SECRETARIA ESTADUAL DE SAÚDE DE PERNAMBUCO — SES-PE
Sistema de Gestão de Segurança da Informação (SGSI)
ANEXO H – POLÍTICA DE CLASSIFICAÇÃO E ROTULAGEM 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 institui a Política de Classificação e Rotulagem da Informação da SES-PE, estabelecendo os níveis formais de classificação (pública, interna, restrita e sigilosa), os critérios de enquadramento, os rótulos padronizados e as regras de manuseio aplicáveis a todo o ciclo de vida da informação, em qualquer meio ou ambiente em que se encontre.

Esta política está alinhada às normas de transparência, segurança da informação e proteção de dados pessoais vigentes, em especial ao Decreto nº 49.914/2020 (Política Estadual de Segurança da Informação – PESI), ao Decreto nº 38.787/2012, que regulamenta a Lei nº

14.804/2012, à Lei nº 12.527/2011 (Lei de Acesso à Informação – LAI), e à Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD).

Sumário

1. Objetivo

Estabelecer os níveis oficiais de **classificação, rotulagem e regras de manuseio** do dado no âmbito da SES-PE, viabilizando que cada informação receba proteção proporcional ao risco e esteja em conformidade com a Política de Segurança da Informação da Secretaria de Saúde (PSI-SES/PE) e com as normas vigentes.

2. Escopo

Aplica-se a **todas as informações** produzidas, recebidas ou custodiadas pela SES-PE, em qualquer **meio** (físico ou digital), **fase do ciclo de vida** (criação, uso, armazenamento, transmissão e descarte) e **ambiente** (infraestrutura própria, computação em nuvem, dispositivos móveis, mídias removíveis ou com terceiros/fornecedores).

3. Integração com a Política de Segurança da Informação da SES/PE

Esta política integra-se aos seguintes anexos da PSI :

- **Anexo A – Controle de Acesso Lógico e Físico:** concessão de acessos baseada no princípio do menor privilégio e no nível de classificação;
- **Anexo B – Gerenciamento de Ativos:** inventário e proteção de ativos de informação por nível;
- **Anexo C – Criptografia e Proteção de Dados:** requisitos de criptografia e salvaguardas proporcionais ao nível;
- **Anexo D – Resposta a Incidentes:** severidade e tratamento de incidentes considerando o nível da informação;
- **Anexo E – Políticas de Senhas e Controle de Alterações:** reforço de autenticação e rastreabilidade por criticidade;
- **Anexo F – Controle de Backup:** política de retenção e proteção por nível;
- **Anexo G – Controle de Publicações de Sistema para Produção:** validação de rótulos e dados sensíveis antes da promoção.

4. Definições

- **informação:** dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;
- **informação pessoal:** informação relacionada à pessoa natural identificada ou identificável, relativa à intimidade, vida privada, honra e imagem;
- **classificação da informação:** categorização da informação segundo o impacto potencial à Confidencialidade, Integridade e Disponibilidade (CID), à conformidade legal e ao risco para a missão institucional;
- **rotulagem da informação:** marcação visível e/ou uso de metadados que indiquem o nível de classificação e, quando aplicável, o proprietário da informação e o prazo de retenção;
- **gestor do processo, da informação ou do sistema:** unidade administrativa ou agente responsável pela produção, custódia ou utilização da informação, no âmbito de processos de trabalho e sistemas sob sua responsabilidade funcional, no exercício de atividades finalísticas ou de apoio;
- **autoridade classificadora:** agente responsável por classificar informações em grau de sigilo, nos termos do art. 13 da Lei nº 14.804/2012. No âmbito da SES/PE, a autoridade classificadora é o Secretário de Saúde;
- **autoridade classificadora por delegação de competência:** pessoa formalmente designada para exercer atribuições de classificação no limite da delegação conferida, conforme § 1º do art. 13 da Lei nº 14.804/2012;
- **Termo de Classificação de Informação (TCI):** documento que registra formalmente a decisão de classificação da informação, conforme modelo constante do Anexo II desta Política.

