Processo de Desenvolvimento Seguro de Software

Abril de 2026

SUMÁRIO

INFORMAÇÃO

O documento contempla a apresentação das características do **processo de Desenvolvimento Seguro de Software** utilizado no âmbito do Tribunal Regional Federal da 6ª Região (TRF6), contendo seu objetivo, políticas e demais informações necessárias para se manter e executar de forma correta este processo.

FINALIDADE DO DOCUMENTO

O objetivo deste documento é detalhar as características que determinam o modo de funcionamento do **processo de Desenvolvimento Seguro de Software**, apresentando as políticas a serem seguidas, o processo com suas entradas e saídas, seus controles e responsáveis por atividades no processo, visando ser mais seguro e eficiente no desenvolvimento, sustentação e implantação de sistemas no âmbito do TRF6.

CONCEITOS E DEFINIÇÕES

a. **SUDES:** Subsecretaria de desenvolvimento de soluções.
b. **ETIR (Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação):** Grupo de trabalho responsável por identificar, analisar, responder e mitigar incidentes de segurança, visando reduzir impactos e restaurar a normalidade dos serviços;
c. **Vulnerabilidade:** Fragilidade ou falha em um sistema, processo ou controle que pode ser explorada para comprometer a segurança da informação;
d. **CSTI:** Central de atendimento aos usuários.
e. **AN:** Área de negócio.
f. **CGTIC:** Comitê de Governança de Tecnologia da Informação e Comunicação
g. **Usuário:** Indivíduo responsável por solicitar e testar correções e melhorias em sistemas.
h. **Software/Sistema:** Aplicações utilizadas dentro da infraestrutura do TRF6, divididas entre "Administrativas" e Judiciais".
i. **Homologação**: A homologação envolve validar uma versão do sistema com o usuário ou demandante em ambiente controlado (não-produção) com a finalidade de aprovação para que esta versão seja liberada para implantação em ambiente de produção.
j. **Produção:** Local onde um sistema, software ou aplicação é executado para uso real pelos usuários finais, após ter passado por todas as fases de desenvolvimento, testes e homologação.
k. **Kanban:** Metodologia de gestão visual de trabalho que visa melhorar a eficiência e o fluxo de processos.

PRÁTICAS DO PROCESSO

O **Processo de Desenvolvimento Seguro de Software** deve ser iniciado em conjunto com os processos de Desenvolvimento e Sustentação de Sistemas. Uma vez identificada uma vulnerabilidade, esta deve ser devidamente tratada e integrada ao Processo de Resposta a Incidentes de Segurança da Informação, seguindo as fases estabelecidas no Guia de Comunicação e Resposta a Incidentes de Segurança da Informação (GCRISI-JF6):

I. Recebimento de notificação de vulnerabilidades;
II. Classificação das vulnerabilidades quanto a gravidade para priorização;
III. Análise de riscos das vulnerabilidades;
IV. Correção das vulnerabilidades;
V. Notificação da correção das vulnerabilidades;
VI. Análise da causa raiz das vulnerabilidades.

Práticas Técnicas

I. O modelo de desenvolvimento seguro de software deve adotar o princípio do privilégio mínimo, assegurando que os desenvolvedores possuam apenas os acessos estritamente necessários para a execução de suas atividades. A concessão de permissões deve ser controlada, temporária, quando aplicável, e revisada periodicamente, de forma a reduzir riscos de acesso indevido, vazamento de informações e comprometimento dos ambientes de desenvolvimento, teste e produção.
II. Para garantir segurança no processo de desenvolvimento deve-se, dentro das possibilidades, seguir as seguintes diretrizes:
    a) Manter treinamento contínuo dos desenvolvedores;
    b) Utilizar ferramentas para o gerenciamento de configurações (exemplo: controle de versões/mudanças, automação de deploys, entre outros);
    c) Usar bibliotecas seguras;
    d) Utilizar ferramentas de análise de código (SAST) para analisar padrões de configuração seguras e convenções;
    e) Utilizar ferramentas de teste dinâmico (DAST) de código visando encontrar vulnerabilidades. Manter os softwares atualizados;
    f) Avaliar os riscos de segurança e propor ações de combate.

