

	Política de Retenção e Descarte		
Classificação: INTERNA			
Responsável(eis):			
Versão	Aprovado em:	Revisado em:	Publicado em:

1. Introdução

Esta Política estabelece diretrizes para o armazenamento, retenção e descarte de documentos físicos e digitais sob responsabilidade do Instituto de Gestão Previdenciária do Estado do Pará - IGEPPS. Ela se aplica a registros que contenham ou não dados pessoais, abrangendo informações administrativas, previdenciárias, fiscais, jurídicas, contábeis e operacionais.

Seu objetivo é garantir que os documentos do IGEPPS sejam mantidos apenas pelo tempo necessário, em conformidade com as exigências legais e regulatórias aplicáveis, bem como com as boas práticas de governança da informação e gestão de riscos do setor público.

Embora a Lei Geral de Proteção de Dados Pessoais (LGPD) imponha cuidados especiais ao tratamento de dados pessoais, esta Política também atende a outras normas legais, como a legislação previdenciária, contábil, trabalhista, fiscal e administrativa, bem como aos requisitos contratuais com terceiros (fornecedores).

2. Objetivo

Esta Política tem como objetivo estabelecer diretrizes claras, seguras e alinhadas à Lei Geral de Proteção de Dados Pessoais (LGPD), à legislação previdenciária, contábil, trabalhista, fiscal e administrativa, bem como as demais normas internas do IGEPPS, sobre os critérios e procedimentos para retenção, armazenamento e descarte seguro de documentos físicos e digitais.

3. Abrangência

Esta Política se aplica a todos os departamentos, unidades, colaboradores, terceiros e prestadores de serviço que, no exercício de suas funções, produzam, utilizem, arquivem ou tenham acesso a documentos físicos e/ou digitais sob a guarda do IGEPPS.

Aplica-se tanto a documentos que contenham dados pessoais quanto a documentos de natureza administrativa, previdenciária, contratual, contábil, trabalhista, jurídica e técnica.

	Política de Retenção e Descarte		
Classificação: INTERNA			
Responsável(eis):			
Versão	Aprovado em:	Revisado em:	Publicado em:

4. Definições Importantes

Para a compreensão desta Política adotam-se os seguintes termos e definições:

- **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;
- **Dado anonimizado:** dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;
- **Banco de dados:** conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;
- **Titular dos dados:** pessoa natural a quem se referem os dados pessoais que são objeto de tratamento. Somos nós;
- **Controlador:** pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
- **Encarregado de dados (DPO):** pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);
- **Autoridade Nacional de Proteção de Dados (ANPD):** órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional;
- **Tratamento dos dados pessoais:** toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

	Política de Retenção e Descarte		
Classificação: INTERNA			
Responsável(eis):			
Versão	Aprovado em:	Revisado em:	Publicado em:

- **Anonimização:** utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;
- **Consentimento:** manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;
- **Bloqueio:** suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;
- **Eliminação:** exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;
- **Transferência internacional de dados:** transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;
- **Uso compartilhado de dados:** comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;
- **Incidente de segurança:** qualquer evento adverso confirmado, relacionado à violação das propriedades de confidencialidade, integridade, disponibilidade e autenticidade da segurança de dados pessoais;
- **Medidas de segurança:** medidas técnicas e/ou administrativas adotadas para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

5. Princípios a serem observados

O IGEPPS adota os seguintes princípios para a gestão de documentos:

- **Finalidade:** manter documentos apenas pelo tempo necessário para atender a finalidade informada ou obrigações legais;
- **Minimização de dados:** armazenar apenas os dados estritamente necessários;

	Política de Retenção e Descarte			
Classificação: INTERNA				
Responsável(eis):				
Versão	Aprovado em:	Revisado em:	Publicado em:	

- **Segurança:** garantir a integridade, confidencialidade e disponibilidade das informações durante o período de guarda;
- **Responsabilidade e transparência:** registrar todas as fases do ciclo de vida do documento;
- **Descarte seguro:** eliminar documentos por métodos que impeçam a recuperação ou acesso indevido aos dados.

