01 / VISÃO EXECUTIVA

Proposta técnica Pentest White Box

Cashfast e Zaztech | Avaliação independente da segurança de aplicações e fluxos financeiros.

Dois projetos. Uma metodologia.

O código e os ambientes de cada empresa são avaliados independentemente, com inventário, cobertura, achados, relatório e encerramento próprios. A condição comercial conjunta não mistura dados nem responsabilidades.

Contexto e objetivo

A Cashfast está expandindo sua operação de pagamentos e banking para crédito e recebíveis. A Zaztech tem contextos próprios de plataforma, integrações e produtos white label, inclusive modernização de sistemas. O objetivo da Ionix é verificar controles internos de aplicações que sustentam essas operações, demonstrar riscos com evidência reproduzível e indicar uma sequência de correções compatível com o plano de negócio.

Resultado esperado

Uma visão tecnicamente fundamentada dos riscos nos ativos disponibilizados, com distinção entre vulnerabilidades confirmadas, indícios, controles verificados, limitações e funcionalidades ainda não implementadas. O serviço não promete ausência de vulnerabilidades ou certificação de prontidão regulatória.

Princípios de execução

- Somente código, serviços e ambientes expressamente autorizados.
- Testes dinâmicos exclusivamente em sandbox clonado e isolado; sem dados, credenciais, valores ou transações reais.
- Integrações críticas de parceiros representadas por simuladores; sem chamadas ou tentativas contra terceiros.
- Até 30 dias úteis por projeto, incluindo relatório e apresentação; execução sequencial na contratação conjunta, até 60 dias úteis de pentests.

Organização do documento

Escopo e fronteiras (02–04); ambiente e proteção (05–06); metodologia e catálogo de testes (07–13); execução, entregas e governança (14–19); condições comerciais (20); cronograma consolidado (Anexo A).

02 / DELIMITAÇÃO

Escopo Cashfast

O inventário final identifica todas as aplicações próprias incluídas, seus componentes e interfaces relevantes. Não há cobrança individual por aplicação dentro do inventário aprovado.

Frente	Cobertura pretendida	Limite
Portal e gestão	Login, recuperação, perfis de estabelecimentos, administração e dados por cliente.	Somente módulos próprios e versão acordada.
Pagadoria	Autorização, regras de pagamento, estado, repetição, webhooks, trilha de auditoria.	Saldo, repasse e execução de pagamento de parceiros são simulados.
Banking / crédito	Fluxos disponíveis de acesso, elegibilidade, limites, antecipação e recebíveis.	Produtos não implementados: apenas dependências/requisitos, sem conclusão de segurança.
APIs e serviços	Endpoints, conectores, jobs e componentes próprios que suportam os fluxos.	Sem teste direto sobre API externa ou rede de parceiros.
Configuração	Controles AWS/Cloudflare associados à aplicação; comparação com clone.	Sem teste invasivo em conta ou serviço de produção.
POS e SDK	Pré-requisição, dados recebidos, retorno e estado na aplicação própria.	Hardware, firmware e SDK de terceiros excluídos.

Dependências entre plataformas

Se a Cashfast consome serviço da Zaztech, o lado consumidor é avaliado com mock do contrato. A implementação do fornecedor só poderá ser examinada dentro do escopo próprio da Zaztech, sem conexão a ambientes reais. A análise conjunta poderá referenciar a dependência, mas não compartilhar evidências sensíveis entre entidades sem autorização expressa.

Critério de conclusão

Inventário versionado, fluxos prioritários confirmados pelo ponto focal, permissões esperadas registradas e cobertura rastreável por componente. Itens indisponíveis terão motivo, impacto e recomendação de próxima avaliação.

03 / DELIMITAÇÃO

Escopo Zaztech

O trabalho é orientado à plataforma própria e ao contexto de serviços compartilhados/white label. A plataforma em modernização tem prioridade, conforme discussão técnica inicial.

