Manifold

PROPOSTA TÉCNICA

Auditoria de Segurança e Avaliação de Escalabilidade da Plataforma Moola

Security Assessment, Load Testing and Stress Testing

Preparado por:	Manifold, Lda
Marca institucional:	MANIFOLD
Preparado para:	FTM - Future Technologies of Mozambique
Referência documental:	01_Proposta_Tecnica_Moola_FTM_MANIFOLD_RevA1
Revisão:	A1
Data de emissão:	03 de agosto de 2026
Classificação:	Confidencial
Revisto por:	Vayile Fumo
Aprovado por:	Rogerio Casimiro

Controlo documental

Elemento	Informação
Documento	Proposta Técnica para Auditoria de Segurança e Avaliação de Escalabilidade da Plataforma Moola
Cliente	FTM - Future Technologies of Mozambique
Prestador	Manifold, Lda
Referência	01_Proposta_Tecnica_Moola_FTM_MANIFOLD_RevA1
Revisão	A1
Data	03 de agosto de 2026
Preparado por	MANIFOLD
Revisto por	Vayile Fumo
Aprovado por	Rogerio Casimiro
Classificação	Confidencial
Validade técnica	Em conformidade com a validade indicada na Proposta Financeira correspondente

Histórico de revisões

Revisão	Data	Descrição	Preparado por	Revisto por	Aprovado por
A0	03/08/2026	Proposta ajustada ao âmbito prioritário de segurança e escalabilidade comunicado pela FTM	MANIFOLD	Vayile Fumo	Rogerio Casimiro
A1	03/08/2026	Revisão contratual do âmbito, limites quantitativos, ciclos de execução, readiness, custos extraordinários e condições de reteste.	MANIFOLD	Vayile Fumo	Rogerio Casimiro

Confidencialidade

O presente documento contém informação técnica, metodológica e comercial proprietária da Manifold, Lda e destina-se exclusivamente à avaliação interna da FTM - Future Technologies of Mozambique.

A sua reprodução, distribuição ou disponibilização a terceiros deverá limitar-se às pessoas diretamente envolvidas na avaliação, contratação e governação dos serviços propostos.

Mensagem executiva

Na sequência da atualização de prioridades comunicada pela FTM - Future Technologies of Mozambique, a MANIFOLD apresenta uma proposta ajustada para a realização de uma **auditoria de segurança** e de uma **auditoria de escalabilidade, incluindo stress testing**, da plataforma Moola.

A proposta foi estruturada para respeitar a intenção da FTM de executar as auditorias de forma faseada, concentrando o investimento atual nos riscos considerados prioritários antes da entrada em produção e reservando outras avaliações complementares para etapas posteriores da evolução da plataforma.

Para apoiar a decisão da FTM, são apresentadas duas alternativas:

- **Opção A - Security & Stress Assessment:** responde estritamente aos dois serviços solicitados pela FTM;
- **Opção B - Security, Scalability & Readiness Assurance:** inclui integralmente o âmbito da Opção A e acrescenta avaliações preventivas recomendadas pela MANIFOLD para reduzir riscos de retrabalho, indisponibilidade, fraude e limitações de crescimento.

A Opção A avalia a plataforma atual sob o âmbito e a carga contratados. A Opção B, recomendada pela MANIFOLD, acrescenta maior profundidade de assurance, maior volume de carga e readiness indicativo para pagamentos reais e canal web. O investimento adicional é de 290 000 MT, IVA incluído, e visa reduzir o risco de retrabalho e de identificação tardia de limitações.

Sumário executivo

A FTM poderá avaliar os riscos prioritários da Moola em 20 a 25 dias úteis

A Moola é uma plataforma digital de jogos peer-to-peer, desenvolvida em Flutter para Android e iOS e suportada por serviços Firebase e Google Cloud.

De acordo com a informação partilhada pela FTM, a plataforma permite que jogadores criem ou aceitem convites, entrem em salas, disputem jogos entre si e utilizem valores atualmente simulados no contexto das partidas. A futura integração com M-Pesa ainda não se encontra implementada.

A arquitetura tecnológica inclui, entre outros componentes:

- Flutter;
- Firebase Authentication;
- Cloud Firestore;
- Cloud Functions;
- Firebase Storage;
- Firebase App Check;
- Firebase Cloud Messaging;
- serviços e infraestrutura Google Cloud;
- APIs e integrações entre a aplicação móvel e o backend.

A prioridade atual da FTM é compreender:

1. se a aplicação, o backend e a infraestrutura apresentam vulnerabilidades relevantes;

2. se a lógica dos jogos, salas, convites e saldos pode ser manipulada;

3. como a plataforma se comporta com múltiplos utilizadores e partidas simultâneas;

4. em que ponto surgem degradação, erros, contenção ou saturação;

5. que correções devem ser realizadas antes da entrada em produção.

Resultado esperado

Ao final dos trabalhos, a FTM receberá uma avaliação baseada em evidências sobre:

- vulnerabilidades técnicas;
- falhas de autenticação e autorização;
- riscos de fraude e abuso da lógica de negócio;
- riscos de manipulação de partidas e saldos;
- exposição decorrente de configurações Firebase ou Google Cloud;
- comportamento da plataforma sob carga;
- limites de capacidade observados;
- principais gargalos;
- prioridades de correção;
- riscos que podem ser tratados numa fase posterior.

A conclusão emitida será limitada aos domínios efetivamente contratados e avaliados.

1. O que entendemos sobre a plataforma Moola

1.1 A Moola combina aplicação móvel, jogos peer-to-peer e lógica transacional

Com base nas informações fornecidas pela FTM, a Moola apresenta atualmente as seguintes características:

Elemento	Entendimento atual
Canal principal	Aplicação móvel

Elemento	Entendimento atual
Plataformas	Android e iOS
Tecnologia mobile	Flutter
Modelo de utilização	Jogos peer-to-peer
Exemplos de jogos	Checkers (Damas); Tic-tac-toe; Chess (Xadrez)
Formação das partidas	Convites entre jogadores ou entrada em sala com jogador disponível
Valores utilizados	Valores simulados, tipicamente entre 50 e 200 MT
Pagamentos reais	Integração M-Pesa ainda não implementada
Aplicação web	Ainda não implementada
Backend	Firebase e Google Cloud
Autenticação	Firebase Authentication
Base de dados	Cloud Firestore
Funções backend	Cloud Functions
Armazenamento	Firebase Storage
Proteção adicional	Firebase App Check
Notificações	Firebase Cloud Messaging

A aplicação apresentada pela FTM demonstrou uma interface visual coerente e aparentemente madura. Esta observação não constitui validação funcional, de segurança, disponibilidade ou escalabilidade.

1.2 A natureza peer-to-peer cria riscos além da segurança convencional

Numa aplicação deste tipo, não basta validar login, APIs e configuração cloud.

A auditoria deve também compreender se um jogador consegue:

- manipular o estado da partida;
- efetuar jogadas inválidas;
- repetir uma jogada;
- alterar o adversário;
- entrar numa sala sem autorização;
- observar ou modificar partidas de terceiros;
- provocar resultados divergentes;
- submeter unilateralmente o resultado;
- explorar desconexões e timeouts;
- criar condições de double spending;
- obter créditos indevidos;
- abusar de convites, salas ou contas;
- automatizar ações através de bots;
- contornar controlos existentes no cliente móvel.

