Manifold

PROPOSTA EXECUTIVA E TÉCNICA

Plataforma Moola

Preparado por: Manifold, Lda

Nome institucional: MANIFOLD

Preparado para: Cliente

Referência do documento: MFD-MOOL-AUD-2026-TEC-A1

Revisão: A1

Data de emissão: 15/07/2026

Estado: Final para submissão

Classificação: Confidencial

---

1. Controlo do Documento

Revisão	Data	Descrição	Preparado por	Revisto por	Aprovado por
A1	15/07/2026	Revisão final com âmbito, pressupostos, preço e cronograma alinhados	MANIFOLD	Vayile Fumo	Rogerio Casimiro

1.1 Documentos de referência

Documento	Descrição	Estado
Pedido de proposta e esclarecimentos sobre a plataforma Moola	Informação funcional e tecnológica recebida por e-mail, incluindo Flutter, Firebase e Google Cloud.	Referência
Termos de Referência - Auditoria de Sistema	Objetivos, âmbito, resultados e benefícios esperados da auditoria.	Referência
Statement of Work da MANIFOLD	Âmbito contratual, responsabilidades, critérios de aceitação e regras de mudança.	Documento associado

2. Sumário Executivo

A MANIFOLD propõe realizar uma auditoria técnica integral, independente e orientada à decisão sobre a plataforma Moola, antes da sua entrada em produção. A avaliação combinará análise de arquitetura, revisão de código, avaliação de configurações Firebase e Google Cloud, testes de segurança controlados, análise de desempenho, revisão de DevSecOps e avaliação de maturidade operacional.

A Moola encontra-se em desenvolvimento ativo e utiliza uma aplicação móvel Flutter, Firebase Authentication, Cloud Firestore, Cloud Functions, Firebase Storage, Firebase App Check, Firebase Cloud Messaging, APIs e serviços Google Cloud. O trabalho será estruturado para identificar riscos materiais, validar a eficácia dos controlos existentes e estabelecer um plano de remediação executável.

> **Conclusão de prontidão para produção**
>
> O relatório executivo classificará a plataforma numa das seguintes posições: Pronta; Pronta com condições; Não pronta até remediação dos bloqueadores; ou Avaliação inconclusiva por limitação material de evidência. A conclusão será acompanhada por riscos residuais, condições de go-live e decisões requeridas à gestão.

2.1 Resultados que o Cliente deverá obter

- Visão independente do estado atual da plataforma e do respetivo nível de maturidade.
- Identificação de pontos fortes, vulnerabilidades, não conformidades e riscos técnicos ou operacionais.
- Classificação consistente das constatações por criticidade, impacto de negócio e probabilidade.
- Definição das correções obrigatórias antes da entrada em produção.
- Roadmap de curto, médio e longo prazo para segurança, escalabilidade, qualidade e operação.
- Base de evidência para decisões de go-live, investimento tecnológico, governação e futuras auditorias.

3. Entendimento do Projeto e do Contexto

A auditoria é solicitada num momento crítico do ciclo de vida da Moola: a solução ainda está em desenvolvimento, mas aproxima-se da sua utilização em produção. Nesta fase, decisões de arquitetura, segurança, dados, operação e processo de desenvolvimento podem afetar diretamente o risco de incidentes, a capacidade de crescimento, a experiência dos utilizadores e o custo total de operação.

Elemento	Entendimento atual
Natureza	Plataforma digital na área de gaming, com aplicação móvel e serviços de backend.
Estado	Desenvolvimento ativo; avaliação solicitada antes da entrada em produção.
Aplicação	Flutter para Android e iOS; uma build candidata a produção por plataforma.
Identidade	Firebase Authentication.
Dados	Cloud Firestore e Firebase Storage.
Backend	Cloud Functions, APIs e integrações entre frontend e backend.
Proteção de chamadas	Firebase App Check.
Mensageria	Firebase Cloud Messaging.
Infraestrutura	Firebase e Google Cloud.
Objetivo de negócio	Crescimento seguro, escalável, sustentável e operacionalmente controlado.

