

Ciclo de Vida do Dado

Grupo 5: Gestão, Descarte e Conformidade

Elifas, Erick, Isabelly, Patrícia, Valdir

27 de Janeiro de 2026

Disciplina: Proteção de Dados — Prof. Dayler

Conceitos Fundamentais

O que é Data Lifecycle Management (DLM)?

Definição

É uma abordagem baseada em políticas para gerenciar o fluxo de informações de um sistema de dados, desde o momento em que é criado até o momento em que se torna obsoleto e é deletado.

As Fases Clássicas:

1. Criação/Coleta
2. Armazenamento
3. Uso/Compartilhamento
4. Arquivamento
5. Descarte Seguro

O Problema: “Data Hoarding”

Cultura Antiga: “Vamos guardar tudo, storage é barato. Um dia podemos precisar.”

Realidade Atual (LGPD):

- Dado sem governança é **Passivo Tóxico**.
- Aumenta a superfície de ataque.
- Dificulta a localização de dados (Direito do Titular).



Acumular dados desnecessários aumenta o impacto financeiro e reputacional de um vazamento.

Fundamentação Legal (LGPD)

Art. 6º - Princípio da Necessidade

A LGPD impõe um freio na coleta indiscriminada.

Minimização de Dados

O tratamento deve ser limitado ao **mínimo necessário** para a realização de suas finalidades.

→ **Na prática:** Se o marketing pede “Religião” do cliente para vender sapato, a TI deve barrar ou questionar a finalidade no sistema.

Art. 15 e 16 - Término do Tratamento

O dado não pode ser eterno.

Regra Geral (Art. 15)

Os dados devem ser eliminados após o término de seu tratamento ou quando a finalidade for alcançada.

Exceções de Retenção (Art. 16)

Pode-se manter o dado se:

- Cumprimento de obrigação legal (ex: Guarda de logs por 6 meses - Marco Civil).
- Uso exclusivo do controlador (desde que **anonimizados**).

O Papel da TI na Gestão

Confusão Comum: Backup ≠ Archive

A TI precisa separar as políticas de Disaster Recovery das políticas de Compliance.

Carac.	Backup	Retenção (Archive)
Objetivo	Recuperação rápida (Disaster Recovery)	Conformidade Legal e Histórica
Alteração	Cópias frequentes e sobreescritas	WORM (Write Once, Read Many)
Busca	Difícil (nível de arquivo/bloco)	Indexado para auditoria
Vida	Curta (ex: 30-90 dias)	Longa (ex: 5, 10, 20 anos)

Como descartar digitalmente?

Dar “Delete” não apaga o dado do disco físico. A TI deve aplicar técnicas forenses:

1. **Sobrescrita (Overwriting):** Escrever zeros ou dados aleatórios sobre o setor do disco (Padrão DoD 5220.22-M).
2. **Degaussing (Desmagnetização):** Destruição magnética (para HDs físicos descartados).
3. **Crypto-shredding (Para Nuvem):** Criptografar o dado e deletar a chave de criptografia. O dado permanece lá, mas é matematicamente ilegível para sempre.

Construindo o Fluxograma do Dado

Para atender à LGPD, mapeamos o ciclo em pontos de decisão crítica:

- **Entrada:** O dado entra validado?
- **Meio:** A finalidade ainda existe?
- **Saída:** Existe lei que obriga a guardar?
- **Fim:** O descarte foi certificado?

O Fluxograma do Dado (Visual)