5. Níveis formais de classificação da informação

As informações produzidas, recebidas ou custodiadas no âmbito da SES/PE devem ser classificadas em um dos seguintes **níveis formais**, de acordo com o **impacto potencial** aos

pilares da Segurança da Informação (Confidencialidade, Integridade e Disponibilidade), às normas de proteção de dados e demais normas vigentes:

- **Informação pública:** é aquela de livre divulgação e acesso pelos cidadãos, disponibilizada por meio de transparência ativa ou passiva, e que não se enquadra em hipóteses legais de sigilo ou restrição.

São exemplos de informação pública, conforme art. 7º da Lei nº 12.527/2011 (LAI), aquelas que:

a) seja produzida ou acumulada por órgãos ou entidades públicas;

b) seja produzida ou mantida por pessoa física ou jurídica em razão de vínculo com a Administração Pública;

c) disponha sobre atividades, políticas, organização, estrutura ou serviços dos órgãos e entidades;

d) trate do patrimônio público, da utilização de recursos públicos, de processos licitatórios ou contratos; e

e) trate de políticas públicas, inspeções, auditorias, prestações e tomadas de contas.

Observação: quando um documento contiver, simultaneamente, informações públicas e dados pessoais, o acesso não deve ser negado. Nesses casos, deve-se proceder à anonimização ou ocultação das informações protegidas, garantindo ao cidadão o acesso ao conteúdo público remanescente, em observância aos princípios da transparência e do controle social.

- **Informação interna:** aquela destinada ao uso exclusivo do órgão, cujo acesso deve permanecer limitado aos servidores e colaboradores envolvidos nas atividades institucionais. Sua divulgação não autorizada pode gerar impacto operacional, organizacional ou de imagem à instituição, ainda que não se enquadre nas hipóteses legais de sigilo ou de restrição previstas na LAI.

São exemplos de documentos classificados como informação interna:

- memorandos, comunicações internas e despachos;
- manuais operacionais, instruções de serviço e notas técnicas internas;
- fluxos de processos, mapeamento de atividades e documentos de padronização interna.

Observação: caso o documento contenha informações sujeitas a proteção legal específica, o seu enquadramento deverá observar o nível de classificação correspondente ao conteúdo, prevalecendo o maior nível de proteção aplicável. Por exemplo, despachos que descrevem dados pessoais sensíveis deverão ser classificados como informação restrita, nos termos da legislação vigente.

- **Informação restrita:** aquela protegida por legislação específica, cujo acesso é limitado a pessoas ou unidades autorizadas e que, apesar da restrição, não demanda classificação em grau de sigilo.

São exemplos de informação restrita:

a) informações pessoais relativas à intimidade, vida privada, honra e imagem da pessoa;

b) documentos preparatórios utilizados como fundamento para a tomada de decisão e para a prática de ato administrativo, até a edição do respectivo ato decisório;

c) informações submetidas a hipóteses de restrição de acesso previstas em legislação específica, incluindo aquelas elencadas no Anexo I desta Política, excetuadas as classificadas em grau de sigilo.

- **Informação sigilosa:** é aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado, e aquelas abrangidas pelas demais hipóteses legais de sigilo.

Essas informações devem ser classificadas de acordo com os níveis e critérios especificados na LAI (ultrassecreta, secreta ou reservada).

São passíveis de classificação de sigilo as informações cuja divulgação ou acesso irrestrito possam:

a) prejudicar ou pôr em risco informações fornecidas em caráter sigiloso por outros Estados e organismos internacionais;
b) pôr em risco a vida, a segurança ou a saúde da população;
c) prejudicar ou causar risco a projetos de pesquisa e desenvolvimento científico ou tecnológico, assim como a sistemas, bens, instalações ou áreas de interesse estratégico estadual;
d) pôr em risco a segurança de instituições, servidores estaduais ou de autoridades estaduais; ou
e) comprometer atividades de inteligência, bem como de investigação ou fiscalização em andamento, relacionadas com a prevenção ou repressão de infrações.

A classificação dessas informações deve ser solicitada pelo gestor do processo à autoridade classificadora, por meio do Termo de Classificação de Informação (TCI), conforme modelo disposto no Anexo II desta Política.

