01 / CONDIÇÃO COMERCIAL

# Pentest White Box Cashfast e Zaztech

Duas avaliações independentes de segurança de aplicações, com uma condição comercial especial para a contratação conjunta.

| Item | Tabela | Condição conjunta | Economia |
|---|---|---|---|
| **White Box Cashfast** | R$ 50.000 | R$ 40.000 | R$ 10.000 |
| **White Box Zaztech** | R$ 50.000 | R$ 40.000 | R$ 10.000 |
| **3 treinamentos × R$ 10.000** | R$ 30.000 | R$ 0 | R$ 30.000 |
| **TOTAL** | R$ 130.000 | R$ 80.000 | R$ 50.000 |

## R$ 50.000 de desconto total

R$ 20.000 de desconto nos dois pentests + R$ 30.000 em treinamentos oferecidos como cortesia. Economia de 38,46% sobre o valor de tabela do pacote de R$ 130.000.

Pagamento em até quatro parcelas. Na contratação conjunta: 4 × R$ 20.000, vinculadas ao kickoff do primeiro projeto, à entrega do primeiro relatório executivo, à entrega do segundo relatório executivo e à conclusão do terceiro treinamento. Na contratação individual: R$ 50.000, em até 4 × R$ 12.500; vencimentos e faturamento a formalizar.

Três sessões gratuitas no total, de 60 min cada (3 h), compartilhadas entre as equipes. Início possível após o primeiro relatório e última sessão após o segundo, em janela de até 30 dias a combinar. Cada pentest tem escopo, relatório e aceite independentes.

## Prazo e condições de início

Os pentests serão executados sequencialmente, um após o outro. A ordem proposta é Cashfast → Zaztech, a confirmar na mobilização. Até 30 dias úteis por frente, incluindo relatório e apresentação, a partir do início formal de cada frente com pré-requisitos atendidos; até 60 dias úteis de execução dos pentests, excluindo impedimentos formalmente acordados.

02 / OBJETIVO E ESCOPO

# Avaliação de segurança das aplicações

A proposta protege a base da operação e ajuda a priorizar melhorias antes da expansão dos produtos financeiros.

## Cashfast

Avaliar o código e os fluxos sob responsabilidade da Cashfast: portal, pagadoria, APIs, identidade, integrações internas e, conforme disponibilidade, módulos de crédito e recebíveis. Verificar controles ligados a operações financeiras, permissões, estados e dados.

## Zaztech

Avaliar as aplicações próprias da Zaztech, com foco na plataforma nova, serviços multiempresa/white label, integrações, módulos cashless, PDV e aplicações móveis próprias quando incluídos no inventário. O legado em migração não integra automaticamente o escopo; delimitação no kickoff.

## O que será feito

- Mapeamento da arquitetura, inventário, interfaces e regras de negócio, seguido da preparação e verificação do ambiente isolado.
- Revisão manual do código, análise pontual de dependências e segredos, verificações de configuração e testes autenticados em sandbox.
- Simulações com dados sintéticos e mocks de parceiros; validação de controles e impactos sem movimentação real de recursos.
- Relatórios independentes, matrizes de cobertura e vulnerabilidades, recomendações priorizadas, apresentação e orientação técnica.

## O que não está incluído

Testes em produção ou em sistemas de terceiros, hardware e firmware de POS, SDKs de parceiros, ações sobre saldo ou repasse real, implementação de correções, retestes formais, Black Box, Purple Team, CI/CD, scanning recorrente, perfilamento de atacantes e certificação regulatória. A proposta técnica detalha as fronteiras.

03 / EXECUÇÃO E ENTREGAS

# Cronograma por frente e entregas

| Fase | Dias úteis | Marco |
|---|---|---|
| **1. Mapeamento e sandbox** | D1–D5 | Inventário, baseline e autorização do sandbox |
| **2. Revisão de código** | D6–D13 | Cobertura técnica e hipóteses priorizadas |
| **3. Testes controlados** | D14–D24 | Resultados e evidências validadas |
| **4. Consolidação** | D25–D30 | Relatórios, roadmap, apresentação e fechamento |

## Entregáveis por projeto

Relatório técnico de pentest; sumário executivo; matriz de vulnerabilidades e cobertura; recomendações e roadmap priorizado; apresentação de resultados; registro de encerramento do ambiente e evidências de descarte conforme controles acordados.

## Treinamento e suporte

Três sessões gratuitas no total, de 60 minutos cada (3 horas), avaliadas em R$ 10.000 por sessão. Online e ao vivo, para as equipes de desenvolvimento; preparação pela Ionix com base nos achados e apresentação de apoio. Podem começar após o primeiro relatório, durante a segunda frente; a última ocorre após o segundo relatório. Janela de até 30 dias a combinar. Sessões adicionais, laboratórios personalizados, certificação e acompanhamento prático prolongado não incluídos. Esclarecimentos sobre achados em janela e canais a formalizar; sem execução de correções.

## Formalização

1. Aceite comercial e faturamento por marcos. 2. NDA, LoA e inventários independentes. 3. Pré-requisitos e janela de testes. 4. Kickoff do primeiro projeto. 5. Entrega do primeiro relatório e início da segunda frente, após pré-requisitos. 6. Entrega do segundo relatório e conclusão das três sessões.

## Condição conjunta: R$ 80.000

Valor de tabela R$ 130.000. Desconto de R$ 50.000. Pagamento em até quatro parcelas.