Manifold

STATEMENT OF WORK (SOW)

Plataforma Moola

Preparado por:	Manifold, Lda
Nome institucional:	MANIFOLD
Preparado para:	Cliente
Referência do documento:	MFD-MOOL-AUD-2026-SOW-A1
Revisão:	A1
Data de emissão:	15/07/2026
Estado:	Final para validação contratual
Classificação:	Confidencial

---

1. Controlo do Documento

Revisão	Data	Descrição	Preparado por	Revisto por	Aprovado por
A1	15/07/2026	Revisão final do âmbito contratual, baseline, cronograma e reteste	MANIFOLD	Vayile Fumo	Rogerio Casimiro

1.1 Documentos de referência

Documento	Descrição	Estado
Proposta Executiva e Técnica da MANIFOLD	Abordagem, metodologia, workstreams, referenciais e entregáveis.	Documento associado
Proposta Comercial da MANIFOLD	Preços, pagamento, opções e pressupostos financeiros.	Documento associado
Termos de Referência - Auditoria de Sistema	Requisitos do Cliente para objetivos, âmbito e resultados.	Referência
Plano de Segurança, Privacidade e RoE	Controlos de informação e regras dos testes.	Documento vinculativo
Pacote Contratual	Termos gerais, NDA, DPA e autorização formal.	Documento vinculativo

2. Partes e Finalidade

O presente Statement of Work (“SOW”) estabelece o âmbito, as responsabilidades, os entregáveis, os critérios de aceitação e as condições de execução da auditoria técnica integral da plataforma Moola entre Manifold, Lda, adiante designada “MANIFOLD”, e Cliente, adiante designado “Cliente”.

Este SOW deverá ser lido em conjunto com o contrato-quadro ou termos gerais, a proposta técnica, a proposta comercial, o acordo de confidencialidade, o aditamento de proteção de dados e as Regras de Execução. O preço fixo da Opção C é MZN 1 280 000,00, acrescido de IVA à taxa legal. Em caso de conflito, prevalecerá a ordem de precedência definida no pacote contratual.

Todos os valores indicados na presente proposta e nos documentos contratuais correspondentes são apresentados sem IVA, ao qual acrescerá o imposto à taxa legal em vigor.

2.1 Objetivo contratual

Avaliar, de forma independente e baseada em evidências, a prontidão da Moola para produção, cobrindo segurança, arquitetura, qualidade de código, cloud, dados, APIs, desempenho, escalabilidade, DevSecOps, observabilidade, resiliência, maturidade e conformidade técnica, e produzir um plano de remediação priorizado.

3. Baseline e Inventário do Âmbito

> **Condição de início**
>
> O âmbito definitivo será congelado após a Fase 0. Qualquer diferença material entre os pressupostos abaixo e o inventário real deverá ser tratada por clarificação formal ou Change Request.

Componente	Baseline quantitativa	Observação
Aplicações Flutter	1 aplicação Flutter; Android e iOS; até 2 builds candidatas	Inclui código, configuração e builds autorizados.
Repositórios de código	Até 3 repositórios e 150 000 linhas lógicas de código	Aplicação, backend, infraestrutura e automação.
Cloud Functions	Até 30 Cloud Functions	Funções ativas, triggers e dependências.
APIs/endpoints	Até 40 endpoints de API	Internos, externos, administrativos e callbacks.
Projetos Firebase/GCP	Até 3 projetos Firebase/GCP	Desenvolvimento, teste, staging e produção.
Ambientes	3 ambientes: desenvolvimento, staging e produção	Separação, dados, acessos e configuração.
Collections Firestore	Até 25 collections; 15 consideradas críticas	Estrutura, regras, índices, retenção e consultas.
Buckets de Storage	Até 3 buckets de Storage	Regras, exposição, upload e retenção.
Contas de serviço	Até 12 contas de serviço	IAM, chaves, rotação e privilégios.
Integrações externas	Até 8 integrações externas	Pagamentos, analytics, notificações e outros terceiros.
Perfis de utilizador	Até 6 perfis de utilizador e administração	Utilizador, moderador, operador, administrador e outros.
Fluxos críticos de negócio	Até 10 fluxos críticos de negócio	Registo, login, jogo, prémio, pagamento e suporte, conforme aplicável.
Volume esperado	Cenário: 100 000 registados; 20 000 MAU; pico 1 000 sessões; 5 milhões de operações/mês	Base para análise de capacidade e custos.
Reteste	1 ciclo; até 12 findings Críticos/Altos	Normalmente limitado a findings críticos e altos.