6. Classificação dos dados pessoais para fins de retenção e descarte

O IGEPPS classifica os dados pessoais de acordo com a finalidade de uso, o que permite aplicar regras adequadas de retenção e descarte. Os dados são armazenados apenas pelo tempo necessário para cumprir a finalidade informada no momento da coleta, conforme a legislação aplicável e os princípios da LGPD.

A seguir estão listadas as principais categorias de dados pessoais tratados pelo IGEPPS e seus respectivos contextos:

a) Dados Administrativos e Fiscais

Dados relacionados ao servidores do IGEPPS, incluindo contracheques, fichas funcionais, exames médicos, processos administrativos, bem como, contratos com terceiros ou fornecedores, e registros de transações orçamentárias e financeiras.

b) Dados de Comunicação e Marketing

Informações utilizadas para ações de comunicação e relacionamento com o titular.

Exemplos: nome, e-mail, telefone, preferências de conteúdo, registros de campanhas e consentimentos.

c) Dados Previdenciários

Dados pessoais usados em processos e requerimentos de aposentadorias, concessão de benefícios, pensões e etc.

Exemplos: dados cadastrais, contratuais, currículos,, fichas de registro, holerites.

	Política de Retenção e Descarte		
Classificação: INTERNA			
Responsável(eis):			
Versão	Aprovado em:	Revisado em:	Publicado em:

d) Dados de segurança e acesso

Informações coletadas para controle de acesso físico e lógico, gestão de identidade e segurança da informação.

Exemplos: login e senha, logs de acesso, imagens de câmeras de segurança, crachás de identificação.

7. Classificação de Armazenamento/Retenção/Registros

Com base na classificação trazida no item anterior, o IGEPPS mantém um conjunto de dados pessoais armazenados/retidos/registrados (aqui chamados de “Registros”) em conformidade com requisitos contratuais, regulatórios e demais bases legais aplicáveis às modalidades de tratamentos de dados pessoais.

É importante que esses Registros sejam protegidos contra perda, destruição, falsificação, acesso não-autorizado e liberação não-autorizada.

Durante o período de retenção:

- Documentos digitais devem ser armazenados em ambientes com proteção contra perda, acesso não autorizado e integridade comprometida;
- Documentos físicos devem ser armazenados em arquivos organizados, com controle de acesso, inventário e rastreabilidade.

Esse controle se aplica a todas as operações, pessoas e processos que constituem o sistema de informações da organização, incluindo colaboradores, diretores, fornecedores, clientes e terceiros que têm acesso aos dados e informações tratadas pelo IGEPPS, razão pela qual classifica os Registros em categorias que estabelecem os requisitos de retenção e de descarte para cada categoria.

Assim sendo, todos os dados pessoais serão retidos pelo tempo necessário ao cumprimento do objetivo para que foram coletados, com finalidades lícitas, específicas e informadas.

	Política de Retenção e Descarte			
Classificação: INTERNA				
Responsável(eis):				
Versão	Aprovado em:	Revisado em:	Publicado em:	

Vale lembrar que há uma diversidade de tratamentos às informações pessoais e sensíveis cujo prazo de arquivamento não é determinado por lei, como, por exemplo, o tempo de guarda dos registros por câmeras de segurança, de acesso às dependências físicas de um lugar, para guarda de cadastros de acessos.

Em tais casos, o IGEPPS estipulará um prazo de guarda coerente com as boas práticas e rotinas do órgão, de acordo com a natureza do tratamento, enquanto não houver determinação específica pela autoridade reguladora.

Para os demais Registros, incluindo aqueles de ordem previdenciária, o IGEPPS se reserva o direito de mantê-los armazenados até o fim do prazo prescricional estipulado em lei, conforme disposto na Tabela de Temporalidade do INSS e o Cronograma, que integra de forma anexa a presente Política de Retenção e Descarte.

8. Procedimento de descarte

Encerrado o prazo de retenção, os documentos deverão ser eliminados com segurança:

- **Documentos físicos:** devem ser triturados ou incinerados, com emissão de certificado de destruição e acompanhamento do setor responsável;
- **Documentos digitais:** devem ser excluídos com uso de ferramentas seguras de apagamento lógico (wipe) e, quando aplicável, com registros de logs de exclusão e auditoria.

O descarte deve seguir procedimento formalizado, com registro da data, responsável e tipo de documento eliminado. Devem ser realizadas auditorias periódicas para verificação da conformidade.

