SECRETARIA DE ESTADO DE TRABALHO E RENDA

DESPACHO DO ORDENADOR DE DESPESAS DE 30/03/2026

PROCESSO Nº SEI-210001/036367/2025 - RECONHEÇO a Dívida de Exercício Anterior e **AUTORIZO** a execução da despesa no valor de R$ 147.615,59 (cento e quarenta e sete mil seiscentos e quinze reais e cinquenta e nove centavos), por Delegação de Competência Resolução SETRAB nº 1070, de 20 de março de 2026, em favor da UG: 250100 - SECRETARIA DE ESTADO DE POLÍCIA PENAL - SEPPEN, referente à Ressarcimento de Pessoal Requisitado no exercício de 2025.

Id: 2725357

Secretaria de Estado de Transformação Digital

SECRETARIA DE ESTADO DE TRANSFORMAÇÃO DIGITAL

ATO DO SECRETÁRIO

RESOLUÇÃO SETD Nº 142 DE 24 DE MARÇO DE 2026

ESTABELECE DIRETRIZES E PROCEDIMENTO MÍNIMO PARA ANONIMIZAÇÃO E PSEUDONIMIZAÇÃO DE DADOS PESSOAIS, INCLUSIVE DADOS PESSOAIS SENSÍVEIS, NO ÂMBITO DOS ÓRGÃOS E ENTIDADES DO PODER EXECUTIVO DO ESTADO DO RIO DE JANEIRO, E DÁ OUTRAS PROVIDÊNCIAS.

O SECRETÁRIO DE ESTADO DE TRANSFORMAÇÃO DIGITAL, no uso de suas atribuições legais e regulamentares, considerando a necessidade de padronizar procedimentos e evidências para aplicação de técnicas de proteção de dados pessoais no âmbito do Poder Executivo Estadual, tendo em vista o que consta no Processo nº SEI-430001/000175/2026, e

CONSIDERANDO:

- a Lei Federal nº 8.159 de 8 de janeiro de 1991 (Política Nacional de Arquivos Públicos e Privados);

- a Lei Federal nº 12.527 de 18 de novembro de 2011 (Lei de Acesso à Informação - LAI);

- a Lei Federal nº 13.709 de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais - LGPD), especialmente, o disposto no art. 1º; no art. 5º, incisos II e XI; no art. 14; e no art. 16, § 1º, inciso I;

- o Decreto Estadual nº 48.891 de 10 de janeiro de 2024, atinente a Política de Governança em Privacidade e Proteção de Dados Pessoais do Estado do Rio de Janeiro, especialmente, o disposto no art. 7º, § 1º; no art. 18, § 2º; e no art. 24, parágrafo único;

- o Acórdão nº 506/2025-TCU-Plenário, atinente ao processo de concessão e restrição de acesso a informações pessoais;

- a competência do Núcleo Normativo do Comitê de Governança em Privacidade e Proteção de Dados Pessoais, nos termos do art. 33 do Decreto Estadual nº 48.891/2024; e

- a necessidade de padronizar procedimentos mínimos, critérios de validação e modelos de evidência documental para a aplicação de anonimização e pseudonimização em documentos, processos administrativos e bases de dados, inclusive para fins de auditoria, controle e encerramento contratual sem dependência de fornecedor.

RESOLVE:

Disposições Preliminares

Art. 1º - Esta Resolução estabelece diretrizes e procedimentos mínimos para anonimização e pseudonimização de dados pessoais, inclusive dados pessoais sensíveis, aplicáveis a documentos, processos administrativos e bases de dados sob controle dos órgãos e entidades do Poder Executivo do Estado do Rio de Janeiro.

Art. 2º - Esta Resolução aplica-se:
aos órgãos e entidades submetidos ao Decreto Estadual 48.891/2024; e
aos operadores, prestadores de serviço e demais terceiros que realizem tratamento de dados pessoais em nome do Estado, quando houver vínculo contratual ou instrumentos congêneres.