3.1 Pressupostos de aplicabilidade adotados

Para apresentar uma proposta fechada e competitiva, a MANIFOLD recomenda a Opção C - Auditoria Completa e Assurance, pelo preço fixo de MZN 1 280 000,00, acrescido de IVA à taxa legal. A baseline comercial e técnica adota os pressupostos abaixo. Qualquer alteração material será avaliada pelo processo de Change Request, sem afetar a cobertura dos componentes definidos no SOW:

- **A plataforma é de gaming digital sem apostas em dinheiro real, prémios monetários, carteira, levantamentos, processamento direto de cartões, KYC/AML ou certificação de RNG.**

- **O serviço destina-se a utilizadores com 18 ou mais anos; não se prevê tratamento intencional de dados de crianças nem consentimento parental.**
- **A baseline inclui uma aplicação Flutter para Android e iOS, backend Firebase/Google Cloud e APIs; não inclui portal web independente, infraestrutura on-premises ou rede corporativa.**
- **Até oito integrações externas serão avaliadas ao nível de configuração, fluxo de dados e fronteira de confiança; sistemas de terceiros não serão testados diretamente sem autorização escrita.**
- **A avaliação de performance incluirá arquitetura, consultas, índices, quotas, cold starts e testes seguros de baixo volume; testes destrutivos, stress e carga de larga escala permanecem excluídos.**
- **A operação de referência é em Moçambique. A conformidade será uma avaliação técnica de boas práticas e não um parecer jurídico, certificação formal ou validação regulatória de gaming.**

4. Objetivos da Auditoria

Domínio	Objetivo
Arquitetura	Avaliar adequação, modularidade, resiliência, dependências, fronteiras de confiança e capacidade de evolução.
Segurança	Identificar vulnerabilidades e validar controlos de confidencialidade, integridade e disponibilidade.
Código	Avaliar organização, legibilidade, manutenibilidade, tratamento de erros, segredos, dependências e testes.
Cloud	Rever configurações Firebase/GCP, IAM, contas de serviço, segredos, logging, quotas, backups e exposição.
Identidade e acesso	Avaliar autenticação, autorização, sessões, perfis, privilégios administrativos e menor privilégio.
APIs e backend	Avaliar validação, autorização, abuso de funcionalidades, rate limiting, erros e integrações.
Desempenho	Identificar gargalos, consultas ineficientes, cold starts, riscos de capacidade e oportunidades de otimização.
DevSecOps	Avaliar repositórios, branches, CI/CD, testes, dependências, releases, segregação e rollback.
Operação	Avaliar monitorização, alertas, resposta a incidentes, continuidade, backup e recuperação.
Privacidade	Avaliar controlos técnicos de minimização, retenção, acesso, eliminação e rastreabilidade de dados.
Prontidão	Emitir conclusão de go-live e plano de ações priorizado.

5. Princípios de Execução

Princípio	Aplicação
Independência	A avaliação será conduzida sem dependência do resultado comercial ou técnico pretendido pelo Cliente.
Baseada em evidências	Cada constatação material será suportada por configuração, código, log, teste, entrevista ou documento verificável.
Proporcionalidade	A profundidade dos testes será ajustada ao risco, à criticidade do ativo e às restrições de segurança.

Princípio	Aplicação
Não destrutiva	Os testes privilegiarão técnicas seguras; ações destrutivas ou de indisponibilidade ficam proibidas sem autorização específica.
Transparência	Limitações, pressupostos, amostragem, falsos positivos e incertezas serão declarados.
Orientação ao negócio	A criticidade considerará impacto técnico, impacto de negócio, probabilidade e contexto operacional.
Confidencialidade	Código, credenciais, dados e vulnerabilidades serão tratados segundo o Plano de Segurança e Privacidade.
Transferência de conhecimento	As recomendações serão discutidas com as equipas executiva e técnica.