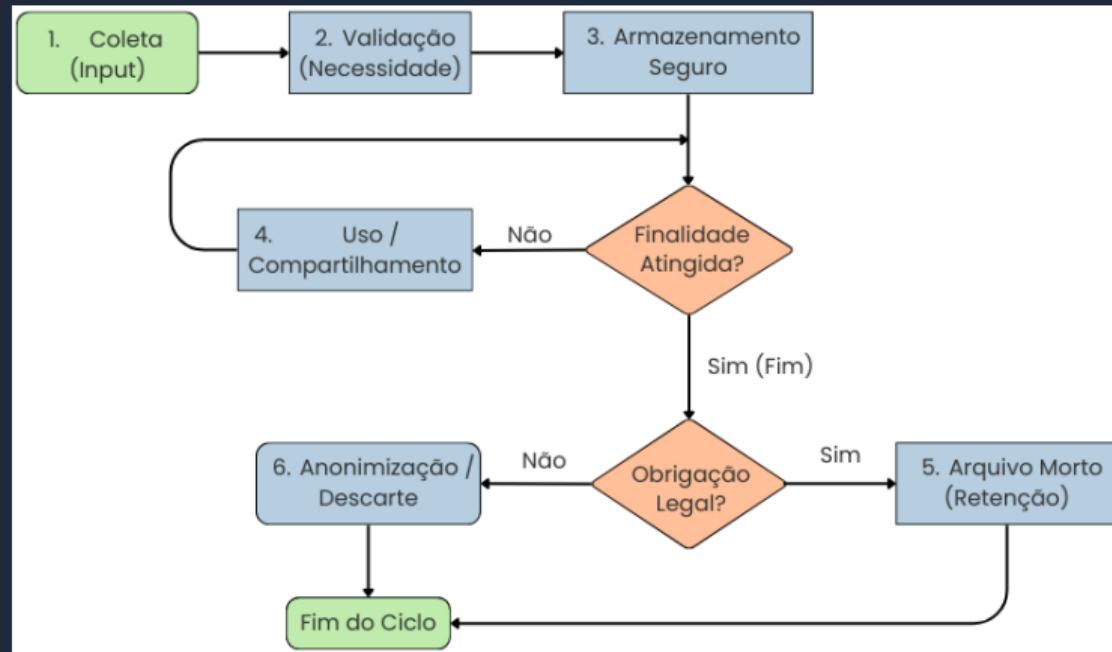


Figura 1: Fluxo de decisão para ciclo de vida e descarte.

Cenário Prático: Implementação

Cenário: “Quero excluir minha conta”

Contexto: Um usuário de e-commerce solicita a exclusão de sua conta via aplicativo, exercendo o Art. 18 da LGPD.

Desafio Técnico: O banco de dados possui integridade referencial (FK). Se apagarmos o usuário, quebramos os relatórios de vendas financeiras.

Como resolver esse conflito entre Direito do Titular vs. Consistência do Banco?

A Abordagem Errada: “Soft Delete”

O desenvolvedor apenas marca o registro como inativo.

Código Inseguro

```
UPDATE clientes SET ativo = FALSE WHERE id = 105;
```

Por que é errado?

- ✗ O dado pessoal (Nome, CPF, E-mail) continua legível no banco.
- ✗ Em caso de vazamento (dump de SQL), os dados dos “excluídos” são expostos.
- ✗ Não atende ao princípio da eliminação da LGPD.

A Abordagem Certa: Anonimização/Sanitização

Transformamos o dado pessoal em dado estatístico não-identificável.

Processo Correto

1. Verificar pendências (ex: pedidos em aberto).
2. **Hard Delete** nos campos diretos: CPF, E-mail, Telefone.
3. **Anonimização** nos campos de display: Nome → “Cliente_Excluido_ID105”.
4. Manter dados transacionais (Vendas) vinculados a esse ID anônimo para fins fiscais.

Perguntas

Questão 1 - Anonimização

Qual a principal distinção jurídica e técnica entre **Anonimização** e **Pseudonimização**?

- A Não há diferença técnica, apenas legal.
- B Pseudonimização é definitiva; anonimização é reversível.
- C Anonimização é irreversível e retira o dado do escopo da LGPD; pseudonimização permite reidentificação.
- D Anonimização só serve para dados bancários.
- E Pseudonimização é mais segura que criptografia.

Questão 1 - Anonimização

Qual a principal distinção jurídica e técnica entre **Anonimização** e **Pseudonimização**?

- A Não há diferença técnica, apenas legal.
- B Pseudonimização é definitiva; anonimização é reversível.
- C **Anonimização é irreversível e retira o dado do escopo da LGPD; pseudonimização permite reidentificação.**
- D Anonimização só serve para dados bancários.
- E Pseudonimização é mais segura que criptografia.

Resposta Correta: C

O dado anonimizado perde a possibilidade de associação ao indivíduo. O pseudonimizado mantém a chave em separado (Art. 13).

Questão 2 - Minimização

O Princípio da Necessidade impacta a coleta. Qual ação viola esse princípio?

- A Coletar e-mail para newsletter solicitada.
- B Solicitar “Religião” e “Time de Futebol” em um cadastro de Wi-Fi gratuito.
- C RH solicitar dados bancários para salário.
- D TI implementar logs de acesso.
- E Excluir dados antigos.

