INORPEL CYBERSECURITY	CÓDIGO POL-SI-017	**Data de Criação:** 27/03/2025
	Número: POL-SI-017 **Localizador:** POL-SI-017 v1.0* | 10/06/2025	**Revisão:** 1.0* **Status:** Vigente **Data para Revisão:** 09/06/2027
Título:	**POLÍTICA DE RETENÇÃO E DESCARTE DE DADOS**	**Área Emitente:** SI
Elaborador:	Carmem Santos — Analista de Processo	**Aprovador:** Rodrigo Agra de Brito — CEO
Data da Publicação:	06/05/2025	**Classificação:** Interno
Normas/Requisitos:	LGPD (Lei 13.709/2018) | ISO/IEC 27701:2019 | ISO/IEC 27001:2022 (A.8.10)	

SUMÁRIO

1. INTRODUÇÃO

A Política de Retenção e Descarte de Dados é o documento que norteia e determina todas as diretrizes relacionadas ao assunto, garantindo que todos os dados que tramitam dentro da INORPEL CYBERSECURITY — pessoais ou não — tenham seus procedimentos realizados em conformidade com a legislação e regulamentação vigente.

2. OBJETIVO E ABRANGÊNCIA

Esta política tem como objetivo formalizar o compromisso da INORPEL com todo o processo de retenção e descarte de dados, sem que haja violação das prerrogativas elencadas. Além disso, estabelece regras claras para todas as etapas desse processo, garantindo que sejam seguidos os seguintes princípios:

1. Assegurar que os Dados Pessoais sejam armazenados pelo período adequado, respeitando o tempo necessário para o cumprimento de sua finalidade e os requisitos legais e regulatórios aplicáveis.
2. Minimizar a retenção desnecessária de Dados Pessoais, garantindo que não sejam mantidos além do necessário.
3. Garantir que os registros relacionados à retenção e ao descarte de Dados Pessoais sejam eficientes, apropriados e devidamente documentados, assegurando transparência e conformidade.

Para a correta retenção e descarte de documentos, devem ser observados os seguintes princípios:

- Legalidade e Regulamentação — os documentos devem ser armazenados conforme exigências legais e regulatórias aplicáveis.
- Necessidade — os documentos não devem ser mantidos além do período necessário para sua finalidade.
- Segurança da Informação — o impacto à segurança deve ser avaliado, considerando a confidencialidade e a presença de Dados Pessoais.
- Acessibilidade — os dados devem permanecer disponíveis enquanto houver necessidade justificada para seu uso.
- Anonimização — sempre que necessário e permitido, devem ser adotadas medidas para anonimizar os Dados Pessoais, reforçando a privacidade e minimizando riscos.

A implementação dessas diretrizes garante que a retenção e o descarte de Dados Pessoais sejam conduzidos de maneira ética, segura e em conformidade com a legislação vigente.

A presente Política se aplica a todos os colaboradores que, em algum momento, tenham contato com dados tratados pela INORPEL ou em seu nome. Políticas adicionais poderão ser elaboradas para situações específicas, especialmente quando exigido por lei ou regulamento.

3. DEFINIÇÕES

Para a correta aplicação das diretrizes desta política, os dados devem ser classificados conforme sua criticidade e sensibilidade:

- Dados Pessoais: qualquer informação relativa a uma pessoa singular, que possa ser identificada, direta ou indiretamente.
- Dados Pessoais Sensíveis: dados ligados às especificidades do titular, como origem racial ou étnica, convicção religiosa, qualquer dado referente à saúde do titular, informações econômicas e sociais, entre outros.
- Dados Públicos: informações acessíveis a qualquer pessoa sem restrição de uso.
- Dados Internos: informações utilizadas internamente pela organização, com acesso restrito a determinados grupos.
- Dados Confidenciais: informações sensíveis que exigem proteção, como dados financeiros e estratégicos.

4. DIRETRIZES GERAIS

4.1 Do Monitoramento e Conformidade

Para assegurar a efetividade das práticas adotadas e um monitoramento eficiente, a área de GRC/DPO é responsável por verificar o cumprimento das diretrizes de proteção de dados em todas as áreas da organização. Quando necessário, poderá contar com o suporte da equipe técnica, que auxiliará na implementação de ajustes e melhorias para reforçar a segurança e reduzir vulnerabilidades.

Os setores responsáveis devem garantir que a eliminação de dados seja definitiva e irreversível, utilizando métodos adequados conforme o meio de armazenamento. Além disso, devem manter registros detalhados das operações de descarte, assegurando rastreabilidade e conformidade com as normas aplicáveis.

