão replicados para os mantidos e/ou desenvolvidos pelas empresas terceirizadas, prestadores (as) de serviços e fábricas de software.

6.6. ACESSO A CÓDIGO FONTE E REPOSITÓRIO

Os códigos-fonte deverão ser hospedados em repositórios internos e custodiados pela DTI. Havendo necessidade de hospedagem em plataformas remotas para uma melhor colaboração e controle de versões, tais como, o **GitHub** (opção preferida para repositórios públicos), **GitLab** (plataforma baseada em nuvem) ou **Bitbucket** (opção preferida para repositórios privados) ou outros especificados pela Arquitetura de Soluções, eles irão requerer autorização e validação prévia.

O acesso aos repositórios deverá ser protegido por autenticação segura, ou seja, utilização de senhas fortes.

Dependendo da sensibilidade do código ou de outros arquivos relacionados ao desenvolvimento, os mesmos poderão ser criptografados (criptografia de disco, criptografia de arquivo ou criptografia de transporte) para impedir o acesso não autorizado, em conformidade comas as regras definidas nas **Políticas Corporativa de Segurança da Informação** e **Privacidade e Proteção de Dados Pessoais do TCE-AL**.

6.7. CONTROLE DE VERSÕES (VERSIONAMENTO)

A equipe de Desenvolvimento e Sustentação de Aplicações na DTI utiliza, onde aplicável, um sistema de controle e de versão (numeração, datas etc) e aplica nos ambientes de desenvolvimento, homologação/teste 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/teste e/ou produção, denominados de "releases" (lançamentos). Da mesma forma, qualquer alteração não emergencial nos sistemas de informação deverá ser incluída no próximo lançamento, de acordo com a capacidade operacional da equipe de Desenvolvimento e Sustentação de Aplicações e seguindo a ordem de priorização definida pela DTI.

A cada ciclo de desenvolvimento, a equipe de Desenvolvimento e Sustentação de Aplicações informará sua capacidade operacional, a fim de suportar a DTI na priorização de suas demandas em detrimento dos seguintes fatores:

a) número de recursos/horas disponíveis para cada lançamento;
b) demandas emergenciais impostas por alterações legais ou normativas;
c) projetos definidos no Planejamento Estratégico do TCE-AL;
d) projetos definidos como prioritários pela Presidência do TCE-AL ou DTI.

6.8. CÓPIAS DE SEGURANÇA

Os sistemas de informações da DTI 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 da **Política de Backup e Recuperação de Dados.**

6.9. PROPRIEDADE INTELECTUAL

O uso não autorizado de software ou sistema de informação de propriedade intelectual da DTI, como reprodução, modificação, distribuição ou qualquer outra forma de uso das aplicações sem permissão expressa da Diretoria, é proibido.

7. ATRIBUIÇÕES E RESPONSABILIDADES

Nesta política são estabelecias funções e responsabilidades no sentido de assegurar confiabilidade no desenvolvimento seguro de softwares e soluções de TI, sempre prezando pela confidencialidade, integridade, disponibilidade e autenticidade dos dados e serviços prestados pela DTI, conforme seguem:

7.1. DA DIRETORIA DE TI

A DTI atua proativamente promovendo ações de conscientização e monitoramento contínuo das diretrizes previstas nesta política e demais normativos descritos no **Item 4 – Referências** para manutenção do processo de desenvolvimento seguro dos ativos de software aplicados em todas as áreas meio e finalísticas do TCE-AL.

7.2. DO NÚCLEO DE SEGURANÇA DA INFORMAÇÃO

Trabalha com as equipes de desenvolvimento e sustentação para ajudá-las a identificar riscos de segurança e privacidade durante todo o ciclo de vida do software e garantir que as melhores práticas de segurança estejam mapeadas e integradas ao processo de desenvolvimento desde a concepção até a entrega final do produto/serviço.