6. Procedimentos de classificação, reclassificação e desclassificação da informação

A decisão que classificar a informação em qualquer grau de sigilo deve ser formalizada no Termo de Classificação de Informação - TCI, conforme modelo contido no Anexo II, e deve indicar:

a) o assunto sobre o qual versa a informação;

b) a identificação da autoridade que a classificou;

c) o dispositivo de lei ou ato normativo que permite a vedação do acesso à informação e/ou proíbe a divulgação da informação e/ou obriga a manutenção do sigilo quanto à informação;

d) o objetivo da Administração Pública ao impedir o acesso à informação, apontando por que deve prevalecer o interesse protegido pela recusa do acesso à informação em detrimento do interesse protegido pela divulgação da informação;

e) se a informação classificada pode ou não ser obtida de forma parcial; e

f) o prazo de sigilo, contado em anos, meses ou dias, ou do evento que defina o seu termo final, conforme limites previstos no art. 32, do Decreto nº 38.787/2012 (ultrassecreto: vinte e cinco anos; grau secreto: quinze anos; e grau reservado: cinco anos).

Quanto à iniciativa para classificação, reclassificação ou desclassificação de informações, observa-se que:

- **o gestor do processo ou da informação**: no exercício de suas atribuições, solicita à autoridade classificadora a classificação, reclassificação ou desclassificação da informação, mediante a formalização do Termo de Classificação de Informação (TCI), registrado no Sistema Eletrônico de Informações (SEI);
- **a autoridade classificadora**: classifica, reclassifica ou desclassifica informações de ofício ou mediante provocação, observados os prazos e procedimentos previstos no Decreto nº 38.787/2012, inclusive quanto à necessidade de encaminhamento ao Comitê de Acesso à Informação (CAI), para fins de padronização, quando aplicável;
- **qualquer interessado**: solicita, por meio dos canais oficiais de ouvidoria, a reclassificação ou desclassificação da informação, nos termos da legislação de acesso à informação.

7. Rotulagem

A rotulagem deve ser aplicada de forma visível e adequada ao meio utilizado:

- **Documentos e arquivos**: inserção, no cabeçalho, do nível de classificação, da identificação do proprietário da informação, da data e, quando aplicável, do prazo de retenção, conforme tabela de temporalidade;
- **E-mails**: prefixo do nível de classificação no campo “Assunto” (ex.: [RESTRITA]) e inclusão de aviso de confidencialidade no rodapé;

- **Relatórios, telas e sistemas**: exibição do nível de classificação em relatórios, exportações e interfaces que contenham informações internas, restritas ou sigilosas, por meio de marca d'água ou banner persistente;

- **Metadados e automação**: aplicação, quando disponíveis, de etiquetas de proteção com políticas associadas, tais como criptografia e prevenção contra perda de dados (DLP).

8. Regras de manuseio da informação por nível

- **Informação pública:**

a) **armazenamento:** repositórios públicos oficiais, assegurada a integridade da versão divulgada;
b) **transmissão e compartilhamento:** livre, observadas as diretrizes institucionais de comunicação;
c) **descarte:** reciclagem ou exclusão simples.

- **Informação Interna:**

a) **acesso**: autenticado, conforme Anexo A;

b) **armazenamento**: repositórios corporativos institucionais;

c) **transmissão**: evitar encaminhar essas informações a domínios externos, utilizar preferencialmente e-mails institucionais (@saude.pe.gov.br);

d) descarte: exclusão lógica conforme tabela de temporalidade.

- **Informação restrita:**

a) acesso: controle de acesso, registro de logs, auditorias e, quando aplicável, autenticação multifator;

b) armazenamento: criptografia obrigatória em repouso, proibição de mídias e dispositivos pessoais, controle de pastas compartilhadas e backup conforme Anexo F;

c) **transmissão:** criptografia em trânsito; controles técnicos conforme o Anexo C, uso de Rede Privada Virtual (VPN) para acesso remoto, bem como compartilhamento externo mediante autorização e instrumentos formais;

d) **impressão:** controlada, com retirada imediata do material impresso pelo responsável, sendo vedado o abandono de documentos em impressoras ou áreas comuns;

e) **descarte:** sanitização segura ou trituração de mídia física.

- **Informação sigilosa:**

a) **acesso:** aprovações formais, segregação de ambientes, contas nominativas, cofre de segredos e *JIT/break-glass* conforme Anexos A e D;

b) **armazenamento:** repositórios segregados, criptografia forte e chaves protegidas sem cópias em mídias removíveis;

c) **transmissão:** canais dedicados e criptografados, com registro e autorização prévia;

d) **descarte:** destruição física ou eliminação criptográfica, com registro do procedimento.

