SECRETARIA ESTADUAL DE SAÚDE DE PERNAMBUCO — SES-PE
Sistema de Gestão de Segurança da Informação (SGSI)
ANEXO D – PLANO DE RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO
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 e procedimentos para a identificação, registro, análise, contenção, resposta, recuperação e documentação de incidentes de segurança da informação que afetem os ativos da Secretaria Estadual de Saúde de Pernambuco (SES-PE), garantindo a mitigação de impactos, a continuidade dos serviços e o fortalecimento das práticas preventivas.

Sumário

1. Objetivo
Estabelecer diretrizes e procedimentos para resposta a incidentes de segurança da informação que afetem os ativos da SES-PE.

2. Abrangência
Aplica-se a todos os ambientes tecnológicos, dados, redes, servidores e sistemas da SES-PE, bem como a todos que tenham acesso a esses ativos.

3. Definições
Incidente de Segurança da Informação: Evento que compromete, ou pode comprometer, a segurança da informação.
Evento de Segurança: Ocorrência que pode indicar um incidente.

4. Classificação dos Incidentes
Os incidentes devem ser avaliados por tipo, escopo, origem, natureza e impacto nos ativos e processos.

Apêndice X – Formulários de Resposta à Incidentes de SI

5. Ciclo de Resposta
O ciclo de resposta a incidentes da SES-PE é composto pelas seguintes fases, que devem ser executadas de forma coordenada:

Identificação: Detecção de eventos que podem constituir um incidente.

Registro: Abertura formal da ocorrência no sistema de chamados.

Classificação: Definição da severidade e prioridade do incidente.

Notificação: Comunicação às partes interessadas conforme a matriz de escalonamento.

Análise: Investigação da causa raiz, extensão e impacto.

Contenção: Medidas imediatas para limitar o dano (ex: isolar rede, suspender serviços).

Recuperação: Restauração dos sistemas e dados para a operação normal.

Documentação e Aprimoramento: Registro detalhado das ações e lições aprendidas para evitar reincidência.

O uso dos Formulários de Notificação Inicial e de Relatório Pós-Incidente (Apêndice X) é obrigatório para todos os incidentes classificados, devendo estes ser anexados ao ticket da ocorrência para fins de auditoria.

5.1. Requisitos para Correções e Recuperação

Qualquer alteração em sistemas, aplicações ou configurações de servidores realizada durante as fases de Contenção ou Recuperação (ex: aplicação de hotfixes, patches de segurança ou ajustes de hardening) deve observar obrigatoriamente as diretrizes do ANEXO G – CONTROLE DE PUBLICAÇÕES DE SISTEMA PARA PRODUÇÃO.

Em casos críticos que exijam ação imediata para conter um ataque ativo, deve-se seguir o fluxo de Publicação Emergencial previsto no referido anexo, garantindo a documentação, validação e aprovação posterior da mudança para assegurar a conformidade do ambiente.

6. Responsabilidades

- Comitê: supervisiona e aprova relatórios.
- Equipes Técnicas: realizam contenção e análise.
- Gestores: informam e apoiam ações corretivas.
- Usuários: notificam qualquer suspeita.

7. Comunicação de Incidentes

- E-mail: incidentes.si@saude.pe.gov.br

8. Disposições Finais

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