6. Âmbito Técnico Proposto

A cobertura será executada contra a baseline quantitativa definida no SOW. A Fase 0 validará identificadores, owners e acessos dos ativos sem alterar o preço enquanto os limites contratados forem respeitados. Os workstreams são:

ID	Workstream	Cobertura
WS1	Governação, arquitetura e threat modelling	Arquitetura lógica e física; fluxos de dados; dependências; fronteiras de confiança; pontos únicos de falha; decisões arquiteturais; escalabilidade; resiliência; documentação.
WS2	Aplicação móvel Flutter	Estrutura do código; armazenamento local; segredos; sessões; tokens; comunicação; validação de certificados; deep links; permissões; logs; builds de produção; dependências; riscos de engenharia reversa.
WS3	Backend, Cloud Functions e APIs	Autenticação; autorização; validação de input; abuso de negócio; tratamento de erros; exposição de dados; rate limiting; idempotência; replay; logging; integrações externas.
WS4	Firebase e Google Cloud	Projetos e ambientes; IAM; contas de serviço; regras Firestore/Storage; App Check; segredos; quotas; funções; storage; networking aplicável; observabilidade; configuração e exposição.
WS5	Dados, privacidade e proteção do utilizador	Classificação; minimização; retenção; eliminação; acesso; encriptação; trilho de auditoria; dados pessoais; consentimento; exportação; pedidos do titular; dados em ambientes não produtivos.
WS6	Qualidade de código e engenharia	Modularidade; padrões; tratamento de exceções; dívida técnica; testes; cobertura; análise estática; dependências; licenças; documentação; manutenção.
WS7	DevSecOps e cadeia de fornecimento	Repositórios; branches; revisão; CI/CD; segregação; secrets scanning; SAST/SCA; builds; artefactos; aprovações; release; rollback; acessos de terceiros.
WS8	Desempenho, escalabilidade e custo	Consultas Firestore; índices; paginação; consumo de rede; cold starts; concorrência; quotas; capacidade; caching; limites; cenários de crescimento e riscos de custos inesperados.
WS9	Operação, observabilidade e resiliência	Logs; métricas; alertas; rastreabilidade; backups; restauro; continuidade; RTO/RPO; incidentes; on-call; runbooks; gestão de mudanças; disponibilidade.
WS10	Conformidade técnica e maturidade	Gap assessment contra boas práticas aplicáveis; avaliação de maturidade; riscos residuais; roadmap e critérios de prontidão.

6.1 Componentes condicionados à aplicabilidade

- **Portal web ou painel administrativo independente; caso seja identificado, será avaliado por Change Request ou numa amostra limitada expressamente aceite.**
- **Infraestrutura on-premises, servidores dedicados, redes privadas, VPN corporativa ou equipamentos de utilizador fora do ecossistema Firebase/Google Cloud.**
- **Serviços de pagamento, carteira, KYC/AML, apostas em dinheiro real, prémios monetários, RNG regulado ou conformidade formal de gaming.**
- **Testes de carga de larga escala, parecer jurídico, auditoria regulatória, certificação ISO, PCI DSS ou avaliação formal de licenciamento.**
- **Testes intrusivos a sistemas de terceiros; integrações permanecem avaliadas na fronteira e configuração sob controlo do Cliente.**

