Processo de Desenvolvimento Seguro de Software do STJ

- Guia de Referência –

Janeiro 2022

Versão 1.0

Sumário

1. Termos e Definições

Para os fins deste processo, são considerados:

I. ameaça: conjunto de fatores externos ou causa potencial de incidente indesejado que podem resultar em dano para um sistema ou organização;

II. 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;

III. 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;

IV. 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;

V. ativo de software: item de solução de Tecnologia da Informação e Comunicação constituído por software

VI. 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;

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

VIII. 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;

IX. 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;

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

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

XII. integridade: propriedade de salvaguarda da exatidão e completude da informação;

XIII. recuperação segura em caso de falha: modelo no qual a falha no processamento de um controle de segurança resulte no mesmo caminho que seria executado no caso de uma vedação emitida por tal controle;

XIV. requisitos de segurança: conjunto de necessidades de segurança que o sistema deve atender, sendo tais necessidades influenciadas fortemente pela política de segurança da organização, 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. São exemplos de requisitos não funcionais, dentre outros, a validação das entradas de dados e o registro de logs de auditoria com informações suficientes para análise forense;

XV. segurança da informação: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade e a confidencialidade das informações;

XVI. 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;

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

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

2. Princípios e Diretrizes

Devem ser observados os seguintes princípios e diretrizes para o desenvolvimento de softwares no âmbito do STJ:

I. identificar, definir, validar e documentar, no ciclo de vida de qualquer demanda, os requisitos de segurança a que os ativos de software deverão atender;

II. implementar controle de acesso baseado em papéis ou perfis de usuários, preferencialmente por meio de componentes isolados;

III. implementar controles de segurança necessários para proteger os ativos de informação e informações digitais, de acordo com a sua criticidade.

a) usar controles de segurança como componentes, de forma que sejam catalogados e reutilizados em outros ativos de software;

IV. implementar os controles de segurança em múltiplas camadas da arquitetura do ativo de software (negócios, dados, aplicações e tecnologia), de acordo com a criticidade das informações tratadas;

V. construir o ativo de software de forma que suas mensagens de erro não revelem detalhes de sua estrutura interna ou a configuração do ambiente;

VI. verificar o atendimento dos requisitos de segurança do software, por meio de análise estática e/ou análise dinâmica, preferencialmente na fase de construção;

VII. identificar e corrigir as vulnerabilidades encontradas anteriormente à entrada de qualquer ativo de software em produção, segundo um critério de prioridade e de aceitação do risco;

VIII. observar os seguintes procedimentos para o ativo de software desenvolvido, quando da passagem para o ambiente de produção:

a) remover arquivos desnecessários para o funcionamento do ativo de software, informações sigilosas nos comentários de código e contas criadas para teste;

b) usar arquivos externos de configuração, adequadamente protegidos contra acesso e alteração indevidos e não implementar parâmetros de configuração dentro do código.

IX. recuperar-se de modo seguro em caso de falha;

X. registrar em logs todos os eventos relevantes para o negócio e para a segurança da informação, com o armazenamento de informações suficientes para investigação e análise forense:

a) os logs que permitam a construção de uma trilha de auditoria deverão ser protegidos de forma consistente com o contexto da aplicação e dos processos de negócios envolvidos;

XI. utilizar controles de segurança da informação específicos para os ativos de software;

XII. utilizar criptografia para a transmissão de dados nos ativos de software que possuam a necessidade de controle de acesso ou lidem com dados sigilosos;

XIII. gerenciar e revalidar os controles de segurança da informação, na fase de manutenção do ativo de software;

XIV. obedecer a Política de Segurança da Informação do STJ;

XV. possuir conformidade com requisitos e normativos vigentes relacionados à privacidade e dados abertos em recursos de Tecnologia da Informação, quando aplicável;

XVI. atender, quando aplicável, a padrões relacionados à segurança da informação que venham a ser recomendados pelo Comitês Diretivos do Conselho Nacional de Justiça.

3. Competências e Responsabilidades

Os envolvidos no processo de desenvolvimento e manutenção de ativos de software no Superior Tribunal de Justiça deverão receber treinamento em segurança de software.

Os desenvolvedores de ativos de software têm como responsabilidade:

I. planejar o desenvolvimento de ativos de software, utilizando como referência os requisitos técnicos de segurança do presente processo e do Guia para Desenvolvimento Seguro de Software.
II. testar o ativo de software implementado para assegurar os requisitos de segurança da informação implementados.
III. resolver ou mitigar as vulnerabilidades de alto impacto dos sistemas desenvolvidos antes de colocá-los em produção.

A Coordenadoria de Desenvolvimento de Soluções de Software será responsável por:

I. acompanhar o cumprimento das diretrizes previstas neste Processo de Desenvolvimento Seguro de Software e no Guia para Desenvolvimento Seguro de Software.
II. promover a conscientização da área de TI em relação à relevância do desenvolvimento seguro para o STJ, mediante campanhas, palestras, *workshops*, treinamentos e outros meios de endomarketing.
III. apoiar a avaliação e a adequação de controles específicos de desenvolvimento seguro para novos sistemas ativos de software.

4. Contratação de Desenvolvimento ou Aquisição de Ativos de Software

O cumprimento deste processo deve ser observado na elaboração de contratos de desenvolvimento ou manutenção ou aquisição de ativos de software, no quer couber.

I. Nas condições contratuais de suporte para o ativo de software, devem ser previstas as correções de vulnerabilidades que venham a ser identificadas na solução desenvolvida pela empresa terceirizada.
II. Para o caso de ativos de software adquiridos, durante a vigência de sua garantia, o fabricante ou fornecedor da solução deverá corrigir eventuais vulnerabilidades identificadas.

Nos processos de contratação voltados ao desenvolvimento de sistemas por terceiros, sugere-se que seja incluído na seção referente à transição contratual a necessidade de confecção do Relatório de Avaliação da Execução Contratual.

Neste relatório deverá constar o registro e a análise crítica das lições aprendidas ao longo da execução contratual, bem como eventuais apontamentos com vistas a aperfeiçoar os requisitos da contratação voltados ao desenvolvimento seguro, em consonância com os princípios e diretrizes da Política de Segurança da Informação do STJ e deste Processo de Desenvolvimento Seguro de Software.