Frente	Cobertura pretendida	Limite
Plataforma nova	Serviços próprios, APIs e regras de autorização em módulos disponibilizados.	Inventário e commits aprovados antes da execução.
Multiempresa	Segregação de tenants/white labels, administradores, recursos e permissões.	Somente dados fictícios e tenants de teste.
Cashless / PDV	Regras próprias de saldo, estados, consumo e integrações internas, quando aplicáveis.	Nenhuma carga ou consumo real, terminal ou firmware de terceiros.
Mobile	APIs e código próprio dos apps incluídos, armazenamento e sessões conforme acesso.	Não inclui laboratórios de hardware, análise de apps externos ou lojas.
Conectores e jobs	Mensagens, webhooks, filas e tarefas de conciliação/sincronização próprias.	Contratos de terceiros em mocks; sem conexão real.
Legado e migração	Mapear dependências do legado e riscos de transição relevantes ao escopo.	Pentest integral do legado PHP somente se expressamente incluído e dimensionado.

Stack informada e validação

O cenário relatado inclui TypeScript/Node.js, frameworks web e APIs, infraestrutura AWS e Cloudflare, além de legado em PHP em migração. O inventário confirmará linguagens, versões, frameworks, serviços, dependências e criticidade. A metodologia será ajustada às tecnologias de fato disponibilizadas, não a uma lista presumida.

Cobertura em contratação individual

O projeto Zaztech não depende da contratação da Cashfast. Interfaces entre empresas são avaliadas pelo lado autorizado; a ausência da outra contratação não autoriza acesso adicional.

04 / FRONTEIRAS

O que este trabalho não cobre

As exclusões integram a proposta técnica e comercial. Não podem ser inferidas a partir da expressão White Box.

Exclusão	Tratamento previsto
Produção e disponibilidade	Sem testes ativos, exploração, varreduras, stress, DoS, mudanças de configuração ou carga contra produção. Levantamento por artefatos/exportações autorizados. Preservar continuidade e evitar impactos reais.
Terceiros e dinheiro real	Sem acesso a bancos, adquirentes, SDKs, POS, firmware ou APIs externas; sem transferências, saldo, repasse ou liquidação reais. Mock no sandbox. Respeitar titularidade e impedir movimentação real.
Remediação e reteste	Não inclui alterações de código, infraestrutura, implantação de recomendações nem certificação da correção. Validação do achado durante a avaliação é incluída. Manter independência do diagnóstico e da validação.
Operação contínua	Sem SOC, monitoramento 24×7, atendimento a incidentes, forense, threat intelligence, hunting, perfilamento/atribuição de atacantes ou medidas legais. Não confundir avaliação pontual com operação contínua.
Outros testes	Sem Black Box independente, Red/Purple Team, engenharia social, phishing, segurança física, auditoria integral de redes/hosts ou benchmark de carga. Modalidades distintas exigem autorização e planejamento próprios.
DevSecOps e compliance	Sem implantação de CI/CD, scanners recorrentes, aquisição de ferramentas, PCI DSS/ISO/SOC 2, parecer jurídico ou certificação de conformidade. Implantação e certificação exigem escopo próprio.
Escopo novo	Funcionalidades, versões, ativos e dependências novos após baseline precisam de avaliação de impacto e eventual aditivo. Evitar cobertura indefinida sobre versões não avaliadas.

Mudanças solicitadas durante o projeto

Qualquer ampliação será registrada com justificativa, ativos afetados, riscos, dependências, esforço e impacto no calendário. A execução fora do inventário original dependerá de autorização por escrito e, se necessário, proposta adicional. Nenhum trabalho fora do escopo será presumido ou cobrado sem acordo.

05 / AMBIENTE

Sandbox clonado e isolado

A fidelidade do ambiente permite avaliar as camadas de defesa sem expor a operação. A Ionix e o cliente definem se o sandbox fica em conta segregada da Ionix ou ambiente segregado do cliente.

Preparação do baseline

- Obter snapshots de código e configurações sanitizados, commits/tags, manifests, diagramas, schemas e documentação de APIs. Não copiar bases de produção.
- Replicar serviços, topologia, variáveis não sensíveis e controles relevantes (AWS, Cloudflare, redes e regras de acesso), por infraestrutura como código, como Terraform, ou exportação acordada. Não utilizar snapshots de disco ou imagem que contenham segredos/dados reais sem saneamento prévio.
- Criar identidades temporárias e segregadas, credenciais sintéticas, bancos de teste, tenants fictícios e simuladores de integrações externas.
- Reproduzir configuração efetiva na medida possível; registrar diferenças, versões, limitações de licença e recursos não replicáveis. Revisar com o cliente antes de iniciar testes dinâmicos.