7.3. DA EQUIPE ENVOLVIDA NA GESTÃO E DESENVOLVIMENTO DE SOFTWARE

Os recursos humanos alocados no processo de desenvolvimento e manutenção dos ativos de software assumem os seguinte papéis e responsabilidades:

a) Cliente: pessoa ou área requisitante dos serviços de desenvolvimento de software que define e prioriza, em conjunto com o Gerente de Projeto, os requisitos da solução a ser entregue;

b) Gerente de Projeto: responsável por liderar e apoiar o desenvolvimento do software, ajudando a resolver problemas técnicos com a finalidade de garantir a entrega de valor esperado de cada fase de desenvolvimento e do produto do projeto;

c) Desenvolvedor: responsável pelo desenvolvimento dos incrementos do software, codificando itens do produto, realizando testes unitários e de integração para assegurar que a solução esteja alinhada com os requisitos especificados no planejamento;

d) Administrador de Banco de Dados: assessora os gerentes de projetos na modelagem de dados de suas aplicações e gerência dos bancos de dados, incluindo planos para a sua definição, padronização, organização, proteção e utilização, assegurando a qualidade das informações;

e) Analista de Testes e Qualidade: analisa os incrementos de software e avalia a qualidade dos artefatos entregues a partir da identificação de técnicas, ferramentas e diretrizes apropriadas para gerenciar os testes de software;

f) Analista de Infraestrutura: prepara e mantém os ambientes de TI e a infraestrutura de hardware e software necessária para assegurar o desenvolvimento dos projetos de software;

g) Equipe de Operação: formada pelas equipes de Sustentação (manutenção dos sistemas) e Central de Serviços (suporte ao usuário interno e externo ao Tribunal) atuando em conjunto para garantir a estabilidade e disponibilidade contínua dos ativos de software da DTI ao longo do tempo;

h) Fábrica de Software: empresas especializadas responsáveis pelas atividades técnicas de desenvolvimento de projetos de softwares na DTI do TCE-AL;

i) Núcleo de Segurança da Informação: atua indiretamente nas políticas de tratamento de dados.

7.4. DA EQUIPE ENVOLVIDA NA CONTRATAÇÃO DOS SERVIÇOS DE FÁBRICA DE SOFTWARE

O cumprimento das diretrizes descritas nesta Política deve ser observado na elaboração de contratos de desenvolvimento, manutenção ou aquisição de ativos de software. Os recursos humanos alocados nesta atividade assumem os seguintes papéis e responsabilidades:

a) Gestor do Contrato: coordena e comanda o processo de gestão e fiscalização da execução contratual;
b) Fiscal Técnico do Contrato: fiscaliza tecnicamente o contrato avaliando, aceitando ou rejeitando os serviços das ordens de serviço;
c) Preposto: acompanha a execução do contrato e atua como interlocutor principal junto à contratante, incumbido de receber, diligenciar, encaminhar e responder as principais questões técnicas, legais e administrativas referentes ao andamento contratual.
d) Governança: emissão das Ordens de Serviços (OS), acompanhamento e no ateste/pagamento dos fornecedores.

8. CICLO DE VIDA DO DESENVOLVIMENTO DO SOFTWARE

A Norma ABNT ISO/IEC 27001:2022 para Gestão da Segurança da Informação, Segurança Cibernética e Proteção à Privacidade direciona o uso de um ciclo de vida de desenvolvimento seguro onde devem ser estabelecidas regras para o desenvolvimento de software, sistemas e aplicações.

A Política em tela aborda duas modalidades para o desenvolvimento seguro:

8.1. SDL (CICLO DE VIDA DO DESENVOLVIMENTO SEGURO)

O SDL (Ciclo de Vida de Desenvolvimento Seguro) onde são estabelecidas práticas de segurança durante o desenvolvimento objetivando a redução dos custos de manutenção de

software e aumento da confiabilidade no que se refere a falhas de segurança. Incorpora requisitos e ferramentas específicas de tecnologia estruturadas nas seguintes fases:

a) Treinamento: capacitação efetiva é importante para analistas e desenvolvedores entenderem os princípios de segurança e possam construir sistemas, aplicações, softwares e produtos mais seguros enquanto ainda visam atender as necessidades do negócio;

b) Requisitos de Segurança: devem ser continuamente mapeados e atualizados durante a concepção e planejamento da solução para refletir as mudanças no cenário de ameaças e minimizar interrupções por problemas de segurança;