Um princípio central da avaliação será verificar se o backend, e não a aplicação do jogador, permanece como autoridade final para decisões críticas.

1.3 A futura utilização de dinheiro real exige preparação adicional

Embora os valores sejam atualmente simulados, a lógica implementada poderá futuramente suportar depósitos, prémios, cobranças ou outras operações monetárias.

A auditoria atual poderá avaliar:

- integridade do saldo simulado;
- atualização concorrente;

- prevenção de créditos ou débitos duplicados;
- idempotência;
- reconciliação entre jogo, resultado e saldo;
- autorização das operações;
- segregação entre cliente e backend.

Contudo, a integração M-Pesa real não poderá ser tecnicamente auditada antes de existir uma implementação funcional.

Qualquer ativação futura de transações reais deverá ser precedida por uma avaliação específica da integração M-Pesa.

1.4 A versão web é uma oportunidade futura, não um ativo atualmente auditável

A plataforma ainda não dispõe de uma versão web implementada.

Consequentemente:

- não existe uma aplicação web funcional para testes;
- não poderá ser emitida uma conclusão de segurança ou performance sobre um produto inexistente;
- o desenvolvimento da versão web não faz parte da presente auditoria.

Na Opção B, a MANIFOLD propõe apenas uma avaliação indicativa de compatibilidade e prontidão do projeto Flutter para futura disponibilização web.

2. O pedido atualizado da FTM orienta esta proposta

A FTM comunicou que, nesta fase, pretende priorizar:

1. auditoria de segurança;

2. auditoria de escalabilidade, incluindo Stress Test.

A FTM indicou igualmente a intenção de realizar outras auditorias complementares de forma progressiva, à medida que a plataforma evoluir.

A presente proposta respeita essa abordagem faseada.

Não são reintroduzidos na Opção A domínios que a FTM decidiu adiar, como uma auditoria integral de maturidade, qualidade global do código, DevSecOps completo, privacidade, continuidade ou conformidade regulatória.

3. A MANIFOLD apresenta duas opções independentes

3.1 Estrutura das opções

Elemento	Opção A	Opção B
Designação	Security & Stress Assessment	Security, Scalability & Readiness Assurance
Revisão de código	Orientada ao risco e por amostragem	Orientada ao risco, com cobertura adicional
Fluxos críticos	Até 10	Até 15
Utilizadores virtuais	Até 500	Até 1 000
Partidas simultâneas	Até 250	Até 500
Campanha de load/stress	Uma	Uma
Spike test	Não incluído	Um
Soak test	Não incluído	Um, até 2 horas
Threat model	Simplificado	Formal e documentado
Ciclos de comentários	Um	Um
Reteste	Não incluído	Um ciclo; todos os Críticos e até 8 Altos
M-Pesa	Não incluído	Readiness indicativo

Elemento	Opção A	Opção B
Flutter Web	Não incluído	Readiness indicativo
Prazo principal até à versão preliminar	20 dias úteis	25 dias úteis

3.2 A Opção A responde exatamente à prioridade comunicada pela FTM

A Opção A concentra a execução nos serviços prioritários comunicados pela FTM:

- revisão de segurança orientada ao risco e por amostragem;
- até dez fluxos críticos;
- um shakedown test, uma baseline e uma campanha principal de load e stress testing;
- até 500 utilizadores virtuais e 250 partidas simultâneas;
- versão preliminar, um ciclo consolidado de comentários e versão final dos relatórios;
- apresentação executiva.

Não inclui readiness M-Pesa ou Flutter Web, spike test, soak test ou reteste.

3.3 A Opção B acrescenta assurance sobre riscos próximos

A Opção B inclui integralmente a Opção A e é recomendada para antecipar riscos de crescimento, monetização e disponibilização de novos canais antes de essas evoluções se tornarem mais críticas ou dispendiosas de corrigir. Acrescenta:

- cobertura orientada ao risco superior à Opção A e threat model formal;
- até quinze fluxos críticos;
- até 1 000 utilizadores virtuais e 500 partidas simultâneas;
- um spike test e um soak test de até duas horas;
- avaliação de observabilidade e modelo inicial de capacidade;
- M-Pesa Security Readiness e Flutter Web Readiness, ambos indicativos;
- workshop técnico;
- um único ciclo de reteste, abrangendo todos os findings originalmente classificados como Críticos e até oito findings classificados como Altos.

4. A execução será independente, controlada e baseada em evidências

4.1 Princípios de execução

Princípio	Aplicação
Independência	As conclusões serão baseadas nas evidências observadas, independentemente das equipas que desenvolveram a plataforma
Risk-based approach	O esforço será concentrado nos ativos e fluxos com maior impacto técnico e de negócio
Least privilege	Os acessos da MANIFOLD serão limitados ao estritamente necessário
Staging-first	Testes intrusivos e de carga ocorrerão preferencialmente num ambiente de staging
Não destrutivo	Não serão executados testes destinados a provocar perda de dados ou indisponibilidade em produção
Evidência reproduzível	Findings materiais deverão possuir evidência e método de reprodução
Validação humana	Ferramentas automáticas não substituirão análise e validação por especialistas
Confidencialidade	Código, credenciais, logs, dados e findings serão tratados como informação confidencial
Transparência	Limitações técnicas e resultados inconclusivos serão declarados

Princípio	Aplicação
Controlo de custos	A geração de carga será acompanhada por limites, alertas e critérios de paragem

4.2 A auditoria não constitui garantia absoluta

A avaliação representa o estado observado:

- durante o período contratado;
- sobre os ativos disponibilizados;
- com os acessos concedidos;
- dentro dos limites de teste aprovados;
- com base nas versões de código e configurações avaliadas.

A ausência de um finding não constitui garantia absoluta de inexistência de vulnerabilidades.

Alterações posteriores ao código, infraestrutura, regras, integrações ou arquitetura poderão exigir nova validação.

5. A metodologia combina revisão, testes manuais e simulação controlada

Fase 0 - Mobilização e confirmação do âmbito

Atividades:

- reunião de abertura;
- confirmação dos objetivos;
- validação da opção selecionada;
- confirmação do inventário;
- identificação dos fluxos críticos;
- validação dos ambientes;
- confirmação dos acessos;
- definição dos contactos;
- aprovação das regras de execução;
- validação dos critérios de paragem;
- definição do canal seguro;
- confirmação das janelas de teste.

Saída:

> Plano de Auditoria e baseline de execução.

Fase 1 - Descoberta e modelação técnica

Atividades:

- análise da arquitetura disponível;
- revisão dos fluxos de autenticação;
- revisão dos fluxos de salas e partidas;
- análise dos fluxos de saldos;
- identificação das fronteiras de confiança;
- mapeamento de APIs e Cloud Functions;
- identificação das contas de serviço;
- análise das regras Firestore e Storage;
- compreensão das integrações;
- definição dos cenários de fraude;
- definição dos cenários de carga.

Na Opção A será produzido um threat framing simplificado.

Na Opção B será produzido um threat model formal e documentado.

Fase 2 - Auditoria de segurança

Atividades:

- **revisão de código Flutter orientada ao risco e por amostragem;**
- **revisão das Cloud Functions orientada ao risco e por amostragem;**
- análise das dependências;
- análise de credenciais e segredos;
- revisão das regras Firebase;
- revisão de IAM;
- testes mobile;
- testes às APIs;
- testes de autenticação;
- testes de autorização;
- testes de lógica de negócio;
- testes de concorrência;
- testes de fraude;
- validação manual dos findings.