4. Serviços Incluídos

Área	Atividades incluídas
Mobilização	Kickoff; stakeholders; plano; acessos; inventário; baseline; comunicação; regras de execução.
Arquitetura	Diagramas; fluxos; fronteiras de confiança; resiliência; escalabilidade; dependências; threat modelling.
Mobile Flutter	Revisão de código e configuração; armazenamento; sessão; tokens; comunicação; permissões; release; dependências.
Backend e APIs	Cloud Functions; endpoints; autenticação; autorização; input; erros; abuso; rate limiting; integrações.
Firebase/GCP	IAM; contas de serviço; regras Firestore/Storage; App Check; segredos; logs; quotas; exposição; ambientes.
Dados e privacidade	Classificação; minimização; retenção; eliminação; trilhos; dados pessoais; acessos e ambientes não produtivos.
Qualidade e testes	Estrutura; dívida técnica; exceções; dependências; licenças; testes manuais e automatizados; documentação.
DevSecOps	Repositórios; branches; revisão; CI/CD; SAST/SCA; secrets; artefactos; aprovações; releases e rollback.
Performance	Consultas; índices; paginação; cold starts; concorrência; caching; capacidade; quotas e custo.
Operação	Logs; métricas; alertas; incidentes; backups; restauro; continuidade; RTO/RPO; runbooks e on-call.
Relatórios	Constatações; maturidade; riscos; roadmap; apresentação executiva; workshop técnico.
Reteste	Incluído: validação de até 12 findings críticos e altos, num ciclo, dentro da janela contratual.

4.1 Profundidade e amostragem

A revisão será orientada ao risco. Componentes críticos e fluxos de elevada exposição receberão maior profundidade. A expressão "auditoria completa" significa cobertura de todos os domínios acordados, não uma revisão exaustiva de cada linha de código, configuração ou transação, salvo se tal profundidade for expressamente quantificada no inventário e no preço.

5. Serviços Excluídos

- Ataques de negação de serviço, stress destrutivo, flooding ou indisponibilidade intencional.
- Eliminação, corrupção ou alteração intencional de dados; exploração persistente; exfiltração não necessária.
- Engenharia social, phishing, testes físicos, red team de longa duração ou análise de pessoas.
- Testes sobre sistemas de terceiros sem autorização formal do respetivo proprietário.
- Testes de carga em produção, salvo plano específico, monitorização ativa e autorização adicional.
- Parecer jurídico, certificação ISO, PCI DSS, auditoria financeira, validação de licenças de gaming ou avaliação formal de RNG.
- Implementação de correções, refactoring, migração cloud ou operação continuada, salvo contratação adicional.
- Garantia de ausência de vulnerabilidades ou cobertura de alterações realizadas após a data de corte.

6. Fases e Atividades

Fase	Designação	Atividades	Marco
F0	Mobilização e baseline	Kickoff; documentação; inventário; acessos; regras; calendário; riscos iniciais.	Plano de Auditoria aprovado.
F1	Descoberta e arquitetura	Entrevistas; diagramas; fluxos; criticidade; threat model; riscos.	Arquitetura e risco validados.
F2	Revisão técnica	Código, Firebase/GCP, APIs, dados, CI/CD, configuração e operação.	Evidências e findings preliminares.
F3	Testes controlados	Mobile, APIs, autorização, regras Firebase, sessões e abuso de negócio.	Vulnerabilidades validadas.
F4	Performance e resiliência	Consultas, capacidade, quotas, custos, observabilidade, backup e incidentes.	Avaliação operacional.
F5	Consolidação	Criticidade, maturidade, causa raiz, recomendações e roadmap.	Relatório preliminar.
F6	Validação e fecho	Fact-check, apresentação, workshop, relatório final e revogação de acessos.	Entregáveis aceites.
F7	Reteste incluído	Validação das correções, evidência e atualização do risco residual.	Relatório de reteste.

