Política e Procedimento de Expurgo e Eliminação de Dados (DATA PURGE POLICY)

Procedimento Operacional Padronizado de Offboarding de Tenants, Churn e Rescisão Contratual

Código do Documento: POL-DAT-001	**Versão:** 2.1
Data de Emissão: Setembro de 2026	**Classificação de Informação:** Uso Interno / Governança & LGPD
Área Responsável: Gestão Financeira, Engenharia de Software & DevOps	**Aplica-se a:** Todos os Tenants, Arquivos S3 e Bancos de Dados da Plataforma Sismetro

1. OBJETIVO

Esta política estabelece as diretrizes formais, os requisitos de segurança e os procedimentos operacionais para o encerramento de contas, cancelamento de serviços e o **expurgo definitivo e irreversível de dados operacionais e arquivos (Data Purge)** de *tenants* (unidades) na plataforma SISMETRO, garantindo a conformidade com a LGPD (Lei Geral de Proteção de Dados) e o Marco Civil da Internet.

2. CANAIS E GATILHOS DE ENCERRAMENTO

2.1. Modalidade 1: Cancelamento Voluntário (Churn)

1. **Solicitação Inicial:** Deve ser iniciada obrigatoriamente pela conta Administrativa do cliente no caminho: `Meu Perfil` → `Conta` → `Solicitar Cancelamento da Conta`.
2. **Tratativa Comercial e Contratual:** A ação dispara um alerta automático para `financeiro@sismetro.com`. A equipe de Gestão/Financeiro entra em contato com os representantes legais para análise contratual e tratativas operacionais.
3. **Validação por Código (1º Fator - Validade de 24 horas):** Na tela administrativa dedicada, a equipe informa o ID da Unidade (*Tenant ID*). O sistema gera o **1º Código de Confirmação de Cancelamento**, enviado ao e-mail do usuário administrativo solicitante. O código possui **validade de 24 horas** para inicialização do processo.

2.2. Modalidade 2: Rescisão por Inadimplência (Quebra Contratual)

1. **Critério Temporal:** O atraso de pagamento superior a **4 meses corridos (120 dias)** a contar do vencimento caracteriza descontinuidade e quebra de contrato.
2. **Inclusão na Fila de Expurgo:** A conta entra na fila de exclusão permanente.
3. **Validação da Gestão:** Na tela administrativa dedicada, a equipe de Gestão/Financeiro insere o Número do Contrato e o ID da Unidade (*Tenant ID*), gerando as mesmas etapas de validação por códigos de autorização.

3. FLUXO OPERACIONAL DE SINCRONIA E EXPURGO EM ETAPAS

```
[Solicitação / Inadimplência]
       |
       ▼
[Código 1: Confirmação de Cancelamento (Expira em 24h)]
       |
       ▼
[Validação de Sincronia / "data-sync"] ──(Obrigatório antes da pré-exclusão)
       |
       ▼
[Pausa de Planos às 00:00h e inativação de APIs]
       |
       ▼ (Janela obrigatória de segurança de 45 dias corridos)
       ▼
[Código 2: Autorização de Expurgo (Gestão/Financeiro)]
       |
       ▼
[Código 3: Confirmação Final de Expurgo (Gestão/Diretoria)]
       |
       ▼
[EXPURGO IRREVERSÍVEL: BANCO DE DADOS OPERACIONAL + ARQUIVOS S3]
       |
       ▼
[RETENÇÃO DO REGISTRO DE AUDITORIA NO TENANT E LOGS ISOLADOS]
```

Step 1: Sincronização Final de Dados (*Pre-exclusão*)

- Antes da destruição dos dados, é obrigatório executar a rotina de sincronização final para o banco dedicado de exportação (`data-sync`), mediante informação do **Código de**

Autorização para Sincronia Final.

Step 2: Pausa Operacional dos Serviços

- Com o código de pré-exclusão validado, a rotina automatizada pausa a abertura de novos planos operacionais e uso de APIs a partir das **00:00 horas do dia seguinte**.

Step 3: Janela de Carência e 2º Código de Expurgo

- O sistema aplica uma janela de segurança obrigatória de **45 dias corridos**.
- Transcorrido o prazo, o sistema libera o campo para digitação do **2º Código de Autorização de Expurgo**, fornecido pela equipe de Gestão/Financeiro.

Step 4: Confirmação Final, Destruição de Dados e Limpeza S3 (3º Código)

- A exclusão é autorizada na tela final mediante a inserção do **3º Código de Confirmação** (fornecido pela diretoria/gestão) e preenchimento das informações de encerramento.
- **Ação Técnica de Expurgo:**
  1. **Banco de Dados Operacional (Arquitetura Multi-Tenant):** Execução de instrução de exclusão lógica/física (*Delete Purge*) focada estritamente nas **linhas (registros) vinculadas ao** `Tenant ID` em todas as tabelas operacionais do banco de dados.
  2. **Arquivos em Storage (Amazon S3):** Execução da exclusão paralela e automática de todos os documentos, anexos e mídias vinculados à unidade no bucket do Amazon S3.

4. RASTREABILIDADE (AUDIT TRAIL) E RETENÇÃO LEGAL DE LOGS

4.1. Registro Permanente de Encerramento (Audit Trail)

O cadastro mestre do *Tenant ID* **não é destruído**. Ele permanece em estado inativo e retém o histórico de autorização de expurgo (identificação dos responsáveis, datas, horas e os 3 códigos de confirmação utilizados). Caso o cliente retorne no futuro, um **novo ID de Unidade** será gerado.

4.2. Retenção Isolada de Logs de Acesso

Em cumprimento ao **Marco Civil da Internet (Lei nº 12.965/2014, Art. 15)** e às boas práticas de governança:

- Os registros e logs de acesso dos usuários à unidade são mantidos em banco/repositório isolado de auditoria sob sigilo.
- Os logs passam por uma rotina automatizada de expurgo definitivo após **5 (cinco) anos** contados a partir da data de execução do expurgo operacional da unidade.

5. DECLARAÇÃO DE IRREVERSIBILIDADE

Uma vez concluído o Step 4 com a validação dos três códigos de segurança, **o processo de expurgo das tabelas operacionais e arquivos no S3 é definitivo e irreversível**, não sendo possível a restauração do ambiente por nenhuma das partes.

Revisão #3
Criado 2026-09-23 18:20:22 UTC por Marcio Klitzke
Atualizado: 2026-09-24 14:00:06 UTC por Marcio Klitzke