



GOVERNO DE
PER
NAM
BU
CO
ESTADO DE MUDANÇA

SECRETARIA ESTADUAL DE SAÚDE DE PERNAMBUCO — SES-PE
Sistema de Gestão de Segurança da Informação (SGSI)
ANEXO E – POLÍTICAS DE SENHAS E CONTROLE DE ALTERAÇÕES
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)

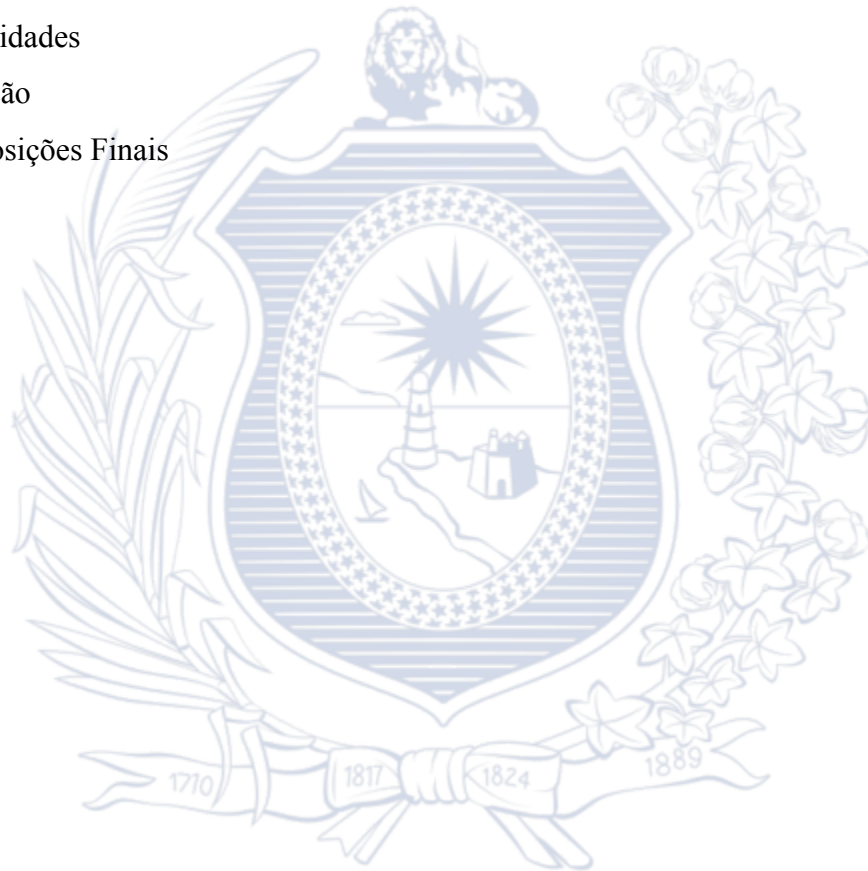
Status: VIGENTE

Descrição:

Estabelece as diretrizes e os requisitos mínimos para a criação, uso e proteção de senhas, bem como os procedimentos para o controle de alterações em sistemas e aplicações da Secretaria Estadual de Saúde de Pernambuco (SES-PE). O objetivo é garantir a autenticação segura, minimizar riscos de acesso não autorizado e assegurar a rastreabilidade e integridade das modificações nos ambientes tecnológicos institucionais.

Sumário

1. Objetivo	3
2. Escopo	3
3. Políticas de Senhas e Controle de Alterações	3
3.1 Políticas de Senhas	3
3.2 Controle de Alterações	3
4. Responsabilidades	3
5. Penalidades	4
6. Revisão	4
7. Disposições Finais	4



1. Objetivo

Estabelecer diretrizes e controles para assegurar que o acesso a recursos físicos e lógicos da Secretaria Estadual de Saúde de Pernambuco (SES-PE) seja restrito apenas a pessoas autorizadas, minimizando riscos de acesso não autorizado, perda, roubo ou comprometimento de informações sensíveis.

2. Escopo

Este plano se aplica a todos os servidores, terceirizados, estagiários, prestadores de serviço, consultores e qualquer pessoa que utilize ou acesse os recursos físicos e tecnológicos da SES-PE.

3. Políticas de Senhas e Controle de Alterações

3.1 Políticas de Senhas

- Senhas devem conter no mínimo 8 caracteres e incluir combinação de letras maiúsculas e minúsculas, números e caracteres especiais.
- As senhas devem ser alteradas a cada 90 dias ou imediatamente em caso de suspeita de comprometimento.
- Não é permitido o reuso das últimas 5 senhas utilizadas.
- As senhas não devem ser compartilhadas ou anotadas em locais de fácil acesso.
- Sempre que possível, deve-se utilizar autenticação multifator (MFA).

3.2 Controle de Alterações

- Todas as alterações em sistemas, aplicações e configurações devem seguir processos de gestão de mudanças aprovados.
- As mudanças devem ser documentadas e registradas, incluindo autorização, impacto, testes e responsáveis.
- Alterações críticas devem passar por avaliação de risco e validação da equipe de segurança da informação.
- Todos os ambientes de produção devem possuir mecanismos de controle de versão e de auditoria.

4. Responsabilidades

- Gestores: Garantir que o controle de acesso lógico e físico seja implementado e monitorado em suas áreas.
- Equipe de TI/Segurança da Informação: Gerenciar os mecanismos de autenticação, logs, auditorias e infraestrutura de segurança.
- Usuários: Utilizar seus acessos de forma responsável e comunicar qualquer uso indevido, perda de equipamento ou suspeita de violação.

5. Penalidades

O descumprimento das diretrizes desta política poderá acarretar sanções administrativas, civis e/ou penais, conforme legislação vigente, incluindo a LGPD (Lei Geral de Proteção de Dados Pessoais - Lei nº 13.709/2018).

6. Revisão

Este plano deve ser revisado anualmente ou sempre que houver mudanças significativas nas operações, legislação ou no ambiente tecnológico da SES-PE.

7. Disposições Finais

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

