Manifold

MATRIZ DE CONFORMIDADE COM OS TOR

Plataforma Moola

Preparado por: Manifold, Lda

Nome institucional: MANIFOLD

Preparado para: Cliente

Referência do documento: MFD-MOOL-AUD-2026-CMP-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 da matriz de conformidade com os TOR	MANIFOLD	Vayile Fumo	Rogerio Casimiro

1.1 Documentos de referência

Documento	Descrição	Estado
Termos de Referência - Auditoria de Sistema	Documento de objetivos, âmbito, resultados e benefícios esperados.	Fonte principal
Esclarecimentos sobre a plataforma Moola	Tecnologias, contexto de pré-produção e preocupações prioritárias.	Fonte complementar
Proposta Executiva e Técnica	Resposta metodológica da MANIFOLD.	Documento associado
Statement of Work	Âmbito contratual e critérios de aceitação.	Documento associado

2. Finalidade e Critérios de Resposta

A presente matriz responde, requisito a requisito, aos Termos de Referência e aos esclarecimentos recebidos. A matriz deve ser lida em conjunto com a Proposta Executiva e Técnica e o Statement of Work; estes documentos definem a profundidade, os limites e os pressupostos aplicáveis.

Estado	Definição
Cumpre	O requisito está incluído na solução proposta e nos entregáveis.
Cumpre quando aplicável	O requisito será coberto se o componente existir e estiver sob autoridade do Cliente.

Estado	Definição
Cobertura por pressuposto	O requisito foi fechado por pressuposto técnico e limite quantitativo explícito no SOW; desvio material segue Change Request.
Cumpre parcialmente	A resposta cobre a componente técnica, mas não certificação, parecer legal ou atividade não contratada.
Não aplicável	O componente não integra a arquitetura confirmada.
Opção adicional	Pode ser contratado separadamente.

3. Matriz de Conformidade Detalhada

Ref.	Requisito TOR	Resposta MANIFOLD	Estado	Entregável/Evidência	Clarificação
1.1	Auditoria por entidade independente e especializada.	A MANIFOLD propõe uma equipa independente, com revisão de qualidade separada da execução e declaração de conflitos de interesse.	Cumpre	Proposta Técnica; Declaração de Independência	Equipa definida no Documento 05; Rogerio Casimiro aprova e Vayile Fumo revê.
1.2	Avaliação técnica imparcial do estado atual.	Metodologia baseada em evidências, fact-check e critérios de risco definidos.	Cumpre	Relatórios Executivo e Técnico	A decisão de go-live permanece do Cliente.
2.1	Auditoria técnica completa ao sistema.	Cobertura de todos os domínios acordados, com profundidade orientada ao risco e baseline quantitativa no SOW.	Cumpre	Plano de Auditoria; Relatório Técnico	"Completa" não significa revisão exaustiva de cada linha sem quantificação.
2.2	Avaliar maturidade, qualidade, segurança, desempenho e conformidade.	Modelo de maturidade 1-5 e workstreams específicos para cada dimensão.	Cumpre	Matriz de Maturidade; Relatórios	Conformidade técnica, não certificação formal.
3.1	Avaliar arquitetura e crescimento	Threat modelling, fluxos, dependências, resiliência, escalabilidade, limites e decisões arquiteturais.	Cumpre	Relatório Técnico; Roadmap	
3.2	Identificar vulnerabilidades e riscos CIA	Revisão de código/configuração e testes controlados de mobile, APIs, Firebase e cloud.	Cumpre	Finding Register; Mapa de Riscos	Testes intrusivos dependem de autorização.
3.3	Avaliar qualidade do código-fonte	Organização, legibilidade, modularidade, erros, dependências, testes, documentação e dívida técnica.	Cumpre	Relatório Técnico	Profundidade depende da dimensão dos repositórios.
3.4	Verificar eficiência da infraestrutura e ambientes	Projetos, segregação, IAM, quotas, configuração, segredos, observabilidade, custos e exposição.	Cumpre	Relatório Técnico	Limitado a Firebase/GCP e outros ativos autorizados.
3.5	Avaliar desempenho e gargalos	Consultas, índices, paginação, cold starts, concorrência, rede, capacidade e limites.	Cumpre	Avaliação de Performance	Testes de carga especializados podem ser opção.
3.6	Analisar desenvolvimento, testes, CI e CD	Repositórios, branches, revisão, SAST/SCA, pipelines, artefactos, releases e rollback.	Cumpre	Avaliação DevSecOps	Acesso aos pipelines e repositórios requerido.
3.7	Avaliar utilizadores, permissões, autenticação e acessos	Firebase Auth, sessões, perfis, claims, IAM, contas de serviço e menor privilégio.	Cumpre	Relatório Técnico	Perfis e matriz de acessos a fornecer.
3.8	Verificar logs, monitorização e recuperação	Cobertura, qualidade, retenção, alertas, backups, restauro, RTO/RPO e runbooks.	Cumpre	Avaliação Operacional	Evidências de testes de restauro requeridas.
3.9	Confirmar conformidade com normas e requisitos legais	Gap assessment técnico contra referenciais e requisitos fornecidos.	Cumpre parcialmente	Matriz de Conformidade	Não inclui parecer jurídico ou certificação.
3.10	Identificar riscos técnicos, operacionais e de segurança	RAID, finding register, mapa de riscos e risco residual.	Cumpre	Mapa de Riscos	
3.11	Recomendações para melhoria contínua	Recomendações, target state, dependências, esforço e roadmap priorizado.	Cumpre	Roadmap de Remediação	
4.1	Arquitetura da solução	Arquitetura lógica/física, fluxos, fronteiras de confiança, integrações, resiliência e capacidade.	Cumpre	Relatório Técnico	