9. Responsabilidades

- **Gestor do processo ou da informação**: conduzir e supervisionar o tratamento dos processos e dados sob sua proteção, solicitar a classificação adequada das informações, justificar a necessidade de acesso, indicar prazos de retenção e critérios de descarte, se for o caso, bem como revisar periodicamente a adequação do nível de classificação, sem prejuízo da competência legal da autoridade classificadora, nos termos do Decreto nº 38.787/2012 e da Lei nº 12.527/2011;

- **Autoridade classificadora**: agente público legalmente competente para classificar, reclassificar ou desclassificar informações em grau de sigilo, de ofício ou mediante

provocação, observados os prazos, fundamentos e procedimentos previstos na Lei nº 12.527/2011 e no Decreto nº 38.787/2012 e em suas alterações;

- **Usuários**: servidores, colaboradores ou terceiros autorizados que acessam informações no exercício de suas atribuições. Compete-lhes cumprir os rótulos e as regras de manuseio correspondentes ao nível de classificação, não reduzir ou alterar indevidamente o nível de proteção atribuído, utilizar a informação exclusivamente para fins institucionais e reportar incidentes, acessos indevidos ou inconformidades relacionadas à segurança da informação;
- **Tecnologia da Informação e Segurança da Informação**: prover, manter e monitorar mecanismos técnicos e administrativos de controle de acesso, autenticação, criptografia, rastreabilidade, auditoria, resposta a incidentes e automação de rótulos, em consonância com os níveis de classificação definidos nesta Política e com a Política de Segurança da Informação da SES/PE;
- **Terceiros e fornecedores**: cumprir os requisitos de segurança da informação e proteção de dados equivalentes aos níveis de classificação definidos nesta Política, conforme previsto em contratos, termos de confidencialidade e demais instrumentos formais, respondendo por eventuais descumprimentos.

10. Conformidade e incidentes

O descumprimento das disposições desta Política caracteriza não conformidade administrativa e poderá ensejar a aplicação de sanções cabíveis, observado o devido processo legal, sem prejuízo das responsabilidades civil, administrativa e penal, conforme a legislação vigente.

Incidentes envolvendo vazamento, acesso indevido, destruição, perda, alteração ou qualquer forma de tratamento irregular de informação classificada deverão ser tratados nos termos do Anexo D da Política de Segurança da Informação da SES/PE.

Nos casos em que o incidente envolver dados pessoais, deverá ser realizada, adicionalmente, a comunicação à Encarregada pelo Tratamento de Dados Pessoais da

Secretaria, para adoção das providências previstas na Lei nº 13.709/2018 (LGPD) e demais normativos aplicáveis.

11. Exceções

As exceções às disposições desta Política deverão ser formalmente solicitadas por meio do SEI, mediante justificativa fundamentada, definição de prazo de vigência, identificação dos riscos envolvidos e indicação dos controles compensatórios adotados, e dependerão de aprovação do gestor do processo ou da informação e da área de Segurança da Informação.

Quando a exceção envolver dados pessoais ou dados pessoais sensíveis, a solicitação deverá ser submetida, adicionalmente, à avaliação da Encarregada pelo Tratamento de Dados Pessoais, a fim de verificar a conformidade com a LGPD e demais normativos aplicáveis.

12. Treinamento e conscientização

A classificação e o manuseio da informação deverão ser objeto de ações periódicas de capacitação e conscientização, com orientações práticas sobre a aplicação dos níveis, rótulos e controles previstos nesta Política.

13. Revisão e vigência

Esta Política deverá ser revisada anualmente ou sempre que houver alterações relevantes de ordem legal, regulatória ou tecnológica.

Esta Política entra em vigor na data de publicação da Política de Segurança da Informação da SES/PE (PSI-SES/PE).