c) Conformidade: níveis de qualidade de segurança mínimos aceitáveis precisam ser definidos no início do processo objetivando apoiar a equipe de desenvolvimento no entendimento dos riscos associados a problemas de segurança, identificação e correção de defeitos e aplicação de padrões de segurança ao longo de todo o ciclo de construção do software;

d) Modelagem de Ameaças: técnica capaz de auxiliar na proteção de sistemas, aplicativos, softwares, redes e serviços identificando possíveis ameaças e desenvolvendo estratégias de mitigação de risco no ciclo de vida de desenvolvimento a partir de um diagrama de fluxo de dados mostrando graficamente como todo o sistema funciona;

e) Requisitos de Desenho: desenho de fluxo de dados (DFDs) são criados para representar visualmente as principais interações, tipos de dados, portas e protocolos utilizados, bem como, identificar e atribuir prioridades a ameaças de mitigação que são adicionadas aos requisitos de segurança do software;

f) Padrões de Criptografia: uso de padrões claros de criptografia é de suma importância, dentro do aplicável, para garantir que todos os dados, incluindo as informações sigilosas estejam protegidos de vazamento não intencionais ou alterações quando transmitidos ou armazenados;

g) Testes de Análise Estática: aplicado pelos desenvolvedores para encontrar certas falhas de funções não seguras ou banidas e as substituem por alternativas mais seguras conforme os mesmos estão escrevendo o código;

h) Teste de Análise Dinâmica: verificação em tempo de execução em um software, sistemas ou aplicações totalmente compilados objetivando checar as funcionalidades que só ficam aparentes quando todos os componentes estão integrados e rodando.

8.2. SDLC (CICLO DE VIDA DO DESENVOLVIMENTO ÁGIL DE SOFTWARE)

O SDLC (Ciclo de Vida de Desenvolvimento Ágil de Software) onde de fato é estabelecido um processo dividido em etapas bem definidas de desenvolvimento seguindo uma abordagem ágil, flexível, progresso iterativo e melhoria contínua, assim descritas:

a) Análise de Requisitos: etapa onde é definido o que a aplicação deve fazer (quais necessidades serão atendidas), todos os recursos que serão incluídos e os obstáculos ao longo do caminho;

b) Projeto e Implementação: etapa onde é definido o projeto/desenho da solução adequando a arquitetura e tecnologia usadas e a implementação. Após a definição do desenho é possível criar um protótipo de uma versão anterior do software para demonstrar uma ideia básica da aparência de uma aplicação, como ela responderá e o que é capaz de fazer. É neste momento que os desenvolvedores recebem um retorno das partes interessadas para aprovação e/ou modificação da aplicação;

c) Revisão de Código: etapa onde o código e solução produzidos são revisados para garantir que os objetivos funcionais e não funcionais, que são passíveis de detectar através da análise do código (a exemplo da manutenibilidade, disponibilidade e performance), necessários sejam atendidos;

d) Homologação/Teste: etapa na qual a solução é continuamente testada com objetivo de encontrar falhas no desempenho e funcionamento. Isso reduz o número de erros que os usuários podem encontrar ao usar a aplicação, bem como, sua maior satisfação;

e) Produção: completado todo o ciclo de desenvolvimento para cada uma das funcionalidades, correções e melhorias esperadas é feita a publicação em produção podendo ser manual ou automatizada a depender da complexidade e das necessidades da aplicação.

9. GUIA DE DESENVOLVIMENTO DE SOFTWARE SEGURO

A construção segura de software e aplicações exige um conhecimento básico dos princípios de segurança (confidencialidade, integridade, disponibilidade e autenticidade) de forma que as operações de negócios sejam bem-sucedidas.

A equipe de Desenvolvimento e Sustentação de Aplicações na DTI considera a segurança como uma das regras mais importantes do planejamento para o desenvolvimento, motivo pelo qual, faz uso da metodologia **OWASP** (Projeto Aberto de Segurança de Aplicações Web) para garantir um padrão de qualidade em suas aplicações e sistemas. Cabe ressaltar que, apesar de usar o termo aplicações web em seu nome a OWASP também trabalha com aplicações mobile, nuvem, APIs, entre outros.