Definições

Art. 3º - Para fins desta Resolução, aplicam-se as definições da Lei Federal 13.709/2018, e do Decreto Estadual 48.891/2024, especialmente as de dado pessoal, dado pessoal sensível, anonimização e pseudonimização.
Dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
Dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
Anonimização: processo por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, por meios técnicos razoáveis e disponíveis no momento do tratamento, de modo irreversível;
Pseudonimização: processo por meio do qual um dado perde a possibilidade de associação direta a um indivíduo sem o uso de informação adicional, mantida separadamente e sob controles, permitindo reversibilidade sob condições e finalidades legítimas;
Cópia de divulgação: versão derivada do documento ou informação, preparada para circulação ampliada ou disponibilização externa, contendo ocultação adequada de dados pessoais;
Documento original: documento arquivístico, registro primário, base primária ou informação de referência mantida sob custódia do órgão ou entidade, preservada para fins administrativos, legais, probatórios, de controle ou auditoria;
Validação: conjunto mínimo de verificações destinadas a confirmar que a técnica aplicada protege adequadamente os dados pessoais e que não há recuperação por meios usuais;
Anonimização para fins desta Resolução: aplicação de técnicas destinadas a tornar o dado pessoal indisponível para tratamento, acesso ou visualização, sem prejuízo da preservação da integridade, autenticidade e rastreabilidade do documento arquivístico original, o qual poderá ser mantido sob custódia segura para fins administrativos, legais, probatórios, de controle ou auditoria;
Criptografia pós-quântica: conjunto de técnicas e algoritmos criptográficos desenvolvidos para resistir a ataques executados por computadores quânticos, com vistas à proteção da confidencialidade, integridade, autenticidade e segurança das informações;
Algoritmos criptográficos pós-quânticos: algoritmos projetados para assegurar proteção criptográfica mesmo diante da capacidade computacional esperada de sistemas quânticos, podendo ser empregados para cifração, assinatura digital, estabelecimento de chaves e outras finalidades de segurança da informação; e
Plano de saída: instrumento que contemple a transferência de conhecimento, a entrega de documentação técnica, a entrega de evidências e a garantia de continuidade operacional e auditabilidade após o término contratual.

Princípios e Diretrizes

Art. 4º - A aplicação de anonimização e pseudonimização observará, no mínimo:
finalidade, necessidade e minimização de dados;
proporcionalidade entre risco e medidas adotadas;
segurança da informação, rastreabilidade e responsabilização;
preservação da integridade e autenticidade documental, quando aplicável; e
rastreabilidade, com registro das decisões e das evidências do procedimento.

Art. 5º - Quando houver necessidade de preservação do documento original para fins administrativos, legais, probatórios, de controle ou auditoria, a anonimização deverá ser aplicada preferencialmente sobre cópia de divulgação ou por mecanismo de ocultação em camada de visualização, sem alteração destrutiva do original.

§1º - O acesso ao documento original deverá ser restrito a perfis autorizados, com controle de acesso e trilha de auditoria, quando aplicável.

§2º - É vedada a adoção de procedimento que resulte na perda de integridade, autenticidade ou rastreabilidade do documento original.

§3º - A anonimização não implicará, em nenhuma hipótese, alteração, sobrescrita ou descaracterização do documento arquivístico original, incidindo exclusivamente sobre a camada de acesso, visualização ou disponibilização da informação.

Art. 6º - Os órgãos e entidades deverão adotar técnicas de anonimização e pseudonimização sempre que possível, observadas as definições da legislação de proteção de dados pessoais, os princípios previstos no art. 6º da Lei Federal nº 13.709/2018, no Decreto Estadual 48.891/2024 e nas disposições desta Resolução.

Art. 7º - Após o decurso do prazo de armazenamento, os dados pessoais somente poderão permanecer disponíveis para tratamento ou visualização quando submetidos ao processo de anonimização, observado o Decreto Estadual nº 48.891/2024.

§1º - A aplicação do disposto no caput não autoriza a alteração, sobrescrita ou descaracterização do documento original, o qual deverá ser mantido íntegro e preservado, nos termos do art. 5º desta Resolução.

§2º - A anonimização referida no caput deverá ser aplicada de forma a tornar o dado pessoal indisponível para qualquer perfil de usuário, inclusive aqueles anteriormente autorizados ao tratamento, observado o disposto no art. 3º desta Resolução.

Art. 8º - A pseudonimização não afasta a necessidade de eliminação dos dados pessoais após o decurso do prazo de armazenamento, quando aplicável.
Parágrafo Único. A pseudonimização com reversibilidade não poderá ser utilizada como mecanismo de prolongamento do prazo de retenção, nem como substituto da anonimização prevista no art. 7º desta Resolução.

Art. 9º - Na disponibilização externa de documentos e informações que contenham dados pessoais, deverá ser preparada cópia de divulgação com ocultação adequada, conforme Anexo Único, preservando-se o conteúdo necessário à finalidade pública.

Art. 10 - A implementação de anonimização e pseudonimização deverá assegurar, no mínimo:

I - segregação entre documento original e cópia de divulgação, quando aplicável;

II - controles de acesso por perfil e trilha de auditoria para acesso ao original, quando aplicável; e

III - validação mínima do resultado, conforme Anexo Único.