7. Metodologia e Fases

Fase	Designação	Principais atividades	Saída
0	Mobilização e confirmação do âmbito	Kickoff; inventário; stakeholders; acessos; ambiente; regras de execução; baseline; plano detalhado.	Memorando de Confirmação do Âmbito e Plano de Auditoria.
1	Descoberta, arquitetura e risco	Entrevistas; análise documental; diagramas; fluxos; threat modelling; criticidade de ativos; riscos preliminares.	Mapa de arquitetura validado e registo inicial de riscos.
2	Revisão técnica e de configurações	Código Flutter; Cloud Functions; APIs; Firebase; GCP; IAM; regras; dados; CI/CD; dependências.	Evidências de revisão e constatações preliminares.
3	Testes de segurança controlados	Testes autenticados e não autenticados; autorização; abuso; regras Firestore/Storage; sessão; APIs; mobile.	Registo validado de vulnerabilidades e provas de conceito seguras.
4	Desempenho, escalabilidade e operação	Consultas; índices; limites; custos; observabilidade; backups; recuperação; incidentes; release e rollback.	Avaliação de capacidade, resiliência e operação.
5	Maturidade, consolidação e priorização	Classificação; causa raiz; impacto; risco residual; maturidade; dependências; plano de ações.	Relatórios preliminares e roadmap.
6	Validação, apresentação e encerramento	Fact-check; comentários; apresentação executiva; workshop técnico; versão final; fecho de acessos.	Relatório final e termo de encerramento.
7	Reteste incluído	Validação de até 12 correções críticas e altas dentro da janela de 60 dias.	Relatório de reteste e atualização do risco residual.

7.1 Técnicas de avaliação

- Entrevistas estruturadas e walkthroughs técnicos.
- Revisão documental, de configuração e de evidências operacionais.
- Revisão manual e automatizada de código e dependências, com validação humana.
- Análise de regras de segurança Firestore e Storage e simulação de perfis de acesso.
- Testes manuais de APIs, fluxos de autenticação, autorização e lógica de negócio.
- Análise da aplicação móvel em builds autorizados e revisão de configurações de release.
- Modelação de ameaças e análise de cenários de abuso.
- Análise de performance e escalabilidade baseada em dados disponíveis, perfis de uso e testes autorizados.

- Revisão de logs, alertas, backups, runbooks, incidentes e evidências de recuperação.

8. Referenciais de Avaliação

Serão utilizados, conforme aplicabilidade e nas versões vigentes à data da execução, os seguintes referenciais:

Área	Referenciais
Segurança mobile	OWASP Mobile Application Security; práticas oficiais Android, iOS e Flutter.
Segurança de aplicações	OWASP Application Security Verification Standard e práticas de secure coding.
APIs	OWASP API Security e princípios de autenticação, autorização e proteção contra abuso.
Cloud e Firebase	Boas práticas oficiais Firebase e Google Cloud; CIS Benchmarks aplicáveis.
Gestão de risco	NIST Cybersecurity Framework e princípios de gestão de risco tecnológico.
Sistemas de gestão	ISO/IEC 27001 e ISO/IEC 27002, como referências de controlos e maturidade, sem implicar certificação.
Privacidade	Privacy by design, minimização, necessidade, retenção, rastreabilidade e requisitos legais aplicáveis.
Desenvolvimento seguro	Secure SDLC, least privilege, defence in depth, zero trust e gestão segura da cadeia de fornecimento.

> **Limite de conformidade**
>
> A avaliação técnica de conformidade ou gap assessment não constitui parecer jurídico, auditoria regulatória formal nem certificação. Qualquer conclusão legal ou certificação dependerá de contratação específica e de entidade competente.

9. Classificação de Risco e Criticidade

A criticidade final resultará da combinação de impacto, probabilidade, explorabilidade, exposição, sensibilidade dos dados, alcance do ativo e relevância para o negócio. O CVSS poderá ser utilizado como informação técnica auxiliar, sem substituir a análise contextual.

Nível	Interpretação	Tratamento esperado
Crítica	Compromisso material, exploração provável ou impacto severo; pode impedir o go-live.	Ação imediata e validação executiva.
Alta	Impacto significativo ou exposição relevante; correção normalmente requerida antes da produção.	Plano e owner definidos; reteste recomendado.
Média	Risco moderado, controlos incompletos ou exposição condicionada.	Correção de curto prazo e monitorização.
Baixa	Impacto limitado, hardening ou melhoria de controlo.	Tratar no ciclo normal de melhoria.
Informativa	Observação, oportunidade ou boa prática sem risco material direto.	Considerar no roadmap.

9.1 Critérios de go-live

Situação	Interpretação
Pronta	Não foram identificados bloqueadores materiais; riscos residuais encontram-se dentro da tolerância formalmente aceite.