Fase 3 - Preparação dos testes de escalabilidade

Atividades:

- criação de utilizadores sintéticos;
- preparação de dados de teste;
- desenvolvimento dos scripts;
- desenvolvimento do simulador de partidas;
- definição do perfil de carga;
- **utilização dos dashboards e métricas disponibilizados pela FTM e, quando necessário, de dashboards internos temporários da MANIFOLD;**
- validação das métricas;
- shakedown test;
- confirmação do kill switch.

Fase 4 - Execução dos testes de escalabilidade

Atividades comuns:

- baseline test;
- load test;
- stress test;
- análise de recuperação;
- recolha de métricas;
- análise de erros;
- identificação de gargalos.

Atividades adicionais da Opção B:

- spike test;
- soak test;
- análise aprofundada de recuperação;
- modelo inicial de capacidade;
- análise dedicada de observabilidade.

Fase 5 - Validação e reporting

Atividades:

- consolidação dos resultados;
- reprodução dos findings;

- eliminação de falsos positivos;
- classificação de criticidade;
- análise de causa raiz;
- preparação das recomendações;
- elaboração do plano de ações;
- preparação dos relatórios;
- revisão independente de qualidade;
- apresentação à FTM.

Fase 6 - Reteste, aplicável à Opção B

Atividades:

- receção das evidências de correção;
- reprodução dos findings;
- validação das correções;
- identificação de risco residual;
- atualização do estado;
- emissão do relatório de reteste.

6. As duas opções avaliam os principais vetores de ataque da Moola

As verificações apresentadas representam os domínios e cenários elegíveis para avaliação. A seleção efetiva dos procedimentos será orientada ao risco, por amostragem e concentrada nos componentes, funções e fluxos com maior impacto sobre autenticação, autorização, dados, partidas, resultados, saldos, privilégios e exposição externa.

A revisão não corresponde a uma análise linha a linha de todo o código-fonte nem a uma auditoria integral de qualidade, arquitetura ou manutenibilidade.

6.1 Aplicação Flutter para Android e iOS

A avaliação deverá abranger:

- armazenamento local;
- tokens;
- sessões;
- cache;
- credenciais;
- dados sensíveis;
- logs;
- builds de debug;
- chaves ou configurações expostas;
- comunicação com o backend;
- validação de certificados;
- deep links;
- notificações;
- dependências;
- plugins;
- engenharia reversa;
- instrumentação;
- clientes modificados;
- emuladores;
- dispositivos com root ou jailbreak, quando aplicável;
- comportamento da aplicação quando o backend está sob carga.

A revisão não será exclusivamente automática.

Os resultados de ferramentas de análise estática ou dinâmica serão validados manualmente.

Os testes dinâmicos iOS dependem da disponibilização de uma build instalável, TestFlight ou mecanismo equivalente, contas de teste e ambiente compatível. Na ausência destes elementos, a cobertura iOS ficará limitada à revisão de código, configuração, dependências e evidências disponibilizadas.

Nessa situação, o esforço previsto para os testes dinâmicos iOS será redirecionado para aprofundar a revisão orientada ao risco do código Flutter e dos componentes backend abrangidos, nomeadamente Cloud Functions e APIs, mantendo os limites de ativos, fluxos e prazo contratados. Esta redistribuição preserva o esforço contratado, mas não equivale à execução de testes dinâmicos iOS; uma build disponibilizada depois da data acordada ficará sujeita à disponibilidade da equipa e, quando houver impacto material, a Change Request.

6.2 Firebase Authentication

A auditoria avaliará:

- registo;
- login;
- recuperação de conta;
- alteração de credenciais;
- criação de múltiplas contas;
- enumeração de utilizadores;
- gestão de tokens;
- expiração;
- revogação;
- persistência de sessões;
- perfis;
- custom claims;
- privilégios;
- contas suspensas;
- controlo de tentativas;
- bypass de autenticação;
- bypass de autorização.

6.3 Cloud Firestore

A auditoria avaliará:

- Security Rules;
- acesso entre utilizadores;
- acesso a salas de terceiros;
- enumeração de documentos;
- leitura indevida;
- escrita indevida;
- alterações diretas ao estado do jogo;
- validação de campos;
- alterações de saldo;
- transações;
- concorrência;
- índices;
- listeners;
- documentos com elevada contenção;
- padrões de leitura e escrita;
- impacto dos padrões de dados na escalabilidade.

6.4 Firebase Storage

A avaliação abrangerá:

- regras de acesso;
- ficheiros privados;

- URLs;
- exposição de objetos;
- upload não autorizado;
- substituição de ficheiros;
- validação de extensão e conteúdo;
- controlo por utilizador;
- retenção;
- permissões administrativas.

6.5 Cloud Functions e Node.js

A avaliação abrangerá:

- autenticação;
- autorização;
- validação de input;
- tratamento de erros;
- funções públicas;
- triggers;
- Admin SDK;
- contas de serviço;
- segredos;
- variáveis de ambiente;
- logging;
- dependências;
- vulnerabilidades conhecidas;
- replay;
- idempotência;
- concorrência;
- race conditions;
- timeouts;
- cold starts;
- quotas;
- limites de instâncias;
- escalonamento;
- risco de custos inesperados.

Um objetivo crítico será identificar funções que operem com privilégios administrativos superiores ao necessário.

6.6 IAM e contas de serviço

A avaliação incluirá:

- inventário de identidades;
- roles;
- permissões;
- contas de serviço;
- chaves;
- segregação entre ambientes;
- princípio do menor privilégio;
- funções administrativas;
- acessos temporários;
- credenciais inativas;
- permissões herdadas;
- exposição de segredos;
- caminhos de elevação de privilégio.

6.7 APIs e integrações

A avaliação incluirá:

- autenticação;
- autorização por função;
- autorização por recurso;
- manipulação de parâmetros;
- validação de input;
- controlo de erros;
- exposição de dados;
- replay;
- rate limiting;
- enumeração;
- abuso de endpoints;
- chamadas repetidas;
- alteração de identificadores;
- utilização de tokens de outros utilizadores;
- integração entre a aplicação móvel e o backend.

7. A lógica peer-to-peer exige testes específicos de fraude e manipulação

7.1 Salas e convites

Serão avaliados cenários como:

- criação de salas sem os controlos esperados;
- criação massiva de salas;
- entrada numa sala sem autorização;
- reutilização de convites;
- previsão ou enumeração de identificadores;
- alteração do destinatário;
- aceitação concorrente;
- entrada de utilizador diferente;
- utilização de sala encerrada;
- observação indevida de partidas;
- manipulação do adversário;
- abandono deliberado.

7.2 Estado da partida

Serão avaliados:

- envio de jogada inválida;
- repetição de jogada;
- alteração da ordem;
- manipulação do tabuleiro;
- alteração do estado local;
- divergência entre jogadores;
- submissão unilateral de resultado;
- alteração do vencedor;
- utilização de versão antiga da aplicação;
- reconexão com estado inconsistente;
- manipulação do relógio;
- abuso de timeout;
- mensagens fora da sequência;

- concorrência entre atualizações.

