

Divergências e pendências

VERSÃO 1.3 | MINUTA PARA REVISÃO

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

DIVERGÊNCIAS E PENDÊNCIAS TÉCNICAS, JURÍDICAS E OPERACIONAIS

DOCUMENTO INTERNO - NÃO PUBLICAR

Versão: 1.3 - 4 de outubro de 2026

PRIORIDADE CRÍTICA

1. Implementar e validar a arquitetura de pagamento de produção.

O banco contém referências históricas a Braspag/Cielo e o responsável do produto confirmou que o checkout planejado utilizará integração segura de pagamento com token transitório. O backend atual também contém rota experimental para PagBank em sandbox, mas ela não representa o checkout definitivo. Essa rota não deve ser exposta em produção nem usada como fundamento dos documentos.

2. Confirmar o fluxo integração segura de pagamento ponta a ponta.

Na arquitetura informada, o navegador envia número, validade e CVV diretamente ao fornecedor especializado. A Pinho recebe um token de pagamento transitório e o utiliza na transação. Antes do lançamento, testar em produção controlada e confirmar por inspeção de rede, logs e código que PAN e CVV não chegam ao backend, observabilidade, analytics, logs de erro ou banco.

3. Determinar e validar o escopo residual de segurança do setor de pagamentos residual.

A integração segura de pagamento reduz a exposição da Pinho aos dados completos do cartão, mas não elimina as obrigações de segurança aplicáveis. As exigências dependem da arquitetura efetivamente utilizada. Obter confirmação formal, preencher a validação aplicável, monitorar anualmente os fornecedores e manter responsabilidades contratuais documentadas.

4. Distinguir token transitório de cartão cadastrado.

Nos documentos e na interface, usar "token transitório de pagamento" ou "token de pagamento". Não prometer cartão salvo. Confirmar validade, uso único ou limitações reais na documentação e configuração do Prestador.

5. Não chamar retenção técnica temporária de estrutura financeira específica.

O sandbox indica uma função de retenção e liberação futura. Isso não basta para caracterizar conta estrutura financeira específica, segregação fiduciária ou conta de pagamento. Exigir contrato do fornecedor e parecer jurídico antes de usar esses termos.

6. Definir responsabilidade regulatória pelo onboarding financeiro.

Identificar quem realiza KYC/KYB, quem aprova recebedores, quem é controlador dos dados, quais documentos são exigidos, qual o canal de recurso e quais registros retornam à Pinho.

PRIORIDADE ALTA

7. Fechar regras de cancelamento e não comparecimento.

Definir prazo, percentual de retenção, exceções, regras por estabelecimento e tratamento do direito de arrependimento. A regra deve aparecer antes da compra e ficar vinculada ao pedido.

8. Fechar fluxos de reembolso e chargeback.

Definir quem inicia, prazos internos, responsável por custos, evidências, comunicação, compensação de saldo negativo e tratamento quando o estabelecimento encerra atividades.

9. Definir comissão e taxas.

O percentual deve vir de fonte controlada e ficar visível no painel. Não transformar valores de sandbox, como divisão 10/90, em cláusula contratual sem aprovação comercial.

10. Auditar todas as funções RPC expostas.

Verificar especialmente funções SECURITY DEFINER acessíveis ao papel anônimo. Confirmar validação de cabeçalho de autenticação, vínculo, isolamento por estabelecimento, permissão, campos editáveis, limites e logs.

11. Implementar trilha de auditoria.

Registrar alteração de permissões, estornos, credenciais, dados bancários, condições comerciais, cancelamentos, reembolsos e aceites.

PRIORIDADE MÉDIA

12. Criar tabela de retenção e descarte.

Definir prazos por cadastro, pedido, pagamento, nota fiscal, logs, suporte, avaliações, arquivos, KYC/KYB e aceite.

13. Completar inventário de fornecedores e transferências internacionais.

Incluir autenticação, banco de dados, hospedagem, arquivos, pagamentos, e-mail, analytics, suporte, assinatura e antifraude.

14. Criar plano de incidentes e canal de privacidade.

Definir responsáveis, classificação, preservação de evidências, avaliação de risco, comunicação à ANPD e titulares quando aplicável.

15. Revisar armazenamento de sessão no navegador.

Validar expiração, rotação, logout, revogação, proteção contra XSS e conteúdo de localStorage/sessionStorage.

16. Definir identidade societária e canais.

Preencher razão social, CNPJ, sede, contato, canal de privacidade e responsável pelo programa de agentes.

CONDIÇÃO PARA PUBLICAÇÃO

Nenhum documento deve ser publicado como versão final enquanto os itens críticos que alteram afirmações públicas não forem resolvidos e aprovados por jurídico, produto e engenharia.