Isolamento e bloqueio de saída

Separação lógica entre frentes; política de acesso restrita e expiração; saídas de rede negadas por padrão e liberadas apenas para dependências expressamente aprovadas e não produtivas. Validar DNS, endpoints, chaves e webhooks para garantir que os testes não alcancem parceiros ou produção. Não reaproveitar tokens, chaves ou certificados produtivos.

Critérios de liberação (gate)

Verificação	Evidência mínima
Fidelidade	Baseline, versão, mapa de diferenças e aprovação do responsável técnico.
Isolamento	Inventário de recursos, rotas, identidades e política de egress revisada.
Dados e mocks	Fixtures sintéticas, endpoints fictícios e validação da não comunicação real.
Autorização	LoA, janela e contatos de emergência confirmados.

06 / CONFIDENCIALIDADE

Proteção do código e das evidências

O modelo de tratamento de informações será formalizado no NDA e nas regras de engajamento, com rastreabilidade e descarte verificável.

Antes e durante o projeto

- Acesso nominal e menor privilégio; MFA quando disponível; repositórios e arquivos temporários restritos ao time autorizado; proibir compartilhamento fora dos canais definidos.
- Criptografia em trânsito e em repouso; trilha de acesso, alterações de permissões e operações de provisionamento/desprovisionamento conforme logs disponíveis.
- Não transmitir código ou evidências a serviços públicos de IA, repositórios externos ou ferramentas SaaS não autorizadas. Ferramentas locais/isoladas quando possível.
- Dados sintéticos por padrão; se material recebido contiver dado pessoal ou segredo real, interromper o tratamento desnecessário, comunicar o ponto focal e solicitar cópia saneada.
- Evidências mínimas necessárias, segredos mascarados, artefatos segregados por empresa e acesso apenas por pessoas autorizadas.

Encerramento e descarte

Após consolidação, revogar identidades temporárias, eliminar cópias de código, bases sintéticas, snapshots e recursos sob gestão da Ionix, conforme política e prazo acordados. Entregar registro do descarte com inventário, data, método, logs de exclusão disponíveis e itens eventualmente retidos por obrigação ou acordo. Não afirmar eliminação de backups fora de controle da Ionix; quando houver retenção técnica, documentar mecanismo, responsável e expiração.

Incidentes e comunicação

Qualquer suspeita de exposição ou comunicação com ambiente indevido gera interrupção da atividade, preservação mínima de evidências e notificação imediata ao ponto focal. Acionar os responsáveis do cliente e seguir o procedimento acordado; não extrapolar para resposta forense ou ações em produção.

07 / METODOLOGIA

Fase 1 — Mapeamento e mobilização

Dias úteis D1–D5. Transformar o contexto comercial e as dependências técnicas em um plano de cobertura verificável.

Atividade	Procedimento e resultado
A. Inventário	Identificar ativos, repositórios, responsáveis, ambiente, versionamento, componentes comuns, interfaces e dependências.
B. Arquitetura	Mapear fluxos de dados, pontos de entrada, fronteiras de confiança, armazenamento, processamento assíncrono e controles.
C. Regras de negócio	Entrevistar equipe e responsáveis pelos fluxos; confirmar atores, permissões, estados, limites e invariantes financeiras.
D. Modelagem de ameaças	Identificar cenários por ativo e fluxo: acesso indevido, alteração, duplicidade, inconsistência, exposição e perda de trilha.
E. Sandbox	Preparar ambiente e mocks; aplicar gate de isolamento, fidelidade, credenciais de teste e logs.
F. Plano de cobertura	Definir prioridades, classes de teste, perfis e conjuntos de dados fictícios, critérios de parada e canal de comunicação.

Entregáveis da fase

Inventário de escopo por empresa, diagrama lógico dos fluxos e fronteiras, matriz inicial de permissões e ameaças, registro do baseline e plano de cobertura. Gate D5: confirmação de prontidão do ambiente e dos limites técnicos.

Critério de aceite do marco

Ativos e versões definidos; autorizações vigentes; mocks e egress verificados; responsáveis e regras prioritárias confirmados. Dependências faltantes formalizadas. Nenhum teste ativo começa sem o gate.

08 / METODOLOGIA

Fase 2 — Revisão de código

Dias úteis D6–D13. Localizar controles e hipóteses relevantes para os fluxos incluídos e separar sinais automáticos de evidências contextualizadas.