Ref.	Requisito TOR	Resposta MANIFOLD	Estado	Entregável/Evidência	Clarificação
4.2	Aplicações Web	Não existe aplicação web independente na baseline; APIs administrativas e backend permanecem abrangidos.	Não aplicável	SOW; Registo de Baseline	Qualquer futuro portal independente será tratado por Change Request.
4.3	Aplicações Mobile	Flutter, builds, armazenamento, sessão, comunicação, permissões e hardening.	Cumpre	Relatório Mobile	Uma aplicação Flutter para Android e iOS, com uma build candidata por plataforma.
4.4	APIs e serviços	Autenticação, autorização, input, abuso, erros, rate limiting, exposição e integrações.	Cumpre	Relatório API/Backend	Inventário de endpoints requerido.
4.5	Bases de dados	Cloud Firestore, modelo, regras, índices, consultas, retenção e acesso.	Cumpre	Relatório de Dados	Cloud Firestore e Firebase Storage; outras bases ficam fora da baseline contratual.
4.6	Infraestrutura Cloud ou On-Premises	Firebase e Google Cloud incluídos; não existe infraestrutura on-premises na baseline.	Cumpre	Relatório Cloud	Cobertura limitada aos três projetos/ambientes e recursos associados definidos no SOW.
4.7	Configuração de servidores	Cloud Functions e serviços geridos incluídos; não existem servidores dedicados na baseline.	Cumpre	Relatório Cloud	Os controlos são avaliados segundo a natureza serverless e managed-service da solução.
4.8	Redes e comunicações	TLS, endpoints, networking GCP aplicável, exposição e comunicações com integrações externas.	Cumpre	Relatório Técnico	Redes corporativas externas e sistemas de terceiros não integram a baseline de testes diretos.
4.9	Segurança da informação	Confidencialidade, integridade, disponibilidade, classificação, acessos e proteção de evidências.	Cumpre	Relatórios; Plano de Segurança	
4.10	Cibersegurança	Testes controlados, vulnerabilidades, ameaças, hardening e resposta.	Cumpre	Finding Register	
4.11	Gestão de utilizadores	Ciclo de vida, registo, recuperação, desativação, sessões e perfis.	Cumpre	Relatório de Identidade	
4.12	Controlo de acessos	RBAC/ABAC, claims, regras, IAM, contas de serviço e menor privilégio.	Cumpre	Relatório de Identidade	
4.13	Integrações externas	Inventário, autenticação, segredos, erros, privacidade e dependências de terceiros.	Cumpre	Relatório de Integrações	Autorizações de terceiros podem ser requeridas.
4.14	Processos DevOps	CI/CD, segurança de pipelines, ambientes, aprovações, release e rollback.	Cumpre	Avaliação DevSecOps	
4.15	Gestão de código-fonte	Acessos, branches, reviews, proteção, segredos, histórico e segregação.	Cumpre	Avaliação de Engenharia	
4.16	Testes automatizados e manuais	Estratégia, cobertura, tipos, qualidade, evidência, integração e critérios de release.	Cumpre	Avaliação de Testes	
4.17	Backup e recuperação	Backups, exportações, restauro, retenção, RTO/RPO e testes.	Cumpre	Avaliação de Resiliência	
4.18	Monitorização	Logs, métricas, alertas, dashboards, ownership, cobertura e retenção.	Cumpre	Avaliação Operacional	
4.19	Gestão de incidentes	Plano, papéis, severidade, escalonamento, comunicação, pós-incidente e exercícios.	Cumpre	Avaliação Operacional	
4.20	Documentação técnica	Arquitetura, APIs, runbooks, decisões, procedimentos, inventário e atualidade.	Cumpre	Relatório Técnico	A ausência será registada como gap.
5.1	Avaliação do estado atual	Síntese executiva e análise técnica por domínio.	Cumpre	Relatórios Executivo e Técnico	