Art. 11 - Na contratação, adoção ou uso de métodos, ferramentas ou serviços de anonimização e pseudonimização, deverá ser assegurado que o Estado mantenha capacidade autônoma de:

I - acessar e preservar o documento original ou base primária, quando aplicável;
II - verificar e auditar o resultado produzido, inclusive após o término do contrato;
III - obter e manter evidências do procedimento adotado, incluindo registros, parâmetros e validações mínimas; e
IV - migrar ou substituir a solução sem perda de capacidade operacional, mediante plano de saída.

Art. 12 - Quando houver pseudonimização com reversibilidade, a informação adicional necessária à reversão, incluindo chaves, tabelas de correspondência, segredos, credenciais e artefatos equivalentes, deverá permanecer sob custódia do Estado, com controles compatíveis com o risco.

Parágrafo Único - É vedada a dependência de meios exclusivos do fornecedor para reversão, auditoria ou validação, salvo em situação devidamente justificada e com plano de transição formalizado.

REQUISITOS TÉCNICOS

Art. 13 - Sempre que houver tratamento de dados pessoais em trânsito ou em repouso, especialmente dados pessoais sensíveis, deverão ser adotadas medidas de proteção técnica compatíveis com o risco, incluindo criptografia e controles de acesso.
Parágrafo Único - A criptografia e os controles de acesso são medidas complementares de segurança e não substituem a anonimização quando esta for exigida pela finalidade ou pela norma aplicável.

Art. 14 - Quando forem utilizados mecanismos criptográficos ou qualquer forma de segredo técnico para proteção de dados pessoais, o órgão ou entidade deverá garantir gestão do ciclo de vida de chaves e segredos, contemplando geração segura, armazenamento protegido, controle de acesso, rotação periódica, revogação, cópia de segurança e trilhas de auditoria.
Parágrafo Único - A gestão de chaves e segredos deverão ser documentadas e auditáveis, com definição clara de responsáveis e segregação de funções, quando aplicável.

Art. 15 - Quando a pseudonimização for adotada com reversibilidade, a informação adicional necessária à reversão, incluindo tabelas de correspondência, chaves, segredos ou artefatos equivalentes, deverá permanecer sob custódia do Estado, segregada e protegida por controles proporcionais ao risco.
Parágrafo Único - É vedada a dependência de meios exclusivos de fornecedor para reversão, validação, auditoria ou continuidade operacional, salvo justificativa formal, com plano de transição e preservação de evidências.

Art. 16 - Em contratações que envolvam anonimização ou pseudonimização, deverá constar plano de saída, contemplando transferência de conhecimento, entrega de documentação técnica, entrega de evidências e garantia de continuidade operacional e auditabilidade após o término contratual.

Art. 17 - Deverá ser adotada criptografia pós-quântica, preferencialmente, quando aplicável.

Art. 18 - Considerando os avanços tecnológicos relacionados à computação quântica e a necessidade de longevidade criptográfica, recomenda-se, preferencialmente, que soluções novas, contratações novas e evoluções arquiteturais relevantes avaliem a adoção de algoritmos criptográficos pós-quânticos padronizados, quando houver viabilidade técnica e interoperabilidade.

Art. 19 - Poderão ser adotados, entre outros, os padrões:

I - para estabelecimento de chaves: preferencialmente a utilização do padrão FIPS 203 ou superior, que especifica o ML-KEM, mecanismo de encapsulamento de chaves para estabelecimento de segredo compartilhado; e
II - para assinaturas digitais: preferencialmente o padrão FIPS 204 ou superior, que especifica o ML-DSA, algoritmo de assinatura digital pós-quântica e do FIPS 205 ou superior, que especifica o SLH-DSA, algoritmo de assinatura digital pós-quântica baseado em hash.

Art. 20 - A adoção de criptografia pós-quântica não elimina a necessidade de criptografia simétrica para proteção de dados, sendo comum o uso de um KEM para derivar chaves simétricas utilizadas em modos autenticados como AES-GCM.

Art. 21 - Devem ser utilizados modos autenticados de cifração e mecanismos que assegurem confidencialidade e integridade, compatíveis com boas práticas e com o risco do tratamento.

Art. 22 - As chaves e segredos utilizados em mecanismos criptográficos e na pseudonimização reversível devem possuir gestão de ciclo de vida auditável, incluindo geração segura, armazenamento protegido, controle de acesso, rotação, revogação, cópia de segurança e trilha de auditoria.

Art. 23 - A custódia de chaves e segredos essenciais deve evitar dependência de meios exclusivos de fornecedor, preservando autonomia do Estado.

Art. 24 - A adoção de algoritmos pós-quânticos deverá observar, conforme o caso, disponibilidade em bibliotecas criptográficas amplamente utilizadas. Registra-se que a biblioteca OpenSSL possui documentação oficial de suporte a ML-KEM e SLH-DSA e, em versões mais recentes, a ML-DSA.