7.3 Resultados e integridade

Serão avaliados:

- resultado submetido pelo cliente;
- resultado não validado pelo backend;
- dois vencedores para a mesma partida;
- múltiplas conclusões;
- reabertura de partida;
- alteração após conclusão;
- replay de mensagem de vitória;
- atualização incompleta;
- discrepância entre partida e histórico.

7.4 Saldos simulados

Serão avaliados:

- alteração direta de saldo;
- saldo negativo;
- crédito sem resultado válido;
- débito duplicado;
- crédito duplicado;
- double spending;
- repetição de pedidos;
- concorrência entre operações;
- manipulação do valor da partida;
- alteração dos limites previstos;
- falhas de idempotência;
- inconsistência entre jogo, resultado e saldo.

7.5 Automação e abuso

Serão considerados:

- múltiplas contas;
- bots;
- scripts automatizados;
- criação massiva de convites;
- criação massiva de partidas;
- repetição de requests;
- bypass do App Check;
- clientes modificados;
- abuso de emuladores;
- colusão;
- farming;
- utilização artificial de partidas.

8. O Stress Test reproduzirá utilizadores e partidas reais

8.1 Não serão necessários centenas de dispositivos físicos

A carga será gerada por utilizadores virtuais que reproduzem as operações efetuadas pela aplicação.

Os dispositivos físicos e emuladores serão utilizados para confirmar o comportamento da aplicação Flutter enquanto o backend está sob carga.8.2 Jornada-base de um par de jogadores

Jogador A autentica
↓
Jogador B autentica
↓
Jogador A envia convite ou entra em matchmaking
↓
Jogador B aceita
↓
A sala é criada
↓
Os dois jogadores iniciam listeners
↓
Jogador A efetua uma jogada
↓
Jogador B recebe a atualização e responde
↓
A partida continua
↓
O backend determina ou valida o resultado
↓
O saldo simulado é atualizado
↓
A partida é encerrada e registada no histórico

8.3 Perfis de utilização

A simulação não colocará todos os utilizadores a executar a mesma atividade.

O perfil de carga poderá incluir:

- utilizadores a autenticar;
- utilizadores a consultar perfil;
- utilizadores a consultar amigos;
- utilizadores a enviar convites;
- utilizadores à espera de adversário;
- utilizadores em partidas;
- utilizadores a consultar histórico;
- utilizadores a abandonar partidas;
- utilizadores a reconectar;
- utilizadores a repetir ações.

8.4 Volume de carga proposto

Utilizadores virtualmente ativos	Partidas simultâneas aproximadas
50	Até 25
100	Até 50
250	Até 125
500	Até 250
1 000	Até 500

A Opção A terá como limite máximo proposto 500 utilizadores virtualmente ativos e 250 partidas simultâneas.

A Opção B terá como limite máximo proposto 1 000 utilizadores virtualmente ativos e 500 partidas simultâneas.

O teste poderá ser interrompido antes de atingir o limite máximo quando forem identificados:

- degradação material;
- saturação;
- erro persistente;
- inconsistência de dados;
- risco de indisponibilidade;

- quota crítica;
- consumo não controlado;
- instrução de paragem.

9. Os testes de escalabilidade serão executados de forma progressiva

Uma campanha de testes corresponde a uma sequência coordenada de execuções realizada sobre o mesmo ambiente, configuração, scripts, dados e modelo de carga aprovados. A campanha pode conter vários patamares progressivos de carga, sem que esses patamares constituam campanhas adicionais.

A Opção A inclui:

- um shakedown test;
- uma baseline;
- uma campanha principal de load e stress testing.

A Opção B inclui:

- um shakedown test;
- uma baseline;
- uma campanha principal de load e stress testing;
- um spike test;
- um soak test de até duas horas.

Está incluída apenas a repetição de um procedimento cuja execução tenha sido invalidada por falha diretamente imputável à MANIFOLD.

Não estão incluídas repetições motivadas por:

- nova build ou alteração do código;
- alteração da arquitetura, configuração ou dados;
- indisponibilidade do ambiente da FTM ou ausência de métricas;
- nova campanha solicitada pela FTM;
- correções implementadas depois da campanha principal.

Estas situações serão tratadas por Change Request ou reteste, conforme aplicável.

9.1 Shakedown test

Objetivo:

- validar os scripts;
- confirmar contas;
- verificar dados sintéticos;
- confirmar logs;
- validar métricas;
- testar o kill switch;
- confirmar os limites de custo.

Carga indicativa:

- 5 a 20 utilizadores.

9.2 Baseline test

Objetivo:

- estabelecer o comportamento normal;
- medir latência inicial;
- medir throughput;
- observar cold starts;
- confirmar estabilidade.

Carga indicativa:

- 25 a 50 utilizadores.

9.3 Load test

Objetivo:

- observar o comportamento sob carga esperada;
- avaliar degradação progressiva;
- medir throughput e erro;
- identificar gargalos iniciais.

Patamares indicativos:

Patamar	Utilizadores ativos	Partidas aproximadas
L1	100	50
L2	250	125
L3	500	250

A Opção B poderá incluir patamares adicionais até 1 000 utilizadores.

9.4 Stress test

Objetivo:

- aumentar progressivamente a carga;
- identificar o ponto de degradação;
- identificar o ponto de saturação;
- avaliar a reação dos serviços;
- medir a recuperação.

O objetivo não será provocar indisponibilidade deliberada, mas compreender os limites da solução.

9.5 Spike test - Opção B

Objetivo:

- simular entrada repentina de utilizadores;
- avaliar autoscaling;
- medir cold starts;
- observar pedidos rejeitados;
- analisar recuperação.

Exemplo de cenário:

> 100 utilizadores → 500 utilizadores num período curto

9.6 Soak test - Opção B

Objetivo:

- manter carga estável durante um período prolongado;
- identificar degradação progressiva;
- detetar listeners abandonados;
- observar fugas de memória;
- analisar filas;
- analisar acumulação de eventos;
- observar crescimento de custos;
- validar estabilidade.

Duração máxima proposta:

Até duas horas de carga sustentada.

10. As métricas demonstrarão capacidade, degradação e recuperação

A avaliação deverá recolher, conforme disponibilidade:

- latência média;
- p50;
- p95;
- p99;
- throughput;
- pedidos por segundo;
- taxa de erro;
- autenticações por minuto;
- partidas iniciadas;
- partidas concluídas;
- partidas falhadas;
- tempo de criação de sala;
- tempo de propagação de jogada;
- sessões;
- listeners;
- reads;
- writes;
- transações;
- contenção;
- Cloud Functions invocadas;
- número de instâncias;
- concurrency;
- CPU;
- memória;
- cold starts;
- quotas;
- timeouts;
- recuperação;
- consumo cloud.

10.1 Metas iniciais indicativas

Indicador	Meta inicial proposta
Taxa de erro sob carga operacional	Inferior a 1%
Login, convite e criação de sala - p95	Inferior a 2 segundos
Propagação de jogada - p95	Inferior a 1 segundo
Inconsistência de resultado	Zero
Inconsistência de saldo	Zero
Recuperação após pico	Até 10 minutos

Estas metas são indicativas e serão confirmadas depois da análise da arquitetura, da baseline e das expectativas de utilização da FTM.

A ausência de requisitos não deverá ser interpretada como garantia de cumprimento automático destes valores.

