

# Retenção, direitos e incidentes

VERSÃO 1.3 | MINUTA PARA REVISÃO

Documento temporário para leitura e validação interna. Não está vigente e não representa oferta ou contrato definitivo.

PROGRAMA INTERNO DE RETENÇÃO, DIREITOS E INCIDENTES - LGPD

DOCUMENTO INTERNO - NÃO PUBLICAR

Versão: 1.3 - 4 de outubro de 2026

## 1. TABELA DE RETENÇÃO A APROVAR

**Categoria:** cadastro e conta ativa.

**Prazo durante a relação:** enquanto necessário à prestação.

**Prazo após encerramento:** [DEFINIR].

**Evento inicial:** exclusão/encerramento da conta.

**Fundamento de conservação:** obrigações, fraude e exercício de direitos.

**Destino:** eliminar, anonimizar ou arquivar com acesso restrito.

**Categoria:** pedidos e agendamentos.

**Prazo:** [DEFINIR COM JURÍDICO, FISCAL E CONSUMIDOR].

**Evento inicial:** conclusão ou cancelamento.

**Destino:** eliminação ou anonimização após encerradas obrigações e prazos de defesa.

**Categoria:** pagamentos, conciliação e comprovantes.

**Prazo:** [DEFINIR COM FINANCEIRO E PRESTADOR].

**Evento inicial:** liquidação ou encerramento da disputa.

**Destino:** arquivo restrito e posterior eliminação.

**Categoria:** KYC/KYB e representação.

**Prazo:** [DEFINIR CONFORME PAPEL DA PINHO E EXIGÊNCIA DO PRESTADOR].

**Evento inicial:** rejeição ou fim da parceria.

**Destino:** eliminar ou conservar somente o necessário.

**Categoria:** logs de autenticação e segurança.

**Prazo:** [DEFINIR POR RISCO E CAPACIDADE DE INVESTIGAÇÃO].

**Destino:** rotação automática, agregação ou eliminação.

**Categoria:** suporte e gravações.

**Prazo:** [DEFINIR]; gravações somente se realmente realizadas e informadas.

**Destino:** eliminar anexos e dados excessivos antes do restante do protocolo, quando possível.

**Categoria:** Google Analytics e Meta Pixel.

**Prazo:** configurar o menor período compatível com a finalidade aprovada.

**Destino:** expiração de cookies, exclusão de propriedades/audiências e bloqueio após retirada.

**Categoria:** provas de aceite.

**Prazo:** [DEFINIR CONFORME RELAÇÃO E EXERCÍCIO DE DIREITOS].

**Destino:** preservação íntegra, acesso restrito e posterior eliminação.

## 2. FLUXO DE DIREITOS DOS TITULARES

**Entrada:** suporte@pinho.app e WhatsApp (16) 99294-4224.

### 2.1. Responsável pelo recebimento

### 2.2. Responsável pela decisão

### 2.3. Substituto

### 2.4. Etapas

- registrar data, identidade alegada, pedido e canal;
- confirmar recebimento;
- autenticar de forma proporcional sem coletar documento excessivo;
- localizar dados em autenticação, banco, arquivos, backups acessíveis e fornecedores;
- verificar direitos de terceiros, segredo comercial e hipóteses de conservação;
- responder de forma clara e dentro do prazo aplicável;
- executar correção, exportação, oposição, retirada, anonimização ou eliminação cabível;
- propagar instruções aos operadores;
- registrar decisão e evidências.

### 2.5. Pedidos previstos

- confirmação e acesso;
- correção;
- informação sobre compartilhamentos;
- portabilidade, quando regulamentada e aplicável;
- anonimização, bloqueio ou eliminação de dados excessivos ou irregulares;

- eliminação baseada em consentimento, ressalvadas conservações legais;
- informação e retirada do consentimento;
- oposição;
- revisão de decisão automatizada, quando aplicável;
- exclusão de conta.

## 3. EXCLUSÃO DE CONTA

### 3.1. Separar

- desativação de acesso;
- revogação de sessões;
- retirada da publicação de conteúdo;
- eliminação de dados sem fundamento de conservação;
- bloqueio e arquivo restrito de registros necessários;
- anonimização de métricas;
- instrução aos fornecedores.

Não prometer eliminação imediata e absoluta quando houver pedido em andamento, obrigação legal, prevenção a fraude ou exercício de direitos. Informar o que foi eliminado, o que foi conservado e por quê.

## 4. INCIDENTES DE SEGURANÇA

### 4.1. Canal interno de urgência

### 4.2. Responsável técnico

### 4.3. Responsável jurídico/privacidade

### 4.4. Contato de cada fornecedor

### 4.5. Procedimento

- conter o evento e preservar evidências;
- registrar quando a Pinho tomou conhecimento;
- identificar sistemas, titulares, dados e volume afetados;
- avaliar confidencialidade, integridade, disponibilidade e autenticidade;
- avaliar risco ou dano relevante;
- acionar operadores e suboperadores;
- corrigir vulnerabilidade e impedir recorrência;
- preparar comunicação à ANPD e aos titulares quando exigida;
- manter registro mesmo quando não houver comunicação;

- produzir relatório pós-incidente.

**Prazo regulatório de referência:** incidentes que possam acarretar risco ou dano relevante devem ser comunicados pela controladora à ANPD e aos titulares em até três dias úteis, ressalvada regra específica. O cronômetro interno deve ser menor para permitir avaliação e aprovação.

## 5. RELATÓRIO DE IMPACTO E PRIVACY BY DESIGN

### 5.1. Avaliar RIPD antes de

- ampliar uso de CPF ou dados de identidade;
- iniciar perfilamento publicitário ou correspondência avançada;
- tratar dados em grande escala ou de menores;
- integrar nova biometria, localização precisa ou dado sensível;
- compartilhar dados para finalidade nova;
- implantar decisão automatizada com efeito relevante;
- alterar materialmente a arquitetura de pagamento ou autenticação.

### 5.2. Todo novo recurso deve responder

- quais dados são indispensáveis;
- qual é a finalidade específica;
- qual base legal é adequada;
- quem terá acesso;
- onde e por quanto tempo serão mantidos;
- quais fornecedores e países estão envolvidos;
- como o titular será informado e exercerá direitos;
- quais riscos existem e quais salvaguardas serão aplicadas.