Situação	Interpretação
Pronta com condições	A produção pode avançar após cumprimento de condições objetivas e verificáveis definidas no relatório.
Não pronta	Existem vulnerabilidades críticas, riscos altos não mitigados ou lacunas operacionais que tornam o go-live desaconselhável.
Inconclusiva	Limitações materiais de acesso, evidência, ambiente ou cobertura impedem uma conclusão responsável.

10. Modelo de Maturidade

Nível	Descrição
1 - Inicial	Controlos inexistentes, informais, reativos ou dependentes de pessoas.
2 - Básico	Práticas parcialmente implementadas, com consistência limitada.
3 - Definido	Processos documentados, atribuídos e aplicados de forma consistente.
4 - Gerido	Controlos medidos, monitorizados, testados e sujeitos a governação.
5 - Otimizado	Automação, melhoria contínua, métricas preditivas e integração sistemática no negócio.

A maturidade será avaliada, no mínimo, para arquitetura, segurança, engenharia, cloud, identidade, dados, DevSecOps, testes, observabilidade, continuidade e governação.

11. Entregáveis

ID	Entregável	Conteúdo
D1	Plano de Auditoria e Memorando de Confirmação do Âmbito	Ativos, métodos, calendário, acessos, limitações, regras e baseline.
D2	Relatório Executivo	Prontidão, maturidade, riscos principais, pontos fortes, bloqueadores e decisões.
D3	Relatório Técnico Detalhado	Constatações, evidências, impacto, causa raiz, recomendações e referências.
D4	Registo Consolidado de Constatações	Finding ID, ativo, criticidade, owner, esforço, prioridade, estado e dependências.
D5	Matriz de Maturidade	Pontuação, racional, evidências e target state por domínio.
D6	Mapa de Riscos	Riscos técnicos, operacionais, de segurança e privacidade, com resposta proposta.
D7	Roadmap de Remediação	Ações pré-go-live, curto prazo, médio prazo, dependências, responsáveis e sequência.
D8	Apresentação Executiva	Síntese para gestão e decisões requeridas.
D9	Workshop Técnico	Discussão de causa raiz, prioridades, remediação e dúvidas.
D10	Relatório de Reteste	Estado de até 12 correções críticas e altas abrangidas pelo reteste incluído.

11.1 Conteúdo mínimo de cada constatação

- Identificador, título, domínio, ativo e ambiente afetados.
- Descrição, evidência, pré-condições e cenário de exploração ou falha.
- Impacto técnico, impacto de negócio, probabilidade e criticidade.

- Causa raiz, recomendação, prioridade, esforço estimado e dependências.
- **Referências de boas práticas e estado após o reteste incluído.**

12. Plano de Trabalho e Marcos

A execução principal terá duração de 30 dias úteis a partir de T0. O relatório preliminar será emitido até ao 23.º dia útil, o fact-check será concluído em cinco dias úteis e a versão final, apresentação executiva e workshop técnico serão concluídos até ao 30.º dia útil. O reteste incluído será executado em até cinco dias úteis após a disponibilização das correções, dentro de uma janela de 60 dias após o relatório final.

Gate	Critério
G0	Contrato, NDA, DPA e autorização para testes assinados.
G1	Inventário, acessos, ambientes, limitações e regras de execução aprovados.
G2	Arquitetura, fluxos críticos e threat model validados.
G3	Revisões e testes técnicos concluídos; vulnerabilidades críticas comunicadas.
G4	Constatações preliminares submetidas a fact-check.
G5	Relatórios preliminares e roadmap apresentados.
G6	Relatórios finais e sessões de encerramento concluídos.
G7	Reteste incluído e encerramento administrativo.

