SECRETARIA ESTADUAL DE SAÚDE DE PERNAMBUCO — SES-PE
Sistema de Gestão de Segurança da Informação (SGSI)
ANEXO A – CONTROLE DE ACESSO LÓGICO E FÍSICO
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 estabelece as diretrizes para o controle de acesso físico e lógico aos ambientes e ativos de informação da SES-PE. O objetivo é garantir que apenas pessoas autorizadas tenham acesso às informações, sistemas e infraestruturas, de acordo com os princípios de confidencialidade, integridade e disponibilidade.

Sumário

1. Objetivo

Definir os critérios, mecanismos e responsabilidades para assegurar o controle de acesso físico e lógico aos ativos informacionais da Secretaria Estadual de Saúde de Pernambuco (SES-PE), garantindo a proteção contra acessos não autorizados, uso indevido ou divulgação indevida de informações.

2. Abrangência

Aplica-se a todos os ambientes, recursos computacionais, sistemas de informação, redes, documentos físicos e digitais sob responsabilidade da SES-PE, incluindo acesso por servidores, terceirizados, estagiários, prestadores de serviço, consultores e qualquer pessoa que utilize ou acesse os recursos físicos e tecnológicos da SES-PE.

3. Diretrizes Gerais

- O acesso aos recursos informacionais deve ser concedido conforme o princípio do menor privilégio e da real necessidade de negócio.
- Todos os acessos devem ser individualizados e autenticados.
- É proibido o compartilhamento de credenciais de acesso.
- Todo acesso deverá ser registrado, monitorado e revisado periodicamente.

4. Acesso Lógico

Implantar mecanismos de autenticação segura (senha forte mínimo de 8 caracteres, incluindo letras, números e símbolos, autenticação em dois fatores quando aplicável).

- Controlar o acesso a sistemas e redes com base em perfis de usuários.
- Realizar o bloqueio automático de sessões inativas.
- Manter registros (logs) de acesso por tempo definido em política interna.
- Garantir que os acessos de usuários desligados sejam imediatamente revogados.
- As contas devem ser desativadas imediatamente após desligamento ou mudança de função do colaborador.
- Contas privilegiadas devem ser controladas, monitoradas e utilizadas apenas quando necessário.
- Os acessos devem ser revistos periodicamente (pelo menos a cada 6 meses).
- Os acessos remotos serão permitidos somente por canais criptografados (VPN) e com autorização prévia
- O acesso remoto a sistemas sensíveis deve ser logado e auditado.

5. Acesso Físico

Controlar fisicamente o acesso a salas técnicas, data centers e locais que armazenem informações sensíveis.

- Utilizar mecanismos como crachás identificadores, fechaduras eletrônicas, câmeras e registros de entrada.

- Garantir que visitantes ou terceiros sejam sempre identificados e acompanhados por servidor autorizado.
- Implementar barreiras físicas e controles de acesso em áreas críticas.

6. Responsabilidades

- Comitê de Segurança da Informação: define diretrizes e supervisiona sua aplicação.
- Gestores de unidades: autorizam acessos dentro de sua alçada e monitoram a conformidade.
- Área de TI: implementa controles técnicos e realiza auditoria de acessos.
- Usuários: Utilizar seus acessos de forma responsável e comunicar qualquer uso indevido, perda de equipamento ou suspeita de violação.

7. Penalidades e Sanções

O descumprimento das diretrizes estabelecidas neste anexo poderá implicar em responsabilização administrativa, civil e/ou penal, conforme a gravidade da infração e legislação vigente.

8. Auditoria e Revisão

O controle de acesso será auditado regularmente e poderá ser revisado sempre que houver mudanças significativas na estrutura organizacional, tecnológica ou normativa.

9. Disposições Finais

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