11. A execução combinará especialistas, automação e validação manual

11.1 Ferramentas previstas

Função	Ferramentas ou tecnologias previstas
Segurança mobile	MobSF, JADX, Apktool, Frida, Objection, Android Studio e Xcode
Segurança de APIs	Burp Suite Professional e ferramentas auxiliares
Código e dependências	Semgrep, Gitleaks, Trivy, OSV-Scanner e gestores de dependências
Firebase Rules	Firebase Emulator Suite e testes unitários de regras
Geração de carga	Grafana k6
Simulação de jogadores	Node.js com Firebase Client SDK
Observabilidade	Cloud Monitoring, Cloud Logging e dashboards
Evidências	Repositório seguro e Finding Register controlado

A seleção final dependerá:

- da arquitetura confirmada;
- das interfaces disponíveis;
- do ambiente;
- dos acessos;
- das autorizações aprovadas.

11.2 Ferramentas não substituem especialistas

Scanners e ferramentas automáticas podem:

- identificar padrões;
- acelerar verificações;
- sinalizar dependências;
- gerar carga;
- recolher métricas.

Não podem, isoladamente:

- compreender completamente a lógica dos jogos;
- determinar impacto de negócio;
- validar fraude;
- interpretar race conditions;
- distinguir falsos positivos;
- emitir conclusões de prontidão;
- priorizar adequadamente as correções.

12. A auditoria poderá exigir código de teste, não alterações ao produto

12.1 Código de produção

Por regra, a MANIFOLD não alterará diretamente:

- código de produção;
- regras de produção;
- configuração de produção;

- funções de produção;
- dados de produção.

Os acessos deverão ser predominantemente:

- read-only;
- Viewer;
- temporários;
- individualizados;
- protegidos por MFA.

12.2 Código de teste

Será necessário desenvolver código separado para:

- utilizadores virtuais;
- autenticação;
- convites;
- salas;
- listeners;
- jogadas;
- resultados;
- saldos simulados;
- concorrência;
- recolha de métricas;
- limpeza de dados.

Estrutura indicativa:

```
moola-audit-tests/
├── k6/
│   ├── authentication
│   ├── invitations
│   ├── matchmaking
│   ├── game-room
│   ├── gameplay
│   ├── wallet-simulation
│   └── stress-scenarios
├── firebase-simulator/
│   ├── users
│   ├── rooms
│   ├── games
│   ├── balances
│   └── listeners
├── security-rules-tests/
├── synthetic-data/
├── metrics/
└── evidence/
```

Este código não será incorporado no produto sem contratação e aprovação específicas.

12.3 Alterações de instrumentação

Poderá ser necessário solicitar à FTM:

- uma build de staging;
- logging adicional;
- correlation IDs;
- contas de teste;
- configuração de App Check para testes autorizados;
- dashboards;
- acesso a métricas;
- índices de staging;
- limites de instâncias;
- feature flags;
- separação de dados sintéticos.

Qualquer alteração será:

- documentada;
- aprovada;
- limitada ao ambiente autorizado;
- reversível;
- executada pela FTM ou mediante autorização específica.

13. A inteligência artificial não será o auditor

A metodologia será:

> **Human-led, tool-assisted and evidence-based.**

A inteligência artificial poderá apoiar tarefas como:

- estruturação inicial de casos de teste;
- geração assistida de código repetitivo;
- organização de logs;
- identificação preliminar de padrões;
- preparação de resumos;
- revisão linguística.

A inteligência artificial não será utilizada para:

- executar autonomamente testes intrusivos;
- autorizar exploração;
- classificar definitivamente findings;
- substituir revisão manual;
- tomar decisões de risco;
- aceder a credenciais;
- processar código ou dados da FTM em serviços públicos não autorizados.

Nenhum código, credencial, log, dado pessoal ou evidência confidencial da FTM será submetido a serviços públicos de inteligência artificial sem autorização escrita.

14. A Opção B acrescenta avaliações preventivas de evolução

14.1 Threat model formal

A Opção B incluirá um documento com:

- ativos;
- atores;
- fluxos;
- fronteiras de confiança;
- superfícies de ataque;
- ameaças;
- cenários de abuso;
- controlos;
- riscos residuais;
- prioridades.

14.2 Segurança aprofundada

A Opção B acrescentará cobertura orientada ao risco superior à Opção A, incluindo:

- amostragem adicional de funções privilegiadas e fluxos transacionais;
- pesquisa expandida de segredos e dependências críticas;
- cenários avançados de fraude, bots, múltiplas contas, colusão e farming;

- análise aprofundada de concorrência e integridade dos resultados;
- manipulação de clientes e avaliação adicional de recuperação e inconsistência.

14.3 Capacidade e observabilidade

A Opção B acrescentará:

- revisão de dashboards;
- avaliação de alertas;
- análise de métricas;
- avaliação de logging;
- análise de limites de autoscaling;
- análise de concurrency;
- análise de instâncias mínimas e máximas;
- identificação de hotspots;
- modelo inicial de capacidade;
- análise indicativa de custos.

14.4 M-Pesa Security Readiness (avaliação indicativa)

A Opção B incluirá uma avaliação indicativa do desenho previsto para a futura integração M-Pesa, limitada à identificação de requisitos de segurança, idempotência, callbacks, webhooks, reconciliação, reversões, estados pendentes, gestão de credenciais e trilho de auditoria.

Esta atividade exclui expressamente:

- testes à API M-Pesa e transações reais;
- validação end-to-end e reconciliação efetiva;
- certificação e parecer regulatório;
- implementação;
- revisão contratual do provedor.

14.5 Flutter Web Readiness (avaliação indicativa)

A Opção B incluirá uma avaliação indicativa da prontidão técnica do projeto Flutter para futura compilação web, incluindo configuração, inventário de plugins, dependências, autenticação no browser, armazenamento local, viewport e limitações técnicas identificáveis.

Esta atividade exclui expressamente:

- desenvolvimento web e alteração do código;
- correção de plugins;
- implementação de responsividade;
- testes cross-browser completos;
- UX/UI web;
- auditoria de uma aplicação web funcional.

14.6 Reteste

A Opção B inclui um único ciclo de reteste, abrangendo todos os findings originalmente classificados como Críticos e até oito findings classificados como Altos.

O reteste será realizado dentro de uma janela de 45 dias e limita-se à validação das correções implementadas sobre os mesmos ativos, fluxos e arquitetura material.

Não inclui novos módulos, novas funcionalidades, nova campanha, novos findings ou reabertura integral da auditoria.

Caso existam mais de oito findings Altos elegíveis, serão selecionados:

1. os findings Altos com maior impacto de negócio;
2. depois, os de maior exposição ou urgência de remediação;
3. em caso de empate, os oito acordados entre a MANIFOLD e a FTM.

Findings Altos além dos oito, e findings Médios ou Baixos, poderão ser retestados por Change Request. Um finding corresponde a uma vulnerabilidade distinta, não a cada ocorrência do mesmo problema.