13. Governação e Comunicação

Papel	Responsabilidade principal
Sponsor Executivo do Cliente	Patrocínio, decisões, aceitação de risco e escalonamentos materiais.
Gestor do Projeto do Cliente	Coordenação de acessos, stakeholders, evidências, comentários e aprovações.
Engagement Partner MANIFOLD	Accountability executiva, independência, qualidade e escalonamento.
Diretor/Gestor de Projeto MANIFOLD	Planeamento, coordenação, reporte, riscos, dependências e entregáveis.
Líder Técnico de Auditoria	Coordenação técnica, coerência das constatações e integração dos workstreams.
Quality Reviewer	Revisão independente da evidência, criticidade, redação e conclusões.

- Kickoff formal e confirmação de canais seguros.
- Reuniões semanais de progresso e relatório de estado.
- Canal de emergência para vulnerabilidades críticas e incidentes.
- Steering Committee em marcos relevantes ou sempre que exista decisão material.
- Registo de decisões, RAID log, change requests e aprovações formais.

14. Garantia de Qualidade

A qualidade será assegurada por um processo de revisão independente e rastreável:

- Princípio de quatro olhos para constatações críticas e altas.
- Reprodução ou validação independente das vulnerabilidades materiais.
- Eliminação de falsos positivos e distinção entre observação, risco e não conformidade.

- Revisão de consistência entre evidência, impacto, criticidade e recomendação.
- Fact-check com o Cliente sem transferência da responsabilidade pela conclusão.
- Revisão editorial, executiva e técnica antes da emissão final.
- Rastreabilidade entre âmbito, procedimentos executados, evidências e entregáveis.

15. Responsabilidades do Cliente

- Nomear sponsor, gestor de projeto, responsáveis técnicos e contactos de emergência.
- Confirmar que possui autoridade para autorizar os testes e obter consentimento de terceiros.
- Disponibilizar código-fonte, builds, documentação, diagramas, contas de teste, logs e acessos de leitura.
- Manter backups e monitorização adequados antes de qualquer teste em ambiente sensível.
- Fornecer informação completa e consolidar comentários dentro dos prazos acordados.
- Comunicar alterações materiais durante a auditoria.
- Implementar correções e aceitar formalmente quaisquer riscos residuais.

16. Pressupostos, Dependências e Limitações

Tema	Condição
Ambiente	Será privilegiado ambiente controlado e representativo; produção exige autorização específica.
Acessos	Atrasos ou restrições de acesso podem reduzir cobertura ou afetar o calendário.
Amostragem	A auditoria pode utilizar amostragem baseada em risco; não representa garantia de ausência de falhas.
Mudanças	Alterações posteriores à data de corte podem exigir nova validação.
Terceiros	Sistemas de terceiros só serão testados com autorização adequada.
Testes destrutivos	Negação de serviço, destruição de dados, engenharia social e testes físicos estão excluídos salvo contratação expressa.
Legal e certificação	Não inclui parecer jurídico, certificação formal ou auditoria regulatória, salvo acordo específico.
Remediação	A implementação das correções não está incluída, salvo opção comercial própria.

17. Valor para o Cliente

- Redução do risco de lançar vulnerabilidades ou fragilidades operacionais em produção.
- Priorização objetiva do investimento, evitando correções dispersas ou sem contexto de negócio.
- Melhoria da segurança, qualidade, desempenho, resiliência e previsibilidade de custos.
- Maior confiança da gestão, utilizadores, parceiros e potenciais investidores.
- Base estruturada para futuras certificações, auditorias, due diligence ou expansão regulatória.
- Fortalecimento dos processos de engenharia e da capacidade interna de melhoria contínua.

18. Próximos Passos

1. Validar o âmbito quantitativo e os componentes aplicáveis.
2. **Formalizar a Opção C, o calendário, a equipa e a janela de reteste definidos no pacote.**
3. Concluir a due diligence de ambas as partes e assinar o pacote contratual.
4. Executar a Fase 0, aprovar as Regras de Execução e iniciar a auditoria.

Pela Manifold, Lda

Nome: Rogerio Casimiro

Função: Representante Autorizado

Assinatura: _____

Data: na data da assinatura

Pelo Cliente

Nome: Cliente

Função: Representante Autorizado

Assinatura: _____

Data: na data da assinatura