Leitura manual orientada ao risco

- Percorrer roteamento, middleware, controladores, serviços, camadas de domínio, acesso a dados, jobs e adaptadores de integração. Identificar pontos de validação e decisões de autorização.
- Rastrear origem e destino de entradas externas; verificar processamento, persistência, serialização, tratamento de erros e exposição de dados.
- Rastrear decisões financeiras: cálculo, origem dos valores, verificação de limites, transição de estado, persistência, repetição e conciliação.
- Avaliar código de integrações próprias: validação de respostas, associação ao contexto, assinatura, tratamento de erros e repetição de eventos.

Verificações pontuais apoiadas por ferramentas

Técnica	Finalidade e tratamento
SAST	Identificar padrões de risco em código. Revisar contexto, caminhos alcançáveis e controles compensatórios.
SCA	Inventariar dependências diretas/transitivas disponíveis; correlacionar versões com vulnerabilidades conhecidas, configuração e exposição.
Secrets scanning	Identificar indícios de credenciais em artefatos autorizados; mascarar evidências; recomendar revogação/rotação sem testar credencial real.
Configuração	Avaliar manifests e configurações de aplicação/ambiente, permissões e regras de defesa replicadas.

Gate D13

Hipóteses classificadas, cobertura de leitura registrada, limitações e plano de testes atualizado. Alertas sem confirmação não são reportados como vulnerabilidade comprovada.

09 / METODOLOGIA

Fase 3 — Testes controlados

Dias úteis D14–D24. Verificar o comportamento real dos componentes próprios dentro do sandbox autorizado, com dados e identidades fictícias.

Sequência operacional

- Confirmar o cenário de referência e o comportamento esperado com o ponto focal; estabelecer estado inicial e registrar versão.
- Executar testes positivos e negativos por perfil, objeto, tenant e operação, respeitando os limites e janelas do sandbox.
- Correlacionar comportamento observado com o código e configuração; verificar o estado resultante, logs e chamadas ao simulador.
- Validar hipóteses com evidência mínima, reproduzível e não destrutiva; avaliar controles compensatórios e possíveis encadeamentos apenas quando seguros e necessários.
- Restaurar fixtures e estado de teste; anotar resultados, evidências mascaradas, bloqueios e justificativas para itens inconclusivos.

Instrumentação

Ferramentas de proxy de testes, como Burp Suite, clientes HTTP e testes unitários/integrados temporários quando adequados; logs e inspeção dos recursos autorizados. Não instalar agentes ou ferramentas em produção. Testes de taxa e concorrência são limitados ao sandbox e não são testes de carga.

Controle de execução

Condições de parada: egress inesperado, credencial real, alerta de ambiente, risco de impacto fora do sandbox ou falta de autorização. Suspender a atividade, comunicar ponto focal e só retomar com validação. Achados críticos com evidência suficiente serão comunicados durante a execução, não apenas no relatório final.

Marco D24

Matriz de cobertura atualizada com status por cenário, evidências, riscos e justificativas. O prazo não implica testar todas as combinações possíveis de entradas, perfis e estados.

10 / CATÁLOGO DE TESTES

Identidade, acesso e sessões

Exemplos de objetivos de teste; não constituem resultados encontrados. A matriz final será derivada dos ativos, perfis e tecnologias aprovados.

Domínio	Verificações planejadas	Evidência/critério
Autenticação	Login, recuperação, expiração de tokens, encerramento de sessão, MFA se existente e controles de tentativa.	Resultado autorizado/negado, estado da sessão e logs.
Autorização por objeto	Acesso a registros de outro cliente, estabelecimento, conta, tenant ou recurso por identidade de teste.	Regra no código, resposta e ausência/presença de exposição fictícia.
Autorização por função	Operações administrativas, alterações de privilégio, endpoints internos e rotas sensíveis.	Matriz de perfis × ações × resultado.
Separação de tenants	Contexto de white label, isolamento em consultas, caches, filas, arquivos e serviços compartilhados.	Comparação de dois tenants sintéticos e efeito observado.
Identidade de serviço	Credenciais e escopos entre serviços, validação de contexto e privilégios técnicos.	Configuração/classe de acesso, sem credencial real.
Sessões e tokens	Emissão, validação, renovação, revogação e comportamento após troca de perfil, quando aplicável.	Caminho relevante e comportamento controlado.