Art. 25 - A adoção de criptografia pós-quântica não substitui os requisitos mínimos de proteção em trânsito e em repouso definidos nesta Resolução e deve preservar auditabilidade, portabilidade e continuidade operacional, inclusive para encerramento contratual.

Procedimentos Mínimos

Art. 26 - Todo procedimento de anonimização ou pseudonimização deverá conter, no mínimo, as seguintes etapas:

I - triagem e identificação de dados pessoais e, quando aplicável, de dados pessoais sensíveis;
II - definição da finalidade e do contexto do uso, compartilhamento ou divulgação;
III - seleção da técnica adequada;
IV - execução da técnica em cópia de divulgação ou mecanismo equivalente;
V - validação mínima do resultado; e
VI - registro das evidências e guarda do registro.

Art. 27 - Os registros e evidências do procedimento deverão ser mantidos conforme prazos legais e regras aplicáveis de gestão documental e segurança da informação.

Art. 28 - Esta Resolução entrará em vigor na data de sua publicação.

Rio de Janeiro, 24 de março de 2026

FEU BRAGA
Secretário de Estado

ANEXO ÚNICO

objetivo
Estabelecer técnicas mínimas, validações mínimas e regras de evidência para anonimização e pseudonimização no âmbito estadual.
Regras operacionais
A anonimização para disponibilização externa deve ser aplicada em cópia de divulgação ou em camada de visualização, quando aplicável.
A pseudonimização deve ser utilizada quando houver necessidade legítima de reversibilidade, com custódia estatal da informação adicional.
técnicas mínimas
Redação de conteúdo textual: substituição do dado pessoal por máscara padronizada, preservando coerência do texto quando necessário.
Tarjamento em documentos digitalizados e imagens: ocultação visual permanente na cópia de divulgação, assegurando inexistência de camadas recuperáveis.
Generalização e agregação: redução de granularidade e agrupamento de valores, quando aplicável, evitando singularização.
Pseudonimização por tokenização: substituição de identificadores por token, com tabela de correspondência segregada e sob custódia estatal.
Validações mínimas obrigatórias
Verificar a possibilidade de copiar e colar, busca de texto, exportação e conversão de formato.
Verificar metadados do arquivo e existência de camadas ocultas.
Verificar risco de identificação indireta por combinação de atributos, quando aplicável.
Para dados pessoais sensíveis, realizar validação ampliada e revisão por amostragem documentada.
evidências mínimas
Registrar finalidade e contexto.
Registrar técnica aplicada e responsável.
Registrar validações executadas e resultado.
Guardar cópia de divulgação e registros de auditoria, quando aplicável.
GLOSSÁRIO
Para fins de compreensão desta Resolução, adotam-se, no presente Anexo, as seguintes siglas, padrões e expressões técnicas:
- FIPS: padrão ou publicação aplicável à segurança da informação, conforme referência adotada nesta Resolução;
- ML-KEM: sigla técnica utilizada nesta Resolução, conforme padrão de criptografia pós-quântica aplicável;
- ML-DSA: sigla técnica utilizada nesta Resolução, conforme padrão de assinatura digital pós-quântica aplicável;
- SLH-DSA: sigla técnica utilizada nesta Resolução, conforme padrão de assinatura digital pós-quântica aplicável;
- AES-GCM: modo de operação criptográfica referido nesta Resolução para proteção de dados e informações; e
- OpenSSL: biblioteca de referência utilizada no contexto dos mecanismos criptográficos mencionados nesta Resolução.

Id: 2725721

SECRETARIA DE ESTADO DE TRANSFORMAÇÃO DIGITAL
SUBSECRETARIA EXECUTIVA

ATO DO SUBSECRETÁRIO EXECUTIVO

PORTARIA SETD/SUBEXE Nº 33 DE 26 DE MARÇO DE 2026

ALTERA E CONSOLIDA A COMPOSIÇÃO DA COMISSÃO DE FISCALIZAÇÃO E ACOMPANHAMENTO DO CONTRATO Nº 004/2024 INSTITUÍDA PELA PORTARIA SETD/SUBEXE Nº 27, DE 02 DE SETEMBRO DE 2025.

O SUBSECRETÁRIO EXECUTIVO DA SECRETARIA DE ESTADO DE TRANSFORMAÇÃO DIGITAL, no uso de suas atribuições legais e com base na Resolução SETD n.º 101, de 08 de Setembro de 2025, bem como no inciso V do Art. 42, em consonância com o que delega o inciso III do Art. 43, ambos da Resolução SETD n.º 98 de 28 de agosto de 2025, e