15. Os entregáveis suportarão a decisão da FTM

15.1 Entregáveis comuns

Entregável	Opção A	Opção B
Plano de Auditoria	Incluído	Incluído
Rules of Engagement	Incluídas	Incluídas
Sumário Executivo	Incluído	Incluído
Relatório Técnico de Segurança	Incluído	Incluído
Relatório de Escalabilidade	Incluído	Incluído
Finding Register	Incluído	Incluído
Plano de Ações Priorizado	Incluído	Incluído
Apresentação Executiva	Incluída	Incluída
Ciclo consolidado de comentários	Incluído	Incluído

15.2 Entregáveis adicionais da Opção B

Entregável	Estado
Threat Model formal	Incluído
Modelo inicial de capacidade	Incluído
Nota de M-Pesa Security Readiness	Incluída
Nota de Flutter Web Readiness	Incluída
Workshop técnico	Incluído
Relatório de reteste	Incluído

15.3 Conteúdo do relatório técnico de segurança

Cada finding deverá apresentar:

- identificador;
- título;
- ativo;
- domínio;
- descrição;
- evidência;
- cenário de reprodução;
- impacto;
- probabilidade;
- criticidade;
- causa raiz;
- recomendação;
- prioridade;
- dependências;
- responsável sugerido;
- referência técnica.

15.4 Conteúdo do relatório de escalabilidade

O relatório deverá apresentar:

- ambiente;
- data;
- configuração;
- carga executada;
- jornadas;
- duração;
- utilizadores virtuais;
- partidas simultâneas;
- latência;
- p50;
- p95;
- p99;
- throughput;
- taxa de erro;
- ponto de degradação;
- ponto de saturação;
- recuperação;
- gargalos;
- quotas;
- observações de custo;
- recomendações.

15.5 Revisão e finalização dos entregáveis

Cada entregável incluirá:

- uma versão preliminar;
- um ciclo consolidado de comentários;
- uma versão final.

A FTM deverá apresentar comentários consolidados no prazo de cinco dias úteis. A MANIFOLD emitirá a versão final até dois dias úteis após a receção dos comentários consolidados.

Na ausência de comentários dentro do prazo, a MANIFOLD emitirá a versão final com base na versão preliminar. Esta regra não constitui aceitação contratual automática; o mecanismo formal de aceitação será definido no SOW ou contrato.

Comentários adicionais, novos requisitos ou pedidos de reestruturação material poderão ser tratados através de Change Request.

16. A criticidade será técnica e orientada ao negócio

16.1 Escala proposta

Nível	Interpretação
Crítica	Exploração com impacto grave ou imediato sobre dados, contas, saldos, resultados, privilégios ou disponibilidade
Alta	Vulnerabilidade relevante com impacto material e exploração plausível
Média	Risco com impacto limitado, dependente de condições ou controlos compensatórios
Baixa	Fraqueza de menor impacto ou boa prática não implementada
Informativa	Observação, melhoria ou oportunidade sem vulnerabilidade confirmada

16.2 Segurança e prontidão

A conclusão poderá ser apresentada como:

- adequada no domínio avaliado;
- adequada com condições;
- inadequada até correção de bloqueadores;
- inconclusiva por limitação material.

A conclusão não equivalerá a:

- certificação;
- aprovação regulatória;
- parecer jurídico;
- validação financeira;
- garantia de ausência de vulnerabilidades;
- autorização automática para pagamentos reais.

17. Uma equipa multidisciplinar será mobilizada por fase

17.1 Estrutura da equipa

Função	Responsabilidade
Engagement Sponsor	Supervisão executiva, escalonamento e relação institucional
Engagement Manager e QA Reviewer	Gestão, âmbito, governação, revisão e qualidade
Security Lead / AppSec Specialist	Segurança de APIs, lógica de negócio, fraude e testes manuais
Firebase/GCP Security Specialist	Firestore, Storage, Cloud Functions, IAM, segredos e cloud
Performance/SRE Specialist	Carga, stress, observabilidade, capacidade e gargalos
Flutter/Mobile Security Specialist	Android, iOS, Flutter e segurança mobile

17.2 Liderança

Papel	Recurso
Engagement Sponsor	Rogerio Casimiro
Engagement Manager e QA Reviewer	Vayile Fumo
Especialistas técnicos	Recursos MANIFOLD mobilizados de acordo com a opção selecionada

Os perfis curriculares e comprovativos profissionais dos especialistas mobilizados serão disponibilizados durante o onboarding, após aprovação comercial e sob condições de confidencialidade.

17.3 Quality Assurance

Antes da emissão, os resultados serão sujeitos a:

- revisão de evidências;
- reprodução de findings materiais;
- eliminação de falsos positivos;
- revisão de criticidade;
- revisão técnica;
- revisão executiva;
- controlo de versões;
- verificação de consistência;
- validação factual com a FTM.

18. A governação reduzirá atrasos e ambiguidades

18.1 Fóruns

Fórum	Participantes	Objetivo	Cadência
Kickoff	FTM e MANIFOLD	Confirmar âmbito, acessos, regras e calendário	Uma vez
Reunião de progresso	Project Managers e especialistas	Progresso, bloqueios, riscos e decisões	Semanal
Reunião técnica	Especialistas	Acessos, arquitetura, findings e testes	Conforme necessidade
Escalonamento crítico	Sponsor e responsáveis autorizados	Vulnerabilidade crítica ou risco operacional	Imediato
Apresentação final	Gestão e equipa técnica	Resultados, prioridades e próximos passos	Encerramento
Workshop de remediação	Equipa técnica	Orientação sobre correções	Opção B

18.2 Comunicação de findings críticos

Um finding crítico validado será comunicado:

- sem aguardar o relatório final;
- por canal seguro;
- ao contacto autorizado;
- com evidência suficiente;
- com recomendação imediata de contenção.

18.3 Fonte única de verdade

A documentação oficial será mantida num repositório controlado.

Mensagens informais ou cópias locais não substituirão:

- inventário aprovado;
- plano de auditoria;
- decisões;
- findings;
- relatórios;
- aprovações;
- Change Requests.

19. O prazo principal será de 20 a 25 dias úteis

19.1 Opção A - 20 dias úteis

Período	Atividade
Dias 1-3	Mobilização, acessos, inventário e plano
Dias 4-10	Auditoria Flutter, APIs, Firebase e Cloud Functions
Dias 6-12	Cenários de fraude e desenvolvimento dos scripts
Dias 11-15	Baseline, load test e stress test
Dias 16-18	Consolidação e versão preliminar dos relatórios
Dias 19-20	QA, apresentação e encerramento

Representação executiva

Semana 1 Semana 2 Semana 3 Semana 4
Mobilização → Segurança → Stress Test → Relatórios

19.2 Opção B - 25 dias úteis

Período	Atividade
Dias 1-4	Mobilização e threat model
Dias 5-13	Auditoria de segurança aprofundada
Dias 7-15	Desenvolvimento e validação dos simuladores
Dias 13-19	Load, stress, spike e soak tests
Dias 20-22	Consolidação e versão preliminar dos relatórios
Dias 23-25	Relatórios, QA, apresentação e workshop

Representação executiva

Semana 1 Semana 2 Semana 3 Semana 4 Semana 5
Mobilização → Segurança → Escalabilidade → Readiness → Relatórios

19.3 Reteste da Opção B

O reteste ocorrerá depois da correção pela FTM, dentro de uma janela de 45 dias e em até cinco dias úteis após a disponibilização das evidências e do ambiente.

Fica limitado a um ciclo, abrangendo todos os findings originalmente classificados como Críticos e até oito Altos, sem reabertura integral da auditoria.

19.4 Período de revisão e finalização

O prazo principal da Opção A termina ao fim de 20 dias úteis, com a entrega da versão preliminar dos relatórios.

