ATIVIDADE — LGPD E PRIVACY BY DESIGN

1. Contexto

Esta atividade foca nos princípios da Necessidade e Finalidade (Art. 6º da LGPD) e na estruturação do banco de dados desde a concepção, aplicando o conceito de Privacy by Design.

2. Objetivo

O grupo deverá analisar um cenário de negócio, identificar os dados pessoais, mapear seu ciclo de vida (tratamento) e propor uma modelagem de banco de dados (Modelo Entidade-Relacionamento e Relacional) que minimize a coleta e garanta a proteção.

3. Cenário

Uma startup está desenvolvendo um novo Sistema de Gerenciamento de Reservas de uma Clínica de Fisioterapia. O sistema precisa registrar pacientes, agendamentos e histórico de sessões.

4. Identificação e Classificação de Dados

Dados coletados:

- Nome completo (Pessoal Comum) — Finalidade: identificação / Base Legal: Execução de Contrato
- CPF (Pessoal Comum) — Finalidade: identificação fiscal / Base Legal: Obrigação legal
- Telefone e Email (Pessoal Comum) — Finalidade: contato e confirmação de agendamento / Base Legal: Execução de Contrato
- Endereço (Pessoal Comum) — Finalidade: cadastro do paciente / Base Legal: Execução de Contrato
- Histórico Clínico (Pessoal Sensível) — Finalidade: acompanhamento terapêutico / Base Legal: Tutela da Saúde
- Data da Sessão (Pessoal Comum) — Finalidade: registro operacional / Base Legal: Execução de Contrato

5. Princípio da Necessidade (Minimização)

Dados excessivos: data de nascimento, nome da mãe, profissão — não são necessários para o agendamento.

Minimização: coletar apenas os dados essenciais. CPF e contato devem ser anonimizados após 5 anos.

Técnica sugerida: anonimização e criptografia AES-256 para CPF, Hash SHA-256 para senha.

6. Modelagem LGPD-Friendly

Separação lógica de dados:

- Dados pessoais identificáveis em tabela `pacientes_identificacao`
- Dados clínicos em tabela `historico_clinico` com chave estrangeira referenciando o paciente.

Modelo Entidade-Relacionamento (MER)

[Paciente] 1---N [Agendamento]
[Paciente] 1---N [Historico_Clinico]
[Agendamento] 1---1 [Fisioterapeuta]

Esquema Relacional:

```
CREATE TABLE pacientes_identificacao (
id_paciente INT PRIMARY KEY AUTO_INCREMENT,
nome VARCHAR(100) NOT NULL,
cpf VARBINARY(256) NOT NULL, -- criptografado com AES-256
telefone VARCHAR(20),
email VARCHAR(100),
endereco VARCHAR(255)
);
CREATE TABLE agendamentos (
id_agendamento INT PRIMARY KEY AUTO_INCREMENT,
id_paciente INT NOT NULL,
data_agendamento DATE NOT NULL,
horario TIME NOT NULL,
id_fisioterapeuta INT,
FOREIGN KEY (id_paciente) REFERENCES pacientes_identificacao(id_paciente)
);
CREATE TABLE historico_clinico (
id_historico INT PRIMARY KEY AUTO_INCREMENT,
```

id_paciente INT NOT NULL,
descricao TEXT NOT NULL, -- dado sensível
data_sessao DATE,
FOREIGN KEY (id_paciente) REFERENCES pacientes_identificacao(id_paciente)
);
CREATE TABLE fisioterapeutas (
id_fisioterapeuta INT PRIMARY KEY AUTO_INCREMENT,
nome VARCHAR(100),
registro_profissional VARCHAR(50)
);
Campos sensíveis: descricao (histórico clínico).
Campos criptografados: cpf (AES-256).
7. Proteção e Conformidade
- Acesso restrito aos dados sensíveis.
- Logs de auditoria para acesso e alteração.
- Políticas de retenção: exclusão após 5 anos de inatividade.