Referências de segurança

OWASP ASVS e OWASP Web/API Security Top 10 para requisitos e classes de risco; OWASP WSTG como referência de teste. A matriz não representa auditoria integral de todos os requisitos desses frameworks.

11 / CATÁLOGO DE TESTES

APIs, código e proteção de dados

Domínio	Verificações planejadas	Resultado esperado
Entradas e consultas	Validação de schema, tipos, limites, parâmetros, consultas e comandos; classes de injeção aplicáveis.	Entradas inválidas rejeitadas sem efeitos indevidos.
Saídas e front-end	Exposição excessiva de campos, tratamento de conteúdo, XSS, CORS e CSRF quando aplicável.	Respostas mínimas e controles coerentes.
Erros e exceções	Mensagens, falhas parciais, traces, fallback, timeout e tratamento de respostas inesperadas.	Sem exposição de dados/segredos ou decisão indevida.
Dados e segredos	Chaves e tokens em artefatos, logs, configurações e respostas; criptografia e armazenamento relevantes.	Achados mascarados; indicação de risco e correção.
Dependências	Versões vulneráveis, bibliotecas desnecessárias e dependência de componentes externos.	Versão, referência, alcance e recomendação.
Defesa em camadas	Regras WAF, limites de tentativa, headers, allowlists, configuração de segurança de serviços clonados.	Distinguir falha no código, exposição observada e controle compensatório.

Tratamento de falso positivo

O resultado automático deve ser correlacionado com a versão, o caminho alcançável, permissões, configuração e comportamento. Registrar controles que reduzam a explorabilidade sem eliminar a causa raiz. Uma camada de defesa não autoriza declarar que o código é seguro por si só.

12 / CATÁLOGO DE TESTES

Integridade financeira e regras de negócio

A análise concentra-se nos efeitos internos sobre dados, estados, registros e decisões financeiras, nunca em saldo ou movimentação real.

Cenário fictício	Verificação de controle	Evidência
Operação repetida	Idempotência, deduplicação e consistência quando uma solicitação/evento legítimo é repetido.	Estado inicial/final, registros e eventos de mock.
Valor ou contexto incorreto	Validação server-side de parâmetros, vínculo da operação ao titular e limites esperados.	Resultado, regra e ausência/presença de efeito indevido.
Estado incompatível	Transições válidas, cancelamento, reversão e tratamento de reprocessamento.	Histórico de estados e justificativa da decisão.
Concorrência	Invariantes financeiras em operações simultâneas controladas e falhas parciais.	Conciliação de registros sintéticos e logs.
Crédito e recebíveis	Elegibilidade, limites, antecipação, validação de identidade e associação de dados, se implementados.	Regra fornecida e versão examinada.
Auditoria e conciliação	Correlação de identificadores, origem de evento, trilha, reprocessamento e inconsistências.	Rastreabilidade do fluxo e registros de teste.

Limites de interpretação

Não constitui auditoria contábil, antifraude transacional em produção, validação de algoritmo de crédito ou verificação de liquidação de parceiros. Riscos são qualificados por plausibilidade e efeito técnico/financeiro potencial, sem estimar perdas monetárias sem dados validados.

13 / CATÁLOGO DE TESTES

Integrações e configurações de suporte

A fronteira de responsabilidade é central: analisar o antes e o depois de uma integração; não testar o sistema financeiro do parceiro.

Estratégia de mocks

Componente	Simulação
Contratos de API	Definir campos, estados, autenticação fictícia e respostas esperadas a partir de documentação disponibilizada.
Eventos e webhooks	Gerar eventos sintéticos válidos, inválidos, repetidos, fora de ordem ou com falha, verificando tratamento interno.
Falhas de dependência	Respostas de erro, timeout, indisponibilidade simulada e estados parciais; verificar tratamento, idempotência e rastreabilidade.
Serviços internos	Integrar clones próprios autorizados, com versionamento e dados sintéticos, sem tráfego para produção.
Controles de nuvem	Revisar exportações AWS/Cloudflare e testar somente configurações replicadas, com equivalência e desvios documentados.