7. Entregáveis e Critérios de Aceitação

Entregável	Formato	Conteúdo	Aceitação
Plano de Auditoria	DOCX/PDF	Âmbito, ativos, métodos, acessos, calendário, RoE e limitações.	Aprovação do gestor do Cliente.
Relatório Executivo	DOCX/PDF	Prontidão, maturidade, riscos, pontos fortes, bloqueadores e decisões.	Coerência com o relatório técnico.
Relatório Técnico	DOCX/PDF	Findings, evidências, impacto, causa raiz, recomendações e referências.	Cobertura dos domínios acordados.
Registo de Findings	XLSX/CSV	ID, ativo, criticidade, owner, prazo, esforço, estado e dependências.	Consistência com relatórios.

Entregável	Formato	Conteúdo	Aceitação
Matriz de Maturidade	XLSX/PDF	Nível atual, target, evidências e lacunas por domínio.	Racional documentado.
Mapa de Riscos	XLSX/PDF	Risco, causa, impacto, resposta, owner e risco residual.	Rastreabilidade com findings.
Roadmap	XLSX/PDF	Pré-go-live, curto, médio e longo prazo; dependências e prioridades.	Ações executáveis e priorizadas.
Apresentação Executiva	PPTX/PDF	Síntese e decisões.	Sessão realizada.
Workshop Técnico	Sessão/ata	Discussão detalhada e esclarecimentos.	Ata ou registo de conclusão.
Relatório de Reteste	DOCX/PDF	Estado das correções abrangidas.	Evidência de validação.

7.1 Processo de revisão e aceitação

1. A MANIFOLD submete a versão preliminar pelo canal seguro acordado.
2. **O Cliente consolida comentários num único ciclo de fact-check dentro de cinco dias úteis após cada entrega material.**
3. A MANIFOLD trata correções factuais e esclarecimentos dentro do âmbito; pedidos novos são avaliados como mudança.
4. A versão final é emitida e submetida à aprovação dos responsáveis definidos.
5. A ausência de comentários dentro do prazo não implica aceitação automática, salvo disposição contratual expressa.

8. Cronograma e Dependências

A auditoria principal terá duração de 30 dias úteis a partir de T0. T0 corresponde à data em que o contrato, a ordem de compra, o pagamento de mobilização, as autorizações, os acessos e a informação mínima estiverem disponíveis. O reteste incluído será executado em até cinco dias úteis, dentro de uma janela de 60 dias de calendário após a emissão do relatório final.

Marco temporal	Resultado
T0	Condições de início satisfeitas e kickoff realizado.
T0 + 3 dias úteis	Fase 0 concluída, inventário e baseline aprovados.
T0 + 20 dias úteis	Revisões técnicas e testes controlados concluídos.
T0 + 23 dias úteis	Relatório preliminar emitido e fact-check iniciado.
T0 + 30 dias úteis	Relatório final, apresentação executiva e workshop concluídos.
Até 5 dias úteis após correções	Reteste incluído, dentro de 60 dias após o relatório final.

Atrasos na disponibilização de acessos, documentação, contas de teste, decisões ou ambientes deslocam proporcionalmente o calendário e podem exigir replaneamento.

9. Responsabilidades da MANIFOLD

- Executar os serviços com diligência profissional, independência, confidencialidade e competência adequada.
- Manter plano, registos de evidência, RAID log, decisões, mudanças e controlo de qualidade.
- Utilizar técnicas proporcionais e respeitar integralmente as Regras de Execução.
- Comunicar de imediato vulnerabilidades críticas validadas e qualquer incidente associado aos trabalhos.
- Proteger, restringir, reter e eliminar informação nos termos acordados.

- Entregar os produtos contratados e prestar esclarecimentos durante os ciclos previstos.

10. Responsabilidades do Cliente

Tema	Responsabilidade
Autoridade	Confirmar propriedade ou autorização sobre todos os ativos e terceiros.
Stakeholders	Nomear sponsor, gestor, responsáveis técnicos, segurança, privacidade e emergência.
Acessos	Fornecer acessos de leitura, código, builds, contas, logs, diagramas e documentação.
Ambientes	Disponibilizar ambiente controlado, dados de teste, backups e monitorização.
Informação	Responder a pedidos de informação de forma completa e dentro dos prazos.
Mudanças	Notificar alterações materiais e congelar, quando possível, a baseline durante a avaliação.
Comentários	Consolidar fact-check, aprovações e decisões.
Remediação	Implementar correções e formalizar aceitação de riscos residuais.