4.2 Retenção dos Dados

A retenção de Dados Pessoais é permitida sempre que houver uma base legal válida e apropriada que justifique seu tratamento para uma finalidade legítima, conforme os prazos estabelecidos na tabela do Anexo I.

Caso seja identificada a necessidade de manter os dados por um período superior ao previsto, o responsável pelo tratamento deverá preencher o formulário disponível no Anexo II, detalhando o motivo da retenção adicional e informando

o novo prazo. Após o preenchimento, o formulário será encaminhado à área de GRC/DPO, que analisará a solicitação e decidirá pela aprovação ou rejeição da extensão do prazo de retenção.

4.3 Descarte dos Dados

O descarte de dados deve ser realizado de forma que garanta a impossibilidade de recuperação de qualquer informação ligada a ele. Partindo dessa premissa, todo dado pessoal deverá ser descartado nas seguintes hipóteses:

a) Quando encerrado o prazo estabelecido na tabela do Anexo I e não houver nenhuma outra finalidade ou justificativa legítima para retenção do dado. Nos casos em que os dados sejam mantidos além do período estabelecido, após processo aprovado pela área de GRC/DPO e encerrado o novo prazo, o dado será descartado.

b) Quando a finalidade do tratamento dos Dados Pessoais for alcançada ou quando eles deixarem de ser necessários ou pertinentes para os objetivos específicos estabelecidos pela INORPEL.

c) Quando o Titular solicitar a interrupção do tratamento de seus Dados Pessoais, como nos casos em que um Cliente revoga seu consentimento, e não houver fundamento legal para a continuidade da retenção conforme as hipóteses previstas no Anexo I.

d) Quando houver determinação expressa da área Jurídica ou de GRC/DPO em cumprimento a uma ordem judicial ou administrativa.

e) Quando a área de GRC/DPO determinar a exclusão dos dados com base nas diretrizes de segurança, privacidade e conformidade da organização.

Nas hipóteses previstas nos itens c e d, o agente responsável deverá comunicar de forma IMEDIATA o DPO, por meio do e-mail: dpo@inorpelcybersecurity.com.br.

Por fim, para cada tipo de armazenamento, devem ser seguidas as seguintes regras:

- Documentos físicos: são todos os papéis ou documentos que contenham dados. Sua forma de descarte deverá ser por meio de fragmentador.
- Mídias digitais removíveis: arquivos armazenados em mídias digitais flexíveis devem ser destruídos por meio de um fragmentador apropriado. As mídias digitais rígidas, como HDs e pen drives, devem ser encaminhadas ao Centro de Serviços Compartilhados (CSC), acompanhadas de um termo contendo informações detalhadas sobre a mídia, incluindo tipo, tamanho, marca e número de série.
- Arquivos digitais: arquivos digitais que contenham dados devem ser permanentemente excluídos da rede e de todos os dispositivos que armazenem cópias, incluindo computadores, celulares e tablets, garantindo que não possam ser recuperados. O time de suporte será responsável por aplicar métodos adequados de exclusão segura, como o de Criptografia, inviabilizando a recuperação do documento por terceiros.

Nos casos de descarte de Mídia e Arquivos Digitais, a solicitação deve ocorrer por meio do Service Desk, onde o solicitante deverá indicar: os dados que devem ser deletados, as razões, o meio de armazenamento e a justificativa. Após o envio da solicitação, o pedido passará por aprovação do DPO, que verificará a conformidade do descarte antes de sua execução.

5. CONTROLES E AUDITORIA

Para evitar a retenção indevida ou descarte inadequado, a presente política será monitorada por meio de auditorias periódicas para garantir a eficácia dos processos de retenção e descarte. O descumprimento poderá resultar em medidas disciplinares.

6. DISPOSIÇÕES FINAIS

As previsões dispostas na presente Política poderão ser alteradas a qualquer momento, devendo haver revisões anuais de tais disposições.

Caberá à INORPEL CYBERSECURITY assegurar o conhecimento e divulgação do presente documento, suas alterações, processos e procedimentos, por meio de treinamento e confirmação por escrito da ciência dos envolvidos das normas previstas.

7. HISTÓRICO DE VERSÕES

Versão	Data	Responsável	Descrição
v0.1	27/03/2025	Carmem Santos	Criação do documento
v1.0	06/05/2025	CGSPC (via D4Sign)	Aprovação do documento
v1.0*	10/06/2025	Rodrigo Agra de Brito — CEO	Migração taxonômica SGI. Prorrogação de prazo. Atualização de cabeçalho. Instrumento: MEM-GRC-0004.