ANEXO I

HIPÓTESES DE RESTRIÇÃO DE ACESSO

Hipótese Legal	Dispositivo Legal ou Regulatório
Atividade de Inteligência ou Fiscalização	Art. 23, VIII, da Lei Federal nº 12.527/2011
Controle Interno	Art. 26, §3º, da Lei Federal nº 10.180/2001
Direito Autoral	Art. 24, III, da Lei Federal nº 9.610/1998
Documento Preparatório	Art. 7º, §3º , da Lei Federal nº 12.527/2011
Informação Pessoal	Art. 31 da Lei Federal nº 12.527/2011 e Lei Federal nº 13.709/2018
Protocolo - Pendente Análise de Restrição	Art. 6º, II, da Lei Federal nº 12.527/2011
Investigação de Responsabilidade de Servidor	Art. 150 da Lei Federal nº 8.112/1990
Livros e Registros Contábeis Empresariais	Art. 1.190 do Código Civil
Operações Bancárias	Art. 1º da Lei Complementar Federal nº 105/2001
Ouvidoria	Art. 13, inciso V, e art. 15, inciso VIII, da Lei nº 16.420/2018
Proteção da Propriedade Intelectual de Software	Art. 2º da Lei Federal nº 9.609/1998

Risco à Segurança de Alta Autoridade Estadual	Art.11, IV, da Lei nº 14.804/2012
Risco à Segurança de Instituições Estaduais	Art.11, IV, da Lei nº 14.804/2012
Segredo de Justiça no Processo Civil	Art. 189 do Código de Processo Civil
Segredo de Justiça no Processo Penal	Art. 201, §6º, do Código de Processo Penal
Segredo Industrial	Art. 195, XIV da Lei Federal nº 9.279/1996
Serviço de abrigamento mulheres em situação de violência doméstica e familiar	Art. 2º, §1º, da Lei nº 13.977/2009
Sigilo das Comunicações	Art. 3º, V, da Lei Federal nº 9.472/1997
Sigilo de Empresa em Situação Falimentar	Art. 169 da Lei Federal nº 11.101/2005
Sigilo do Inquérito Policial	Art. 20 do Código de Processo Penal
Situação Econômico-Financeira de Sujeito Passivo	Art. 198, caput, da Lei Federal nº 5.172/1966

ANEXO II

TERMO DE CLASSIFICAÇÃO DE INFORMAÇÃO – TCI

Secretaria da Saúde — GOVERNO DE PERNAMBUCO — ESTADO DE MUDANÇA					SERVIÇO DE INFORMAÇÃO AO CIDADÃO	
TERMO DE CLASSIFICAÇÃO DE INFORMAÇÃO - TCI						Nº
ÓRGÃO/ENTIDADE:						
GRAU DE SIGILO:		Reservado		Secreto		Ultrassecreto
TIPO DE DOCUMENTO:						
DATA DA CLASSIFICAÇÃO:						
FUNDAMENTO LEGAL DA CLASSIFICAÇÃO:						
RAZÕES DA CLASSIFICAÇÃO/ RECLASSIFICAÇÃO/ DESCLASSIFICAÇÃO/ REDUÇÃO DO PRAZO:						
A INFORMAÇÃO PODE SER FORNECIDA DE FORMA PARCIAL?		SIM		NÃO		
SE PUDER SER FORNECIDA PARCIALMENTE, INDICAR QUE PARTE DA INFORMAÇÃO ESTÁ DISPONÍVEL:						
PRAZOS MÁXIMOS DE CLASSIFICAÇÃO CONFORME ARTIGO 32 C/C INCISO VI DO ARTIGO 33 DO DECRETO Nº 38.787/2012:						

AUTORIDADE CLASSIFICADORA:	Nome:	
	Cargo:	
	Matrícula:	
CIÊNCIA DO CAI: (§ 2º DO ARTIGO 30 DO DECRETO Nº 38.787/2012	Nome:	
	Cargo:	
	Matrícula:	
	Nome:	
	Cargo:	

DESCLASSIFICAÇÃO EM _____/_____/_____	Matrícula:	
RECLASSIFICAÇÃO EM _____/_____/_____	Nome:	
	Cargo:	
	Matrícula:	
REDUÇÃO DE PRAZO EM ____/_____/_____	Nome:	
	Cargo:	
	Matrícula:	

_____

Assinatura da Autoridade Classificadora

_____

Assinatura da Autoridade do CAI

_____

Assinatura da Autoridade Responsável pela Desclassificação

_____

Assinatura da Autoridade Responsável pela Reclassificação

_____

Assinatura da Autoridade Responsável pela Redução do Prazo