9. Exceções e guarda estendida

	Política de Retenção e Descarte		
Classificação: INTERNA			
Responsável(eis):			
Versão	Aprovado em:	Revisado em:	Publicado em:

Caso existam documentos que estejam sob investigação, auditoria, ordem judicial ou qualquer outra situação que exija a suspensão do descarte, sua retenção deverá ser prorrogada até que haja autorização expressa para sua eliminação.

O mesmo raciocínio se aplica a documentos cujo prazo de guarda possa ser estendido para defesa de direitos em processos administrativos ou judiciais.

10. Responsabilidades

- **Servidores e Comissionados:** seguir as diretrizes desta Política e os prazos estipulados na Tabela de Temporalidade, armazenar e sinalizar documentos conforme os prazos definidos;
- **Coordenadores:** assegurar que o setor siga os procedimentos de guarda e descarte, além de comunicar a TI e o Encarregado de Dados sobre documentos sensíveis ou críticos;
- **TI:** manter infraestrutura adequada para o arquivamento e exclusão segura de documentos digitais;
- **Encarregado de Dados:** supervisionar a execução desta Política, promover treinamentos e revisar os processos periodicamente;
- **Jurídico e Compliance:** orientar sobre prazos legais e situações que exijam retenção adicional de documentos.

11. Solicitação de Exclusão por Titular de Dados

As solicitações de exclusão de dados enviadas por um titular deverão ser analisadas pelo Encarregado de Dados e respondidas conforme os prazos e critérios estabelecidos na LGPD e em outras normas aplicáveis.

	Política de Retenção e Descarte		
Classificação: INTERNA			
Responsável(eis):			
Versão	Aprovado em:	Revisado em:	Publicado em:

Antes de atender à solicitação, será feita uma avaliação para verificar:

- Se os dados ainda são necessários para cumprimento de obrigação legal ou regulatória;
- Se há base legal que justifique sua manutenção (ex: execução de contrato, defesa de direitos em processo judicial);
- Se o prazo de retenção previsto na Tabela de Temporalidade já foi alcançado.

Caso a exclusão seja possível, ela será realizada de forma segura e definitiva, com registro do procedimento em sistema próprio. Caso não seja possível excluir os dados imediatamente, o titular será informado com a devida justificativa e, se for o caso, com a estimativa de prazo para atendimento.

Todas as solicitações e respectivas análises ficarão documentadas para fins de auditoria e prestação de contas.

12. Monitoramento e auditoria

A aplicação desta Política será monitorada por meio de controles internos, registros de descarte e auditorias periódicas conduzidas pela área de T.I em conjunto com o Comitê de Privacidade, o Encarregado de Dados e as áreas envolvidas.

Eventuais não conformidades serão tratadas conforme os procedimentos disciplinares e de segurança da informação.

13. Revisão da Política

Esta Política será revisada a cada dois anos ou sempre que houver alterações relevantes na legislação aplicável, nos processos internos, ou nas tecnologias utilizadas para armazenamento e descarte

A tabela de temporalidade deverá ser atualizada sempre que houver mudanças regulatórias ou operacionais e revisada também no mesmo prazo desta Política.

14. Histórico de versões:

		Política de Retenção e Descarte		
Classificação: INTERNA				
Responsável(eis):				
Versão	Aprovado em:	Revisado em:	Publicado em:	

Versão	Data de publicação	Alterações realizadas	Responsável
1.0			
1.1			
2.0			



ASSINATURAS

Número do Protocolo: 2026/2174887

Anexo/Sequencial: 7

Este documento foi assinado eletronicamente na forma do Art. 6º do Decreto Estadual Nº 2.176, de 12/09/2018.

Assinatura(s) do Documento:

Assinado eletronicamente por: CESAR AUGUSTO CAVALCANTE VALENTE, **CPF:** ***.488.702-**

Em: 04/02/2026 15:01:41

Aut. Assinatura: 83a41e75693a1d4eb3d1dc9ff7399b12b061b14cf5ce7f2f0750855a50d0488a



Identificador de autenticação: faa6e877-75d5-4ed0-8fe9-cd2521d86cc1

Confira a autenticidade deste documento em
<https://www.sistemas.pa.gov.br/validacao-protocolo>