III. Para o uso de componentes de software (ou software completo) de terceiros, somente será admitido se estiverem atualizados e forem adquiridos de fontes confiáveis, além de certificar-se de que suas distribuições estejam em desenvolvimento e manutenção ativos.

IV. Antes da utilização dos componentes, esses deverão passar por análise de vulnerabilidades e consulta em bancos de dados de vulnerabilidades disponíveis na internet como o NIST - National Vulnerability Database (NVD) ou outras fontes confiáveis.

V. Os ambientes de Sistemas de Produção e Não Produção deverão ser especificados e mantidos separados.

Práticas de Processo

I. O processo de desenvolvimento de seguro de software deverá estar alinhado com os padrões mínimos:

a) Privacy By Design: assegura a proteção de dados pessoais deverá 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;

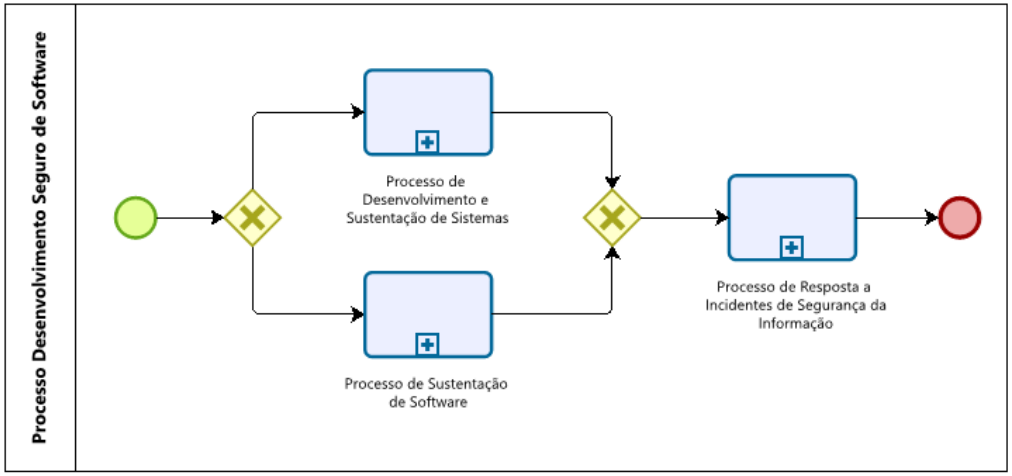
b) Privacy By Default: o software deverá resguardar a exposição de dados pessoais salvaguardando a privacidade, sendo o mais restritivo possível tanto na exposição/visualização de dados pessoais quanto na coleta.

c) O processo de desenvolvimento seguro deve se basear na Lei Geral de Proteção de Dados.

II. Os casos omissos e eventuais dúvidas quanto à aplicação desta norma serão dirimidos pela Comitê de Governança em Segurança da Informação deste Tribunal, que contará com membros da equipe de desenvolvimento para reuniões temáticas.

JUSTIÇA FEDERAL
TRF 6º REGIÃO

DESENHO DO PROCESSO



Legendas Objetos BPMN

Sustentação de Software

Desenvolvimento de Sistemas

Resposta a Incidentes SI

Nota 01: Para acessar o fluxo deve-se clicar duas vezes no ícone de fluxo acima para visualizar o fluxograma em PDF.
Nota 02: Legenda dos principais objetos utilizados em modelagem de processos/subprocessos.

REVISÕES

Controle de Versões					
Título:	Processo de desenvolvimento Seguro de Software				
Código:		Criado em: 07/04/2026	Revisado: 28/04/2026	Versão:	1.0
Classificação:	Interna Informação	Elaborador(es):	Matheus Gonzalez Giovani Gomes		
		Revisor(es):	Jane Pereira Samuel Taveira Rodrigo Vieira Fernando Garcia		
Gestão do Documento:		Governança de TIC			