SECRETARIA ESTADUAL DE SAÚDE DE PERNAMBUCO — SES-PE
Sistema de Gestão de Segurança da Informação (SGSI)
ANEXO G – CONTROLE DE PUBLICAÇÕES DE SISTEMA PARA PRODUÇÃO
Portaria nº 129/2026 — SES-PE

Documento Complementar à Política de Segurança da Informação – SES/PE

Versão: 1.0

Data de Emissão:

Periodicidade de Revisão: Anual ou conforme necessidade

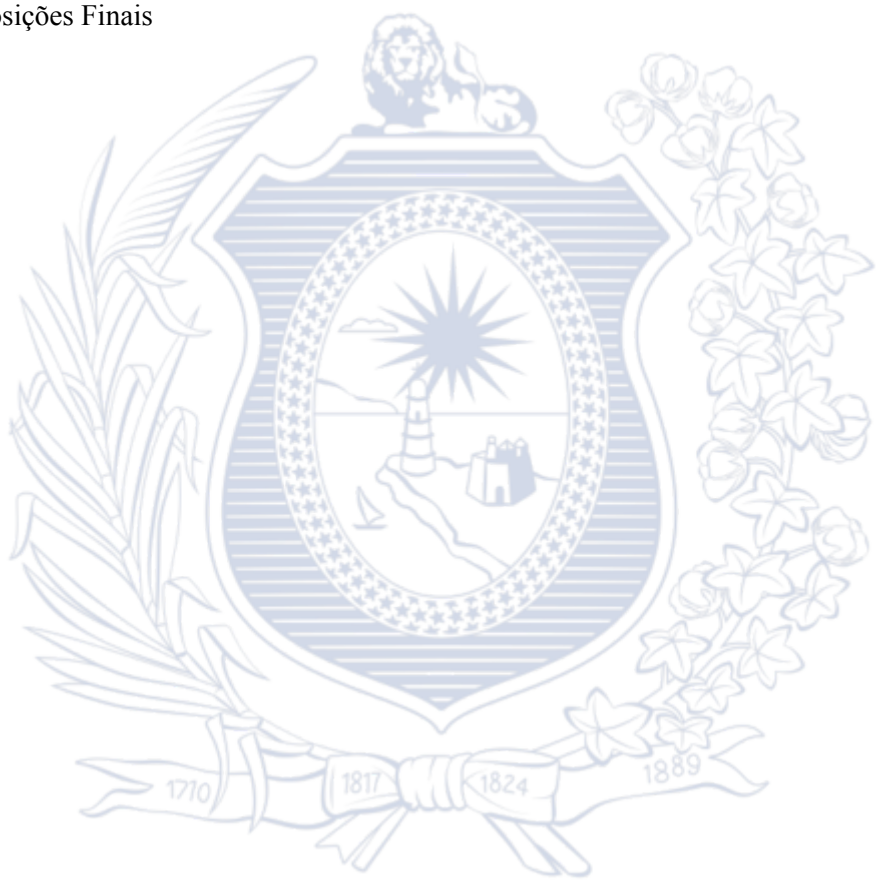
Responsável pela Elaboração: Comitê de Segurança da Informação (CSI/SES)

Status: VIGENTE

Descrição:

Este anexo define os critérios, processos e responsabilidades para controle de publicações de sistemas no ambiente de produção da **SECRETARIA ESTADUAL DE SAÚDE DE PERNAMBUCO — SES-PE**, assegurando que alterações sejam feitas de forma segura, validada e padronizada, minimizando riscos técnicos e operacionais.

Sumário



1. Definição

O **Controle de Publicações de Sistema para Produção** refere-se ao conjunto de procedimentos, critérios e responsabilidades estabelecidos para garantir que qualquer modificação, atualização ou nova funcionalidade de sistemas corporativos da Secretaria Estadual de Saúde de Pernambuco (SES/PE) seja devidamente validada, aprovada e executada de forma segura e controlada no ambiente de produção.

2. Objetivo

Assegurar que todas as alterações realizadas em sistemas de informação sejam executadas de maneira padronizada, evitando falhas, indisponibilidades, vulnerabilidades de segurança e impactos negativos aos serviços essenciais de saúde prestados à população.

3. Diretrizes

Nenhuma alteração ou publicação será realizada diretamente em ambiente de produção sem prévia validação e autorização formal da área de tecnologia da informação e das áreas usuárias envolvidas.

Todas as publicações devem ser precedidas de:

- Registro em sistema de chamados ou ferramenta de controle de mudanças;
- Aprovação formal do Comitê Gestor de Mudanças ou responsável designado;
- Execução de testes em ambiente de homologação com evidências documentadas;
- Análise de riscos e plano de rollback (reversão);
- Verificação de conformidade com os requisitos de segurança da informação.
- As credenciais de acesso ao ambiente de produção devem ser controladas e restritas aos profissionais autorizados.
- Todo processo de publicação deverá ser auditável, com registros completos de data, hora, responsáveis, descrição da mudança e sistemas impactados.
- Publicações emergenciais devem seguir fluxo específico, com registro justificado e documentação posterior à ação.