Exclusões específicas

Não enviar requisições de teste a bancos, adquirentes, BaaS, SDKs de máquinas ou terceiros; não usar endpoints reais, credenciais produtivas nem dados de cartões reais. Hardware, firmware e componentes fechados são caixas externas. A conclusão não certifica o comportamento real do parceiro, apenas a aplicação própria perante os cenários mockados.

Rastreabilidade

Registrar contrato e versão do mock, campos simulados, entradas, resultados, eventos e divergências conhecidas. Limitações por falta de documentação serão indicadas na matriz de cobertura.

14 / METODOLOGIA

Fase 4 — Classificação e roadmap

Dias úteis D25–D30. Transformar evidências em decisões: o que precisa ser corrigido, em que ordem e com que dependências.

Classificação de achados

Classificar severidade técnica em crítica, alta, média, baixa ou informativa, com referência CVSS (versão registrada no relatório, preferencialmente v3.1 para comparabilidade com o modelo Ionix), complementada pela avaliação contextual de impacto, alcance e controles compensatórios. Prioridade de correção poderá divergir da severidade técnica com justificativa explícita.

Eixo	Pergunta de priorização
Impacto	Pode causar acesso a dados financeiros, alteração indevida de estados/saldos simulados, quebra de isolamento ou perda de rastreabilidade?
Exposição	Quais perfis, interfaces e pré-condições são necessários? Qual camada reduz ou amplia a exposição?
Negócio	O achado afeta produto atual, fluxo crítico, integração própria ou lançamento futuro planejado?
Remediação	Há correção localizada, mudança estrutural, dependência de parceiro ou ajuste de processo?
Evidência	É confirmado no sandbox, identificado por revisão estática, inconclusivo ou fora da cobertura?

Roadmap

Agrupar recomendações em contenção prioritária, correções de curto prazo e iniciativas estruturais. Indicar dependências, dono sugerido, critério técnico de validação e relação com a expansão. Recomendar guardrails de código e observabilidade quando relevantes para uma etapa futura de perfilamento, sem implantar nem atribuir atacantes.

Controle de qualidade

Revisar evidências e coerência da severidade, remover dados sensíveis, consolidar duplicidades, validar rastreabilidade e apresentar achados ao ponto focal antes do fechamento. Divergências factuais serão registradas e tratadas no período contratado.

15 / CRONOGRAMA

Até 30 dias úteis por frente

Cada frente tem calendário próprio; a contratação conjunta é executada em sequência, nunca em paralelo. Até 60 dias úteis de pentests, com início de cada frente após pré-requisitos. Ordem proposta: Cashfast e depois Zaztech, a confirmar. Ver Anexo A.

Dias	Foco	Saída / checkpoint
D1–D2	Kickoff, confirmação de LoA e inventário, documentação e entrevistas.	Baseline inicial e canais confirmados.
D3–D5	Fluxos, ameaças, sandbox, dados sintéticos, mocks e egress.	Gate D5: ambiente e escopo liberados.
D6–D9	Leitura dos fluxos críticos, identidade, API e domínio.	Matriz de hipóteses e cobertura.
D10–D13	SAST/SCA/segredos pontuais, dependências e configurações.	Gate D13: plano de validação atualizado.
D14–D17	Testes autenticados de identidade, autorização, APIs e dados.	Resultados por perfil e componente.
D18–D21	Lógica financeira, estados, repetição, integrações e falhas.	Evidências e impacto contextual.
D22–D24	Validações complementares, cadeia de risco e consolidação.	Gate D24: matriz atualizada e limitações.
D25–D27	Classificação, roadmap, revisão e relatório.	Versão técnica em revisão.
D28–D30	Apresentação, entrega e encerramento do sandbox.	Relatórios e registro de fechamento.

Cadência de gestão

Checkpoint semanal: status, cobertura, bloqueios, decisões e próximos passos. Comunicação imediata de risco crítico ou desvio de isolamento. Treinamentos podem começar após o primeiro relatório, durante a segunda frente; a última sessão ocorre após o segundo relatório. Não integram os 30 dias úteis de cada pentest.

Impedimentos

Impedimentos, indisponibilidade ou mudanças de baseline serão registrados com data, responsável e impacto. Atividades não afetadas prosseguem quando seguro; suspensão/replanejamento e retomada exigem acordo escrito, sem extensão unilateral automática.