Questão 2 - Minimização

O Princípio da Necessidade impacta a coleta. Qual ação viola esse princípio?

- A Coletar e-mail para newsletter solicitada.
- B Solicitar “Religião” e “Time de Futebol” em um cadastro de Wi-Fi gratuito.**
- C RH solicitar dados bancários para salário.
- D TI implementar logs de acesso.
- E Excluir dados antigos.

Resposta Correta: B

Coletar dados sensíveis sem finalidade robusta e indispensável é violação direta da minimização (Art. 6º).

Questão 3 - Descarte

Segundo a LGPD, o que deve ocorrer, via de regra, após o término do tratamento?

- A Publicação em portal de transparência.
- B Guarda em backup acessível por 100 anos.
- C Eliminação dos dados.
- D Venda para parceiros comerciais.
- E Impressão física.

Questão 3 - Descarte

Segundo a LGPD, o que deve ocorrer, via de regra, após o término do tratamento?

- A Publicação em portal de transparência.
- B Guarda em backup acessível por 100 anos.
- C **Eliminação dos dados.**
- D Venda para parceiros comerciais.
- E Impressão física.

Resposta Correta: C

A regra é o descarte. A retenção é a exceção (apenas para cumprimento de lei ou uso exclusivo anonimizado).

Questão 4 - Segurança

Qual é o papel fundamental do **Backup** no ciclo de vida?

- A Servir como arquivo morto eterno.
- B Garantir confidencialidade.
- C Anonimizar dados.
- D Substituir o Firewall.
- E Garantir a disponibilidade e recuperação (Disaster Recovery).

Questão 4 - Segurança

Qual é o papel fundamental do **Backup** no ciclo de vida?

- A Servir como arquivo morto eterno.
- B Garantir confidencialidade.
- C Anonimizar dados.
- D Substituir o Firewall.
- E **Garantir a disponibilidade e recuperação (Disaster Recovery).**

Resposta Correta: E

Backup visa a continuidade do negócio (Disponibilidade da tríade CID). Não deve ser usado para retenção de longo prazo.

Questão 5 - Privacy by Design

Se um sistema vem configurado para NÃO compartilhar dados por padrão, isso é:

- A Privacy by Default.
- B Engenharia Social.
- C Phishing.
- D Dados Abertos.
- E Big Data.

Questão 5 - Privacy by Design

Se um sistema vem configurado para NÃO compartilhar dados por padrão, isso é:

- A Privacy by Default.
- B Engenharia Social.
- C Phishing.
- D Dados Abertos.
- E Big Data.

Resposta Correta: A

Privacy by Default exige que a configuração inicial seja a mais protetiva possível à privacidade do usuário.

Conclusão e Referências

Conclusão

Para uma gestão eficiente do Ciclo de Vida do Dado:

- **Governança:** Definir prazos de retenção (Tabela de Temporalidade).
- **Tecnologia:** Automatizar o descarte seguro e diferenciar Backup de Archive.
- **Cultura:** Treinar equipes para não praticarem “Data Hoarding”.
- **Conformidade:** O descarte não é opcional, é lei.

Referências Bibliográficas i

-  Brasil (2018).
Lei nº 13.709, de 14 de agosto de 2018.
Diário Oficial da União.
Lei Geral de Proteção de Dados Pessoais (LGPD).
-  DAMA International (2017).
DAMA-DMBOK: Data Management Body of Knowledge.
Technics Publications, Basking Ridge, NJ, 2 edition.
-  ISO/IEC (2019).
ISO/IEC 27701:2019: Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management.
International Organization for Standardization, Geneva, Switzerland.

Referências Bibliográficas ii

-  Kissel, R., Regenscheid, A., Scholl, M., and Stine, K. (2014).
Nist special publication 800-88 revision 1: Guidelines for media sanitization.
Technical report, National Institute of Standards and Technology (NIST), Gaithersburg, MD.
-  Pinheiro, P. P. (2020).
Proteção de Dados Pessoais: Comentários à Lei 13.709/2018.
Saraiva Educação, São Paulo, 2 edition.

Obrigado!

Dúvidas?

*“Privacidade não é sobre esconder algo,
é sobre ter controle sobre o que é seu.”*