O prazo principal da Opção B termina ao fim de 25 dias úteis, com a entrega da versão preliminar dos relatórios.

Ficam fora do prazo principal:

- os cinco dias úteis de revisão da FTM;
- os até dois dias úteis para emissão da versão final;
- o tempo de implementação das correções;
- a janela de reteste;
- atrasos imputáveis à FTM, que poderão exigir reprogramação ou remobilização da equipa e cujo impacto comercial será tratado nos termos da Proposta Financeira e, quando material, por Change Request.

20. A FTM deverá disponibilizar acessos e condições mínimas

20.1 Acessos

A FTM deverá disponibilizar, conforme aplicável:

- acesso read-only a até três repositórios diretamente relacionados com a aplicação Flutter, Cloud Functions e componentes abrangidos;
- acesso Viewer a até três projetos Firebase/Google Cloud;
- acesso de leitura a IAM, regras, Cloud Functions, logs, métricas e quotas;
- uma build Android e uma build iOS da mesma release candidata ou funcionalmente equivalentes;
- contas de teste representativas de até seis perfis funcionais;
- lista de endpoints, project IDs e documentação disponível.

Repositórios adicionais, microserviços externos, componentes não inventariados ou nova build com alterações materiais poderão exigir Change Request.

20.2 Ambiente

A FTM será responsável por disponibilizar um ambiente de staging funcional, dados sintéticos, contas, segregação de dados, autorização para geração de carga, logs, métricas, quotas, alertas, contactos e kill switch.

Os testes dinâmicos e de carga serão realizados em staging.

A revisão de produção será limitada, em modo read-only, a configuração, IAM, contas de serviço, regras, logs, métricas, quotas, evidências, observabilidade e outros elementos disponibilizados pela FTM.

Continuam excluídos em produção:

- testes intrusivos, exploração e alteração de dados;
- stress test, spike test, soak test e testes de saturação;
- alterações de configuração pela MANIFOLD.

20.3 Disponibilidade da equipa técnica

A FTM deverá nomear:

- sponsor;
- ponto de contacto técnico;
- administrador Firebase/GCP;
- responsável pela aplicação Flutter;
- responsável pelas Cloud Functions;
- contacto de emergência;
- aprovador dos resultados.

Os nomes serão formalizados durante a mobilização.

21. Pressupostos de execução

21.1 Baseline contratual comum às duas opções

Componente	Opção A	Opção B
Aplicação Flutter	1	1
Plataformas	Android e iOS	Android e iOS
Builds	Até 2 no total	Até 2 no total
Repositórios	Até 3	Até 3
Projetos Firebase/GCP	Até 3	Até 3
Cloud Functions	Até 30	Até 30
APIs/endpoints	Até 40	Até 40
Perfis de utilizador	Até 6	Até 6
Fluxos críticos	Até 10	Até 15
Ambiente de testes dinâmicos	1 staging	1 staging
Produção	Read-only limitado	Read-only limitado
Utilizadores virtuais	Até 500	Até 1 000
Partidas simultâneas	Até 250	Até 500
Spike test	Não incluído	1
Soak test	Não incluído	1, até 2 horas
Ciclos de comentários	1	1

Componente	Opção A	Opção B
Reteste	Não incluído	1 ciclo; todos os Críticos e até 8 Altos

Esta tabela constitui a fonte oficial da baseline contratual. As duas builds correspondem a uma build Android e uma build iOS da mesma release candidata ou a versões funcionalmente equivalentes.

Os até três projetos Firebase/Google Cloud correspondem normalmente a desenvolvimento, staging e produção, mantendo-se a revisão de produção limitada ao modo read-only.

Até seis perfis significa até seis perfis funcionais ou níveis de acesso relevantes. Um fluxo crítico corresponde a uma jornada funcional completa; variações menores do mesmo fluxo não constituem automaticamente fluxos adicionais. Exemplos incluem autenticação, recuperação de conta, convite, matchmaking, criação de sala, partida, abandono, conclusão, atualização de saldo e consulta de histórico.

Os limites apresentados constituem a baseline contratual. Qualquer volume superior, ativo adicional, novo ambiente, nova aplicação, nova integração ou alteração material da arquitetura será avaliado através de Change Request.

Os volumes, ativos e atividades indicados constituem limites máximos de execução e não uma garantia de capacidade da plataforma. Os testes poderão ser interrompidos antes de atingir os limites contratados caso sejam observados critérios de erro, degradação, segurança, inconsistência, quota, custo ou risco operacional.

21.2 Pressupostos operacionais

A proposta pressupõe que a FTM disponibilizará, em tempo útil:

- staging funcional e suficientemente próximo de produção;
- uma build Android e uma build iOS;
- contas representativas dos perfis acordados;
- dados sintéticos, acessos, logs e métricas;
- quotas, alertas, contactos e autorização formal;
- documentação razoavelmente atualizada;
- estabilidade suficiente e ausência de alterações materiais durante os testes.

O consumo gerado no ambiente Firebase, Google Cloud ou em serviços de terceiros será controlado através de limites, alertas e critérios de paragem acordados antes da execução.

A MANIFOLD não iniciará testes de carga sem confirmação do orçamento máximo de consumo e dos responsáveis autorizados a aprovar eventual utilização adicional.

O plano de execução incluirá reserva técnica para pequenas variações, correção dos próprios scripts e repetição de procedimentos invalidados por falha diretamente imputável à MANIFOLD.

Correções, testes a terceiros, custos extraordinários e desvios materiais permanecem fora do âmbito e serão tratados por Change Request.

22. Exclusões comuns às duas opções

As duas opções excluem:

- revisão linha a linha de todo o código-fonte;
- auditoria integral de qualidade, arquitetura, manutenibilidade, maturidade ou DevSecOps;
- desenvolvimento, correção de código e implementação das recomendações;
- implementação M-Pesa, testes à API M-Pesa, transações reais, reconciliação efetiva, certificação ou parecer regulatório;
- desenvolvimento web, correção de plugins, responsividade, UX/UI web e testes cross-browser completos;
- implementação permanente de observabilidade, dashboards de produção, alertas definitivos ou tracing;
- testes intrusivos, exploração, alteração de dados ou carga em produção;
- engenharia social, phishing, testes físicos e ataques destrutivos;
- testes diretos a terceiros;
- consumo extraordinário de cloud, aumento de quotas ou infraestrutura dedicada;
- componentes ou builds alterados depois do início dos testes;

- campanhas, comentários ou retestes adicionais.

23. Âmbito consolidado da Opção A

23.1 Designação

Opção A - Security & Stress Assessment

23.2 Objetivo

Responder estritamente à prioridade comunicada pela FTM:

- auditoria de segurança;
- auditoria de escalabilidade com stress test.

23.3 Incluído

- uma aplicação Flutter para Android e iOS;
- uma build Android e uma build iOS;
- revisão de segurança orientada ao risco e por amostragem;
- até 30 Cloud Functions e 40 endpoints;
- até dez fluxos críticos e cenários prioritários de fraude;
- um shakedown test e uma baseline;
- uma campanha principal de load e stress testing;
- até 500 utilizadores virtuais e 250 partidas simultâneas;
- uma versão preliminar dos relatórios;
- um ciclo consolidado de comentários;
- uma versão final e uma apresentação executiva.