16 / ENTREGÁVEIS

Documentação e evidências

Cada projeto recebe seu próprio conjunto de entregáveis. As conclusões são segregadas por titularidade e baseline.

Entregável	Conteúdo mínimo	Marco
Inventário e plano	Ativos, versões, regras, dependências, limites, prioridades e critérios de cobertura.	D5
Registro de ambiente	Baseline, diferenças, mocks, controles de isolamento e gate.	D5; atualizado
Relatório técnico	Metodologia, cobertura, achados, evidências, impacto, recomendações e limitações.	Até D30
Matriz de vulnerabilidades	Identificador, ativo, severidade, prioridade, status, evidência e recomendação.	Até D30
Matriz de cobertura	Cenário × ativo × versão × resultado; não executados/inconclusivos com motivo.	Até D30
Resumo executivo	Riscos materiais, relação com operação e decisões recomendadas.	Até D30
Roadmap e apresentação	Ordem de correção, dependências, próximos passos e reunião de resultados.	Até D30
Encerramento	Revogação de acessos, inventário de descarte e logs disponíveis/limitações.	Até D30, conforme política acordada

Ficha de achado — modelo

ID; título; componente e commit; ambiente; classe; status de evidência; severidade e rationale; contexto e pré-condições; evidência sanitizada; comportamento esperado versus observado; impacto potencial; causa raiz provável; recomendações específicas; prioridade; dependências; critério sugerido de validação. Não incluir dados ou segredos reais.

17 / RESPONSABILIDADES

Papéis, pré-requisitos e aceite

Responsável	Responsabilidades
Ionix / líder técnico	Condução metodológica, plano de cobertura, execução autorizada, escalonamento, evidências e qualidade dos relatórios.
Ionix / gestão do projeto	Kickoff, checkpoints, riscos, comunicação e mudanças formalizadas.
Cashfast / ponto focal	Inventário e titularidade, código/configuração sanitizados, fluxos, regras, dados sintéticos ou orientação para criá-los; validação do escopo.
Zaztech / ponto focal	Mesmas responsabilidades em seus ativos próprios; delimitar plataforma nova e dependências de legado, multiempresa, PDV/mobile.
Patrocinadores / jurídico	NDA, LoA e condições contratuais; autorizar compartilhamentos, mudanças e ambientes; aprovar modalidade comercial.
Equipe de engenharia	Esclarecimentos de domínio e configuração; validar entendimento e receber recomendações; implementar correções posteriormente se desejado.

Pré-requisitos de início

Início: NDA e LoA por titular, inventário, acesso nominal ao material sanitizado, documentação, ponto focal, janela, conta/custos do sandbox e política de retenção. Liberação dinâmica: baseline e fidelidade validados, dados sintéticos, mocks, egress isolado, canais de emergência e gate D5 aprovado.

Aceite do serviço

Aceite por entrega e cobertura aprovada, não por número ou ausência de achados. Cliente revisa os entregáveis, registra divergências fundamentadas e a Ionix corrige erros factuais do material; prazo de revisão e canal formalizados no contrato. Novos testes e mudanças de baseline não são revisão de entregável.

18 / RISCOS E CONTROLES

Riscos de execução e mitigação

Risco	Efeito	Mitigação
Inventário incompleto	Cobertura imprecisa.	Validar titularidade e baseline; registrar componentes não disponibilizados.
Sandbox não equivalente	Conclusões não generalizáveis.	Comparar configurações, documentar desvios; qualificar confiança.
Integração sem documentação	Mock incompleto.	Validar contratos e respostas com ponto focal; registrar limitações.
Dados ou segredos reais recebidos	Exposição indevida.	Saneamento, bloqueio de egress, interrupção e comunicação.
Mudança de versão	Perda de rastreabilidade.	Fixar commit; formalizar alteração e impacto no cronograma.
Achado crítico	Necessidade de ação rápida.	Comunicação imediata e recomendação de contenção; cliente decide ações em produção.
Indisponibilidade de responsáveis	Atraso ou hipótese inconclusiva.	Checkpoints, registro de impedimentos e continuidade de atividades não bloqueadas dentro da mesma frente; replanejamento formal.
Ampliação de escopo	Diluição da cobertura e prazo.	Controle de mudanças e contratação complementar se necessária.