3.1. Desenvolvimento Seguro

Assegurar que os sistemas e aplicações desenvolvidos ou adquiridos pela SES-PE incorporem segurança desde a sua concepção, seguindo as melhores práticas de desenvolvimento seguro, as diretrizes da Política de Segurança da Informação e as

recomendações de segurança reconhecidas pela indústria, como as da Open Web Application Security Project (OWASP).

Este processo inclui a realização de:

- **Análise de Requisitos de Segurança:** Identificação e documentação dos requisitos de segurança no início do ciclo de vida do desenvolvimento de software, garantindo a proteção de dados e a confidencialidade.
- **Segurança em Aplicações Web:** Para aplicações web, deverão ser implementadas práticas que mitiguem vulnerabilidades comuns (OWASP Top 10), incluindo validação de entradas, autenticação robusta e proteção contra CSRF.
- **Servidores Web:** Deve-se implementar restrições de diretório, bloqueio de execução de scripts em pastas de upload e WAF. As configurações de *hardening* mandatórias para servidores Apache, Nginx e IIS estão disponíveis no **Apêndice Técnico 01**.
- **Segurança de Infraestrutura e Sistema Operacional:** O sistema operacional que hospeda a aplicação deve passar por processo de *hardening* para mitigar riscos de acesso remoto não autorizado, exploração de vulnerabilidades e movimentação lateral.

  Para servidores **Linux**, seguir os requisitos de segurança definidos no **Apêndice Técnico 02**.

  Para servidores **Windows**, seguir os requisitos de segurança definidos no **Apêndice Técnico 03**.
- **Monitoramento:** Implementação de logs de segurança para detecção contínua de atividades maliciosas.

3.2. Referência à OWASP Top 10

As equipes de desenvolvimento e segurança devem considerar ativamente as categorias de riscos mais críticas para aplicações web, conforme a lista OWASP Top 10 (última versão vigente), como um guia essencial para identificar, prevenir e mitigar vulnerabilidades. As principais categorias de riscos abordadas pela OWASP Top 10 incluem, mas não se limitam a:

- **Quebra de Controle de Acesso (Broken Access Control):** Falhas na implementação de controles de acesso que permitem que usuários acessem funcionalidades ou dados não autorizados.
- **Falhas Criptográficas (Cryptographic Failures):** Proteção inadequada de dados sensíveis em trânsito e em repouso, levando à exposição de informações confidenciais.
- **Injeção (Injection):** Falhas que permitem a execução de comandos maliciosos em um interpretador (ex: SQL Injection, Command Injection).
- **Design Inseguro (Insecure Design):** Falhas fundamentais de design ou arquitetura que introduzem vulnerabilidades.

- **Configuração de Segurança Incorreta (Security Misconfiguration):** Configurações de segurança padronizadas, incompletas ou ausentes em sistemas e aplicações.
- **Componentes Vulneráveis e Desatualizados (Vulnerable and Outdated Components):** Utilização de bibliotecas, *frameworks* ou outros componentes com vulnerabilidades conhecidas.
- **Falhas de Identificação e Autenticação (Identification and Authentication Failures):** Erros na implementação de mecanismos de autenticação que podem ser explorados para comprometer credenciais.
- **Falhas de Integridade de Software e Dados (Software and Data Integrity Failures):** Riscos relacionados a atualizações de software, dados críticos e *pipelines* de CI/CD sem validação de integridade.
- **Falhas de Registro e Monitoramento de Segurança (Security Logging & Monitoring Failures):** Insuficiência ou ausência de logs de segurança e monitoramento adequado de eventos.
- **Falsificação de Requisições do Lado do Servidor (Server-Side Request Forgery - SSRF):** Falhas que permitem a um invasor fazer com que o servidor de uma aplicação realize requisições HTTP para um domínio arbitrário.

3.3. Documentação e Rastreabilidade da Aplicação

Criação e manutenção de documentação detalhada para cada sistema ou aplicação, abrangendo:

- Identificação dos responsáveis pela criação e manutenção.
- Plataforma ou sistema operacional em que a aplicação está rodando.
- Endereços IP (interno e externo), se aplicável.
- URLs utilizadas para acesso.
- Dependências de software e bibliotecas.
- Data de criação e histórico de versões.
- Fluxos de dados e interações com outros sistemas.
- Diagramas de arquitetura e infraestrutura.
- Registro de todas as alterações relevantes e seus respectivos impactos.

Esta documentação deve ser acessível às equipes de segurança e TI para facilitar a identificação, análise e mitigação proativa de potenciais vulnerabilidades, bem como para apoiar a resposta a incidentes de segurança da informação.

4. Responsabilidades

- **Setor de Tecnologia da Informação (TI)**: Planejar, autorizar, executar e monitorar as publicações, mantendo a rastreabilidade e segurança do processo.

- **Gestores de Sistemas/Usuários Chave**: Participar da homologação, validação e aprovação das mudanças.

- **Comitê Gestor de Mudanças (CGM)**: Avaliar impactos, riscos e aprovar publicações em sistemas críticos.

5. Disposições Finais

Este anexo integra a Portaria nº **129/2026** e deve ser revisto anualmente ou quando necessário.