Na condição de guiar e proteger os desenvolvedores contra ameaças durante a elaboração do código de software, sistemas e aplicações, a comunidade OWASP divulga e atualizada periodicamente as vulnerabilidades mis comuns no meio dos crimes cibernéticos, abaixo descritas, e detalhadas na **Política de Gestão e Análise de Vulnerabilidades de TI**:

a) Controle de acesso quebrado;

b) Falhas de criptografia;

c) Injeção;

d) Desenho Inseguro;

e) Configurações incorretas de segurança;

f) Componentes desatualizados e vulneráveis;

g) Falhas de identificação e autenticação;
h) Falhas de software e de integridade dos dados;
i) Falhas no registro e monitoramento de segurança;
j) Falsificação de solicitação do lado do servidor.

Apesar de mencionar apenas dez, o que significa aparentemente que outras vulnerabilidades ficam de fora, estas são utilizadas como principal referência pelos desenvolvedores como forma de tornar os softwares, plataformas, redes e sistemas mais seguros contra as mais recentes, e principais, estratégias utilizadas por usuários mal-intencionados.

Ainda dentro do propósito de guiar e recomendar a OWASP fornece uma lista de práticas gerais de segurança a serem seguidas com objetivo de reduzir e /ou eliminar os impactos de alguma ameaça explorar as vulnerabilidades acima mencionadas, assim descritas:

a) Ter claramente os papéis e responsabilidades bem definidos;
b) Promover formação adequada em segurança no desenvolvimento;
c) Implementar um ciclo de desenvolvimento seguro;
d) Estabelecer padrões de programação segura;
e) Construir uma biblioteca reutilizável ou fazer uso de uma biblioteca de segurança;
f) Verificar a efetividade dos controles de segurança;
g) Estabelecer práticas para garantir a segurança quando há terceirização no desenvolvimento, incluindo a definição dos requisitos de segurança e metodologias de verificação tanto para os requisitos das propostas, como para o contrato a ser firmado entre as partes envolvidas.

Do exposto, vale mencionar que o guia OWASP é um documento de conscientização o qual pode ser aplicado como um padrão de referência, porém não um exclusivo ponto de partida para o desenvolvimento de aplicações seguras ou para testes. Outras metodologias e documentos devem ser considerados para evitar ao máximo os riscos e problemas que podem surgir no ambiente de TI.

10. SEGREGAÇÃO DE AMBIENTES

Atualmente a DTI adota a regra básica de segregação dos ambientes em desenvolvimento, homologação/teste e produção. O princípio chave é assegurar a integridade e disponibilidade (dois dos pilares da segurança da informação) do ambiente computacional e os dados que nele residem, proteger contra acesso não-autorizado, alterações e outros impactos negativos.

A separação do ambiente operacional evita a contaminação cruzada de aplicativos e é uma prática recomendada no ciclo de vida de desenvolvimento de sistemas. Ao fazer isso, a DTI busca impedir que o software seja usado em produção antes de estar pronto.

Ao isolar ambientes de aplicativos as equipes de TI podem ajudar a evitar interrupções, erros e violações de conformidade que podem afetar negativamente a prestação dos serviços de qualidade da DTI às áreas meio e finalística do Tribunal.

11. DADOS EM AMBIENTE DE HOMOLOGAÇÃO/TESTE

A sistemática de desenvolvimento seguro na DTI envolve uma série de atividades nas quais é muito comum a ocorrência de erros que podem acontecer durante todo o processo, desde a concepção até a construção das aplicações, sistemas e softwares. A tarefa de homologação/teste se propõe a auxiliar na descoberta destes erros, o quanto antes, para que o custo da correção dos mesmos seja o menor possível.

A fase de homologação/teste é um estágio importante no ciclo de vida do desenvolvimento de software e pode decidir o destino final da qualidade das soluções que estão sendo lançadas no ambiente de TI da DTI. Assim sendo, é muito importante garantir que o ambiente usado para homologar/testar seja confiável e o mais próximo possível da produção.

O uso de dados pessoais no ambiente de homologação/teste constitui um dos assuntos mais críticos, uma vez que, o tipo específico de dados a serem processados ou a função do sistema podem exigir o uso dos dados de produção para homologar/testar adequadamente seus recursos. Ambiente de homologação/teste, na maioria das vezes, não é tão completo quanto o de

produção, então certos componentes de um sistema só podem ser testados adequadamente em um cenário ativo.