Limitações de responsabilidade

A avaliação é pontual e condicionada às informações e versões fornecidas, à autorização e à equivalência do ambiente. Não substitui auditoria regulatória, certificação, parecer jurídico ou processo contínuo de segurança. As cláusulas jurídicas de responsabilidade, confidencialidade e proteção de dados serão formalizadas no contrato e no NDA, sem presumir garantias não acordadas.

19 / CAPACITAÇÃO

Treinamentos e próximos ciclos

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.

Sessão	Conteúdo sugerido	Objetivo
01 / Desenvolvimento seguro	Fundamentos OWASP, revisão de código, validação de entradas, tratamento de erros e prevenção de exposição.	Reconhecer e corrigir padrões de risco.
02 / Identidade e finanças	Autorização, segregação, estados, idempotência, tratamento de eventos e lógica de negócio.	Conectar controles a riscos financeiros.
03 / Prevenção e sustentação	Dependências, segredos, revisão segura, critérios de teste, guardrails e práticas DevSecOps.	Reduzir recorrência e preparar próximos ciclos.

Orientação pós-entrega

Esclarecimentos sobre achados e recomendações, por canal e janela a formalizar antes do kickoff; registro e encerramento de dúvidas. Sem implementação, plantão, reteste, monitoramento ou atendimento contínuo.

Trilhas futuras — contratação separada

- Remediação assistida e reteste formal das versões corrigidas.
- Black Box posterior e avaliações periódicas após hardening.
- CI/CD com SAST, SCA, detecção de segredos e políticas de release.
- Perfilamento de atacantes e observabilidade: proposta separada, após avaliação de telemetria, objetivos e período; faixa comercial sujeita à validação, fora dos R$ 80.000.
- Purple Team ou segurança contínua conforme maturidade e prioridades.

20 / INVESTIMENTO

Condições comerciais e próximos passos

A contratação pode ser individual ou conjunta. A condição conjunta reduz o valor de cada Pentest White Box sem reduzir a cobertura técnica acordada.

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. Escopo, relatório e aceite independentes.

Formalização do início

Aceite comercial e condições de pagamento; NDA/LoA e inventário de cada empresa; validação de pré-requisitos; kickoff do primeiro projeto e, após sua conclusão, kickoff do segundo. Até 30 dias úteis por frente; cronograma consolidado no Anexo A.

Contato Ionix Tech

Destinada exclusivamente aos representantes autorizados de Cashfast e Zaztech. Agenda, faturamento, retenção e demais condições pendentes serão formalizados no contrato.

ANEXO A / CRONOGRAMA CONSOLIDADO

Execução sequencial e marcos de pagamento

Ordem proposta: Cashfast primeiro, Zaztech depois, a confirmar na mobilização. Sem sobreposição de pentests. Semanas de cinco dias úteis, relativas ao início de cada frente, não datas de calendário garantidas.

Semanas por frente	Atividades	Saída / marco
S1 / S7 · D1–D5	Inventário, fluxos, sandbox, mocks e gate de isolamento.	Baseline e liberação do ambiente.
S2 / S8 · D6–D10	Revisão manual dos fluxos críticos, identidade e APIs.	Hipóteses e cobertura.
S3 / S9 · D11–D15	Dependências, segredos, configurações e início dos testes.	Plano validado e evidências iniciais.
S4 / S10 · D16–D20	Testes autenticados e lógica financeira.	Resultados por cenário.
S5 / S11 · D21–D25	Validações, limitações, classificação e roadmap.	Matriz consolidada.
S6 / S12 · D26–D30	Revisão, relatórios, apresentação, encerramento.	Relatório executivo da frente.

Quatro marcos da contratação conjunta

M1 · Kickoff do primeiro projeto: R$ 20.000. M2 · Entrega do primeiro relatório executivo: R$ 20.000. M3 · Entrega do segundo relatório executivo: R$ 20.000. M4 · Conclusão do terceiro treinamento: R$ 20.000. Total R$ 80.000. Datas de vencimento e faturamento serão formalizados.

Treinamentos e fechamento

Três sessões de 60 minutos no total, em janela de até 30 dias a combinar; início possível após o primeiro relatório, durante a segunda frente; última sessão após o segundo relatório. Os marcos são relativos aos entregáveis, não meses corridos. Feriados, indisponibilidades e impedimentos acordados podem alterar as datas de calendário.