

Inventário técnico de dados e permissões

VERSÃO 1.3 | MINUTA PARA REVISÃO

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

INVENTÁRIO TÉCNICO PRELIMINAR DE DADOS E PERMISSÕES

DOCUMENTO INTERNO - NÃO PUBLICAR

Fonte: código do painel Pinho e dump mais recente localizado

Versão: 1.3 - 4 de outubro de 2026

1. ESCOPO ANALISADO

- painel web do estabelecimento, conforme inventário técnico interno;
- rotas e funções do backend;
- esquema e funções do banco de dados no dump inventário técnico interno do banco de dados;
- autenticação e armazenamento no navegador;
- integração de pagamento encontrada no código.

Este inventário é técnico e preliminar. Deve ser validado contra o ambiente de produção e os contratos de fornecedores.

2. DADOS DE CONSUMIDORES

- e-mail;
- telefone;
- nome completo;
- CPF;
- data de nascimento;
- fotografia de perfil;
- identificador da conta;
- endereço de faturamento, solicitado em compras com cartão de crédito e salvo para compras futuras somente mediante escolha do Usuário;
- login externo, quando escolhido;
- sinais técnicos do dispositivo e fingerprint para prevenção a fraude;
- resultado de autenticação 3DS, quando aplicável;
- histórico de pedidos e agendamentos;

- serviços, variações, preços e imagens registrados no pedido;
- cancelamentos, estados e horários;
- avaliações, texto, nota, opção de ocultar perfil e fotografias;
- identificadores e contadores operacionais.

3. DADOS DE ESTABELECIMENTOS

- nome fantasia e imagens de perfil, capa e galeria;
- CNPJ, razão social, inscrições estadual e municipal;
- data de fundação;
- endereço;
- situação ativa e métricas de avaliação;
- descritor de cobrança;
- identificador de recebedor ou seller no prestador histórico;
- serviços, itens, categorias, variações, preços e promoções;
- agenda, horários, profissionais, reservas e disponibilidade;
- configurações, parcelamento, comissão e métodos de pagamento.

4. REPRESENTANTES E COLABORADORES

- nome, descrição e fotografia;
- conta, e-mail e vínculo com estabelecimento;
- cargo e situação ativa;
- indicação de responsável legal;
- permissões de acesso e alteração;
- registros técnicos necessários à administração.

5. DADOS DE PAGAMENTOS ENCONTRADOS NO BANCO

- método, valor, parcelas e status;
- identificadores internos e do processador;
- código e estado de Pix;
- informações de divisão de valores;
- IP associado à transação;
- aprovação, negativa, captura e tempos do fluxo;
- código de autorização e comprovante de venda;
- bandeira e últimos dígitos, quando disponíveis;
- indicação de desafio de autenticação;

- juros, valor capturado, estorno e conciliação.

Não foram encontrados campos destinados a persistir número completo do cartão ou CVV no dump analisado.

Segundo a arquitetura de produção informada pelo responsável do produto, a coleta será feita por integração segura de pagamento: o navegador enviará os dados completos diretamente ao fornecedor especializado, que devolverá à Pinho um token de pagamento transitório. O backend usará esse token para realizar a transação, sem receber o número completo ou o CVV.

Essa arquitetura ainda deve ser confrontada com a implementação final antes do lançamento.

6. PERMISSÕES DO PAINEL

- visualizar agendamentos;
- criar agendamento manual;
- editar agendamentos;
- acessar contato de clientes;
- visualizar horários;
- editar horários;
- visualizar serviços;
- editar serviços;
- visualizar itens;
- editar itens;
- visualizar usuários;
- convidar usuários;
- editar usuários;
- visualizar cargos;
- editar cargos;
- visualizar configurações;
- editar configurações;
- estornar pagamentos;
- alterar credencial ou API key.

7. CONTROLES OBSERVADOS

- Row Level Security ativado nas tabelas públicas analisadas;
- acesso administrativo concentrado em funções RPC;
- validação de autenticação, vínculo com estabelecimento e permissões em funções analisadas;
- separação entre projeto de autenticação e projeto de dados;
- sessão de autenticação persistida no navegador;

- JWT e contexto do estabelecimento mantidos em armazenamento de sessão;
- proteção especial do cargo de proprietário em partes do código.

8. PONTOS DE ATENÇÃO

Funções SECURITY DEFINER podem contornar a proteção normal de linha. Por isso, toda função mutável exposta deve validar autenticação, estabelecimento, cargo e permissão exata, limitar campos e produzir auditoria.

O acesso a contato de clientes deve ser restrito a quem realmente atende pedidos. Estorno, alteração de credencial e gestão de usuários são permissões de alto risco.

Credenciais no navegador aumentam o impacto potencial de vulnerabilidades de script. Aplicar política de segurança de conteúdo, prevenção de XSS, rotação, expiração e revogação de sessão.

9. FONTES A VALIDAR

- ambiente de produção e migrações mais recentes;
- serviço de autenticação e configuração do login externo;
- logs e ferramentas de observabilidade;
- armazenamento de arquivos e política de acesso;
- fornecedor de e-mail, notificações e atendimento;
- serviço de processamento financeiro utilizado;
- analytics, pixels, cookies e SDKs;
- backups, replicações e prazos de retenção.