Ref.	Requisito TOR	Resposta MANIFOLD	Estado	Entregável/Evidência	Clarificação
5.2	Pontos fortes	Controlos eficazes e boas práticas serão explicitamente reconhecidos.	Cumpre	Relatórios	
5.3	Não conformidades	Gaps contra requisitos e referenciais serão registados com evidência.	Cumpre	Matriz/Relatório	
5.4	Vulnerabilidades e criticidade	Classificação Crítica, Alta, Média, Baixa ou Informativa, com impacto contextual.	Cumpre	Finding Register	
5.5	Riscos técnicos e operacionais	Mapa de riscos, owner, resposta e risco residual.	Cumpre	Mapa de Riscos	
5.6	Classificação da maturidade	Escala 1-5 por domínio, racional e target state.	Cumpre	Matriz de Maturidade	
5.7	Recomendações técnicas detalhadas	Causa raiz, solução proposta, prioridade, esforço e dependências.	Cumpre	Relatório Técnico	
5.8	Plano de ações corretivas priorizado	Separação entre bloqueadores, pré-go-live, curto, médio e longo prazo.	Cumpre	Roadmap	
5.9	Melhorias de arquitetura, desempenho, segurança e qualidade	Recomendações integradas e target state.	Cumpre	Roadmap; Relatórios	
5.10	Conclusão de conformidade com boas práticas	Conclusão por domínio, limitações e risco residual.	Cumpre parcialmente	Relatório Executivo	Não equivale a certificação formal.
6.1	Aumentar segurança	Priorização e remediação de vulnerabilidades e gaps.	Cumpre	Roadmap	Benefício depende da implementação pelo Cliente.
6.2	Melhorar qualidade do software	Recomendações de código, testes, arquitetura e SDLC.	Cumpre	Relatório Técnico	
6.3	Reduzir riscos operacionais	Observabilidade, continuidade, incidentes, releases e ownership.	Cumpre	Mapa de Riscos	
6.4	Identificar otimizações	Performance, custos, consultas, processos e automação.	Cumpre	Roadmap	
6.5	Melhorar desempenho	Análise e recomendações de capacidade e eficiência.	Cumpre	Avaliação de Performance	
6.6	Reforçar confiança	Evidência independente e transparência de risco.	Cumpre	Relatório Executivo	
6.7	Preparar futuras certificações	Gap assessment e roadmap de maturidade.	Cumpre parcialmente	Matriz de Maturidade	Não inclui certificação.
6.8	Apoiar decisões estratégicas	Conclusão de go-live, prioridades e investimento.	Cumpre	Relatório Executivo	
7.1	Conclusão e base para melhoria contínua	O encerramento consolida resultados, risco residual, roadmap, ownership e mecanismos de acompanhamento.	Cumpre	Relatórios; Roadmap; Workshop	

4. Resumo de Conformidade

Estado	Quantidade de requisitos
Cumpre	50
Cumpre parcialmente	3
Cumpre quando aplicável	0
Não aplicável	1

A matriz adota uma baseline contratual fechada. Os requisitos condicionais são tratados pelos limites explícitos do SOW; a Fase 0 valida o inventário e os acessos sem reabrir preço ou calendário, salvo desvio material sujeito a Change Request. A autorização formal permanece obrigatória antes de testes intrusivos.

5. Decisões de Baseline e Limites Contratuais

- **Não existe aplicação web ou painel administrativo independente na baseline; interfaces administrativas expostas pelas APIs e pelo backend permanecem abrangidas.**
- **Limites incluídos: 1 aplicação Flutter Android/iOS, 3 repositórios ou 150 000 linhas lógicas de código, 30 Cloud Functions, 40 endpoints, 3 projetos/ambientes, 25 collections, 3 buckets e 8 integrações.**
- **A baseline considera gaming sem apostas em dinheiro real, prémios monetários, carteira, processamento direto de cartões, KYC/AML, RNG regulado ou utilização intencional por menores; operação de referência em Moçambique.**
- **Infraestrutura on-premises, redes corporativas, testes destrutivos ou de carga, parecer jurídico e certificação formal estão excluídos; a cobertura Firebase/GCP inclui análises seguras de capacidade. Prazo: 30 dias úteis, mobilização até cinco dias úteis e um reteste numa janela de 60 dias.**