23.4 Não incluído

- revisão linha a linha de todo o código;
- threat model formal;
- spike test e soak test;
- modelo de capacidade e revisão dedicada de observabilidade;
- M-Pesa Security Readiness e Flutter Web Readiness;
- workshop técnico e reteste;
- ciclos adicionais de comentários ou campanhas adicionais;
- correções, desenvolvimento e consumo extraordinário de cloud.

23.5 Duração

20 dias úteis

23.6 Critério de conclusão

A fase principal da Opção A termina com a entrega da versão preliminar dos relatórios, após avaliação dos ativos acordados, execução dos testes aprovados e documentação das limitações e findings.

O engagement da Opção A será encerrado após o ciclo consolidado de comentários, emissão da versão final e realização da apresentação executiva.

24. Âmbito consolidado da Opção B

24.1 Designação

Opção B - Security, Scalability & Readiness Assurance

24.2 Objetivo

Executar integralmente o âmbito solicitado pela FTM e acrescentar avaliações preventivas sobre riscos próximos de evolução.

24.3 Incluído

Tudo o que está incluído na Opção A, com:

- cobertura orientada ao risco superior e threat model formal;
- até quinze fluxos críticos e cenários avançados de fraude;
- até 1 000 utilizadores virtuais e 500 partidas simultâneas;
- um spike test e um soak test de até duas horas;
- avaliação de observabilidade e modelo inicial de capacidade;
- M-Pesa Security Readiness indicativo;
- Flutter Web Readiness indicativo;
- um workshop técnico;
- um único ciclo de reteste, abrangendo todos os findings originalmente classificados como Críticos e até oito findings classificados como Altos.

24.4 Não incluído

- revisão integral de todo o código;
- implementação M-Pesa ou testes à integração real;
- desenvolvimento web, correção de plugins ou testes cross-browser completos;
- desenvolvimento de dashboards ou implementação de observabilidade;
- correção de findings;
- segundo ciclo de reteste;
- novas funcionalidades ou nova arquitetura;
- consumo extraordinário de cloud.

24.5 Duração

25 dias úteis, acrescidos da janela posterior de reteste.

24.6 Critério de conclusão

A fase principal da Opção B termina com a entrega da versão preliminar dos relatórios ao fim do prazo principal de 25 dias úteis.

A versão final será emitida depois do ciclo consolidado de comentários e será seguida da apresentação executiva e do workshop técnico.

O engagement será encerrado após conclusão do único ciclo de reteste ou expiração da respetiva janela de 45 dias.

25. As restantes auditorias poderão ser realizadas de forma faseada

A presente proposta não elimina a necessidade potencial de avaliações futuras.

A MANIFOLD recomenda que a FTM considere, de acordo com a evolução da Moola:

Fase futura 1 - Qualidade e arquitetura

- qualidade integral do código;
- manutenibilidade;
- arquitetura;
- dívida técnica;
- modularidade;
- testes automatizados.

Fase futura 2 - DevSecOps e operação

- CI/CD;
- segurança da supply chain;
- segregação de ambientes;
- releases;
- rollback;
- logging;
- alertas;
- incidentes;
- continuidade.

Fase futura 3 - Pagamentos reais

- integração M-Pesa;
- callbacks;
- reconciliação;
- idempotência;
- fraude financeira;
- carteira;
- reversões;
- segurança de credenciais;
- testes end-to-end.

Fase futura 4 - Canal web

- arquitetura web;
- Flutter Web;
- responsividade;
- browsers;
- PWA;
- autenticação;
- segurança;
- performance;
- auditoria pré-produção.

Fase futura 5 - Privacidade e conformidade

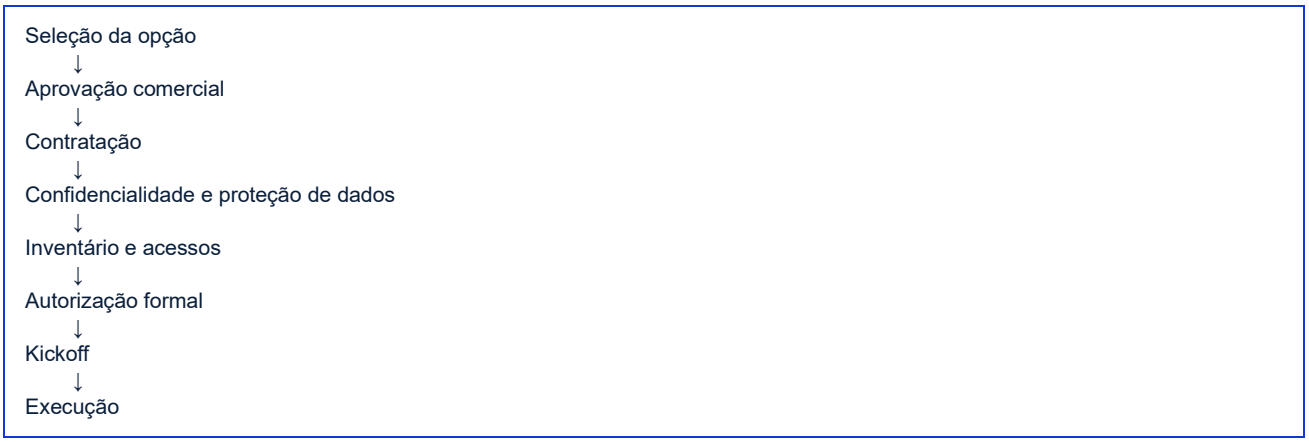
- proteção de dados;
- retenção;
- consentimento;
- direitos dos titulares;
- requisitos aplicáveis a gaming;
- operação com valores monetários;
- controlos regulatórios aplicáveis.

26. Próximos passos

Após seleção da opção e aprovação comercial, a MANIFOLD emitirá:

1. Statement of Work;
2. termos contratuais;
3. NDA e DPA, quando aplicável;
4. Rules of Engagement detalhadas;
5. autorização formal para testes;
6. checklist de acessos;
7. inventário de ativos;
8. plano de comunicação;
9. cronograma detalhado;
10. plano de testes.

Sequência de mobilização



A mobilização poderá iniciar-se após:

- aprovação da opção;
- assinatura dos instrumentos aplicáveis;
- emissão da ordem de compra, quando exigida;
- disponibilização dos acessos;
- autorização formal dos testes.

27. Conclusão

A proposta foi estruturada para permitir que a FTM escolha entre:

executar exatamente os dois serviços considerados prioritários nesta fase;

ou

executar os mesmos serviços com um nível adicional de assurance sobre evolução, capacidade, pagamentos e canal web.

A **Opção A** responde ao pedido atual da FTM sem reintroduzir auditorias que o Cliente pretende contratar posteriormente.

A **Opção B** representa a recomendação da MANIFOLD para reduzir riscos de retrabalho antes:

- do crescimento da base de utilizadores;
- da implementação de pagamentos reais;
- da expansão dos cenários de jogo;
- da disponibilização de um canal web;
- da entrada em produção em maior escala.

Em ambas as opções, a execução será independente, baseada em evidências e conduzida por especialistas, combinando revisão manual, automação controlada, testes de segurança, simulação de utilizadores e análise técnica dos resultados.

Aprovação interna MANIFOLD

Preparado por:	MANIFOLD
Revisto por:	Vayile Fumo
Aprovado por:	Rogerio Casimiro
Entidade:	Manifold, Lda
Data:	03 de agosto de 2026