UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO
SUPERINTENDÊNCIA DE TECNOLOGIA DA INFORMAÇÃO

INSTRUÇÃO NORMATIVA POSIN/STI Nº 11, DE 24 DE NOVEMBRO DE 2025

Estabelece diretrizes e procedimentos para o desenvolvimento de software seguro no âmbito da Universidade Federal do Espírito Santo.

O SUPERINTENDENTE DE TECNOLOGIA DA INFORMAÇÃO DA UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO no uso das suas atribuições e considerando o disposto na Lei nº 13.709 (Lei Geral de Proteção de Dados Pessoais - LGPD), de 14 de agosto de 2018, no Programa de Privacidade e Segurança da Informação (PPSI) do Governo Federal e na Política de Segurança da Informação desta Universidade, resolve:

CAPÍTULO I

DISPOSIÇÕES PRELIMINARES

Art. 1º Esta Instrução Normativa estabelece diretrizes e procedimentos para garantir o desenvolvimento de software seguro no âmbito da Universidade Federal do Espírito Santo (Ufes).

Art. 2º Para os fins desta Instrução Normativa, considera-se:

I. Desenvolvimento de Software Seguro: Processo de criação de software com práticas que garantem a proteção contra vulnerabilidades e ameaças à segurança;
II. Ciclo de Vida do Desenvolvimento de Software: Conjunto de fases que um software atravessa desde sua concepção até sua descontinuação.

CAPÍTULO II

DOS PRINCÍPIOS E DIRETRIZES

Art. 3º O desenvolvimento de software seguro visa:

I. Proteger a confidencialidade, integridade e disponibilidade das informações processadas pelos sistemas;
II. Assegurar que os sistemas desenvolvidos estejam conforme as normativas de segurança da informação e legislações aplicáveis;
III. Promover a reutilização de componentes seguros e homologados pela Superintendência de Tecnologia da Informação (STI); e
IV. Garantir que a proteção de dados e privacidade sejam considerados desde a concepção até a descontinuação, passando por todo o ciclo de vida do desenvolvimento de software.

Art. 4º São princípios que regem o desenvolvimento de software seguro:

I. Segurança por Design: Incorporar requisitos de segurança desde a fase inicial do desenvolvimento;
II. Validação Contínua: Realizar testes de segurança em todas as etapas do desenvolvimento;
III. Atualização e Manutenção: Garantir que os sistemas sejam atualizados regularmente para corrigir vulnerabilidades.

CAPÍTULO III

DO PROCESSO DE DESENVOLVIMENTO

Art. 5º O processo de desenvolvimento de software seguro deve incluir:

I. Análise de Requisitos: Identificação e documentação de requisitos de segurança específicos para cada projeto;
II. Design Seguro: Planejamento da arquitetura do software com foco em segurança;
III. Implementação Segura: Uso de práticas de codificação segura e revisão de código;
IV. Testes de Segurança: Execução de testes de penetração, análise de vulnerabilidades e revisões de segurança;
V. Implantação e Monitoramento: Implementação em ambiente seguro e monitoramento contínuo para detecção de anomalias.

Art. 6º Nos softwares e sistemas desenvolvidos por setores da Ufes, deverão ser observados:

I. A reutilização de código, priorizando soluções existentes no sistema de versionamento;
II. O uso de linguagens, bibliotecas e frameworks homologados pela STI;
III. O uso de arquitetura e padrões de projeto homologados pela STI;
IV. O uso de protocolos criptografados de comunicação, como HTTPS em vez de HTTP.

Art. 7º Todos os sistemas desenvolvidos por setores da Ufes deverão ser hospedados na infraestrutura da STI, e quaisquer alterações devem ser previamente homologadas em um ambiente controlado, derivado do ambiente de produção, antes de ser publicado.

Art. 8º Nos casos de contratação de serviços de desenvolvimento de software, o contrato deverá:

I. Estabelecer critérios objetivos para o aceite das entregas, com base nas especificações técnicas definidas no termo de referência, assegurando a conformidade com normas de qualidade e padrões de mercado;
II. Definir o processo de desenvolvimento a ser empregado, incluindo metodologias, normas técnicas e frameworks, segundo as diretrizes estabelecidas pelo governo federal;
III. Assegurar que os princípios, padrões e processos adotados estejam alinhados às diretrizes do governo federal, em especial às regras e práticas definidas pelo Modelo de Contratação de Serviços de Desenvolvimento e Sustentação de Software instituído pela Portaria SGD/ME nº 5.651/2022;
IV. Atender as regras estabelecidas pela Instrução Normativa SGD/ME nº 94;
V. Atender às condições específicas estabelecidas em Atas de Registro de Preços (ARP) publicadas pelo órgão central do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP), quando aplicável.

CAPÍTULO IV

DAS RESPONSABILIDADES

Art. 9º. Compete à Superintendência de Tecnologia da Informação (STI):

I. Estabelecer diretrizes para o desenvolvimento de software seguro;
II. Realizar verificações periódicas nos sistemas desenvolvidos para garantir a conformidade com as normas de segurança;
III. Promover capacitações e treinamentos em segurança da informação para as equipes de desenvolvimento da própria STI;
IV. Disponibilizar uma ferramenta onde as unidades estratégicas registrem as suas necessidades de desenvolvimento de novas funcionalidades;
V. Disponibilizar uma ferramenta onde os usuários possam reportar incidentes ocorridos na operação dos sistemas; e
VI. Disponibilizar aos desenvolvedores um sistema de controle de versionamento de código unificado para controle de histórico e evolução do software.

Art. 10. Compete às equipes de desenvolvimento:

I. Seguir as diretrizes estabelecidas nesta Instrução Normativa e na Política de Segurança da Informação (Posin) da Ufes;
II. Documentar todas as etapas do desenvolvimento, incluindo decisões de segurança e justificativas;
III. Reportar à STI quaisquer riscos ou vulnerabilidades identificados durante o desenvolvimento.

CAPÍTULO V

DA GESTÃO DE VULNERABILIDADES

Art. 11. A gestão de vulnerabilidades deve incluir:

I. Identificação e Registro: Catalogação de todas as vulnerabilidades identificadas;
II. Análise de Impacto: Avaliação do impacto potencial de cada vulnerabilidade sobre os sistemas;
III. Correção e Verificação: Implementação de correções e verificação da eficácia das mesmas;
IV. Comunicação: Notificação adequada às partes interessadas sobre as vulnerabilidades e ações tomadas.

CAPÍTULO VI

DISPOSIÇÕES FINAIS

Art. 12. Compete à Superintendência de Tecnologia da Informação (STI) orientar e fiscalizar o cumprimento desta Instrução Normativa.

Art. 13. Os casos omissos serão resolvidos pelo Comitê de Governança Digital da Ufes.

Art. 14. Esta Instrução Normativa entra em vigor na data de sua publicação.

Documento assinado digitalmente
gov.br
PAULO ALEXANDRE LOBATO
Data: 08/12/2025 16:54:38-0300
Verifique em https://validar.iti.gov.br

PAULO ALEXANDRE LOBATO

Superintendente de Tecnologia da Informação