



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 F – PLANO DE CONTROLE DE BACKUP
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 diretrizes e requisitos mínimos para uso no plano de controle de backup institucionais da SES-PE, conforme a Política de Segurança da Informação.

Sumário

1. Introdução	3
2. Objetivo	3
3. Abrangência	3
4. Diretrizes Gerais	3
5. Frequência e Tipos de Backup	3
6. Armazenamento e Retenção	3
7. Testes e Validações	4
8. Disposições Finais	4
9. Disposições Finais	4



1. Introdução

Este anexo estabelece as diretrizes e procedimentos para a realização de cópias de segurança (backup) no âmbito da Secretaria Estadual de Saúde de Pernambuco (SES-PE), com base na Política de Segurança da Informação.

2. Objetivo

Garantir a proteção, recuperação e integridade dos dados e informações institucionais da SES-PE em caso de perda, falha, erro humano, desastre natural ou incidente de segurança.

3. Abrangência

Aplica-se a todos os sistemas de informação, bancos de dados, arquivos eletrônicos e demais ativos digitais críticos sob responsabilidade da SECRETARIA ESTADUAL DE SAÚDE – SES/PE.

4. Diretrizes Gerais

- Os backups devem ser realizados de forma periódica, automatizada sempre que possível, e monitorados por equipe responsável.
- Devem ser contemplados backups completos, diferenciais e incrementais, conforme criticidade e volume da informação.
- O processo de backup deve estar documentado e protegido contra alterações não autorizadas.

5. Frequência e Tipos de Backup

- Backup completo: semanal.
- Backup incremental: diário.
- Backup sob demanda: sempre que houver atualização crítica.
- Sistemas essenciais de saúde devem ter backups em tempo quase real, quando tecnicamente possível.

6. Armazenamento e Retenção

- Os arquivos de backup devem ser armazenados em locais seguros, com controle de acesso, preferencialmente com cópias em unidades externas e/ou ambientes em nuvem institucional.
- A retenção dos dados deve respeitar a legislação vigente, políticas internas e a criticidade dos dados.
- Backups antigos devem ser descartados com segurança após o período de retenção.

7. Testes e Validações

Os backups devem ser periodicamente testados e validados para assegurar sua efetividade. Falhas devem ser registradas, analisadas e tratadas tempestivamente.

8. Disposições Finais

Este plano será revisado anualmente ou sempre que houver mudanças relevantes na infraestrutura, processos ou riscos tecnológicos. Sua implementação é obrigatória e está vinculada às diretrizes da Política de Segurança da Informação da SES-PE.

9. Disposições Finais

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