11. Acessos, Evidências e Segurança

- Acessos nominativos, temporários, com MFA e menor privilégio.
- Proibição de credenciais partilhadas ou envio por canais não aprovados.
- Registo de concessão, utilização e revogação de acessos.
- Evidências armazenadas em repositório segregado, encriptado e restrito.
- Dados pessoais e segredos minimizados nas evidências sempre que possível.
- Nenhum código, log ou credencial será submetido a IA pública ou SaaS não autorizado.
- Retenção e destruição conforme o Plano de Segurança, Privacidade e RoE.

12. Regras de Teste e Produção

Tema	Regra
Autorização	Nenhum teste intrusivo antes da autorização formal e aprovação dos ativos.
Produção	Apenas técnicas não destrutivas, janelas aprovadas e contacto de emergência disponível.
Proibido	DoS, flooding, destruição de dados, persistência, engenharia social e exploração de terceiros não autorizados.
Paragem	Interrupção imediata em caso de degradação, risco inesperado, incidente ou instrução do Cliente.
Críticas	Comunicação imediata por canal seguro, sem aguardar o relatório final.
Registos	O Cliente deverá preservar logs e monitorizar os testes nos períodos acordados.

13. Gestão de Riscos, Issues e Decisões

Será mantido um RAID log com riscos, pressupostos, issues e dependências. Cada item terá owner, prazo, resposta e estado. Decisões materiais serão registadas no Decision Log e escaladas segundo a matriz de governação.

14. Controlo de Mudanças

Etapa	Regra
Gatilhos	Aumento de ativos, repositórios, endpoints, ambientes, integrações, profundidade, testes, entregáveis ou ciclos.
Pedido	Descrição da mudança, motivo, impacto, prioridade e data requerida.

Etapa	Regra
Avaliação	Impacto em preço, esforço, calendário, risco, equipa e dependências.
Aprovação	Assinatura ou aprovação formal por representantes autorizados de ambas as partes.
Execução	Nenhuma mudança material é executada antes da aprovação.

15. Reteste

O reteste abrangerá apenas as constatações, ativos e ambientes expressamente identificados na proposta comercial. O Cliente deverá fornecer evidências das correções, descrição das mudanças e acesso ao ambiente estável. Alterações de arquitetura ou novos componentes podem exigir avaliação adicional.

- **Janela de reteste: 60 dias de calendário após a emissão do relatório final.**
- **Número de ciclos incluídos: um ciclo, executado em até cinco dias úteis após a disponibilização das correções.**
- **Severidades incluídas: até 12 findings classificados como Críticos ou Altos.**
- Resultado por finding: Corrigido; Parcialmente corrigido; Não corrigido; Não retestado; Risco aceite.

16. Critérios de Conclusão e Encerramento

- Ativos acordados avaliados ou limitações formalmente registadas.
- Findings validados e submetidos a fact-check.
- Entregáveis finais emitidos e sessões concluídas.
- Acessos temporários revogados.
- Evidências devolvidas ou destruídas conforme a política acordada.
- **Riscos residuais e itens em aberto transferidos formalmente ao Cliente.**
- Termo de encerramento e, quando aplicável, certificado de destruição emitidos.

17. Pressupostos Contratuais

Tema	Pressuposto
Informação	A MANIFOLD poderá confiar na informação fornecida, sem auditoria de autenticidade, salvo inconsistências aparentes.
Disponibilidade	Stakeholders e sistemas estarão disponíveis nas janelas acordadas.
Qualidade de ambiente	O ambiente de teste será suficientemente representativo.
Limitações	A auditoria é temporal, baseada em evidências e não garante inexistência de falhas.
Risco de negócio	A decisão de go-live e a aceitação de risco pertencem ao Cliente.
Propriedade	O Cliente mantém propriedade sobre os seus sistemas, dados e código.
Metodologia	A MANIFOLD mantém propriedade sobre metodologias e ferramentas preexistentes.

18. Aprovação do SOW

A assinatura abaixo confirma que as partes compreenderam e aceitaram o âmbito, as responsabilidades, os critérios de aceitação, as limitações e o processo de mudança definidos neste SOW.

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