Como, em determinadas situações, pode não ser possível replicar um processo particularmente especializado dentro do ambiente de homologação/teste devido limitações do próprio processo ou dos dados que ele requer, para garantir a segurança dos mesmos e não prejudicar uma efetiva validação do software, sistema ou aplicação, algumas medidas são necessárias e aplicadas pela DTI.

Todos os dados pessoais usados no ambiente de homologação/teste devem ser estritamente relevantes para o propósito, listados e identificados como:

a) Não pessoais;
b) Pessoais;
c) Pessoais sensíveis.

Uma vez que os dados tenham sido classificados, em conformidade com as diretrizes definidas pelo **Manual de Classificação e Tratamento de Informações Sigilosas**, as razões para inclusão no ambiente de homologação/teste devem ser fornecidas, caso contrário, os mesmos não devem ser usados.

Da mesma forma, torna-se importante a configuração de uma trilha de auditoria no ambiente de homologação/teste para capturar erros durante o processo de validação do sistema, software ou aplicação e permitir a correção imediata. As verificações de integridade devem ser realizadas nos dados que estão sendo alimentados, especialmente se houver a possibilidade de serem mesclados com outros ou realimentados no sistema de origem.

Por fim, é necessário ter mecanismos para garantir que os dados de homologação/teste não sejam retidos por mais tempo do que o necessário com foco no atendimento dos normativos legais do Tribunal, bem como, dados pessoais sensíveis não sejam divulgados para realização de testes por terceiros, prestadores de serviços e fábricas de software.

12. PENALIDADES

Esta Política de Desenvolvimento Seguro, juntamente com os documentos descritos no **Item 4 – Referências**, compõem o conjunto de normativos da DTI os quais direcionam atitudes e comportamentos exigidos aos colaboradores no tocante à proteção dos ativos de TI devendo ser rigorosamente observados.

O descumprimento desta Política será considerado infração disciplinar e poderá acarretar a aplicação de sanções previstas nos normativos da DTI e disposições contratuais.

13. IMPLEMENTAÇÃO E ATUALIZAÇÃO

Espera-se que a Política de Desenvolvimento Seguro seja revisada continuamente e, em intervalos planejados, seguindo as regras dos normativos internos da DTI, não se restringindo apenas a estes. Caso uma parte interessada identifique uma melhoria ela deve ser desenvolvida e implantada dentro do possível e onde for aplicável.

A DTI deve assegurar que as revisões desta política sejam amplamente divulgadas com objetivo de promover a sua observância e cumprimento. Ademais, recursos humanos e tecnológicos devem ser disponibilizados para garantir a execução das regras nela contidos.

14. CONTROLE DE DOCUMENTOS E REGISTE RO

Código	Responsável pela guarda	Permissão de acesso	Meio de arquivo	Indexação	Local de arquivo	Tempo de Arquivo	Forma de Disposição
PL-DTI-009	DTI	Restrito ao setor	Eletrônico	Alfabética	Base de Conhecimento	Permanente	Não aplicável

15. ANEXOS

Não se aplica.

16. HISTÓRICO DAS REVISÕES

Revi-são	Descrição das alterações	Data
00	Emissão Inicial	13/08/2024
01	Padronização da documentação	14/08/2024
02	Inclusão de texto no item 6. Princípios, Diretrizes e Requisitos; Alteração de texto no item 6.7. Controle de Versões (Versionamento); Alteração de texto no item 7.3. Da Equipe Envolvida na Gestão e Desenvolvimento de Softwares, subitem d; Inclusão de texto no item 7.3. Da Equipe Envolvida na Gestão e Desenvolvimento de Softwares, subitem h; Inclusão de texto no item 7.4. Da Equipe Envolvida na Contratação dos Serviços de Fábrica de Softwares, subitem d;	03/10/2024

Elaborado por:	Analisado e Aprovado por:
Equipe de Processos e Projetos	**Diretoria de TI**
Data da Elaboração: 13/08/2024	Data da Aprovação: 21/11/2024