



KLINIKSYS / GOVERNANÇA E PRIVACIDADE

Matriz de Responsabilidade Compartilhada: KlinikSys

Matriz de responsabilidade

CÓDIGO	KS-GOV-003	VERSÃO	1.0
VIGÊNCIA	29/07/2026	PRÓXIMA REVISÃO	Anual
CLASSIFICAÇÃO	Público	PROPRIETÁRIO	Segurança e Privacidade

USO E CONFIDENCIALIDADE

Público. Pode ser compartilhado livremente.

Sumário

1 O "checklist mínimo da ONG" (a parte que é de fato sua)

4

NOTA

Numa diligência de segurança (ex.: questionário de terceiros da RSM), a maioria dos controles **não é da ONG**: é da **plataforma** (KlinikSys) e da **nuvem** (Supabase/Vercel). Uma ONG voluntária não opera servidor, firewall ou EDR: ela **herda** esses controles do provedor. Este documento separa, para cada área, o que é **da plataforma** e o que é **da organização usuária (ONG)**. Numa diligência, o padrão de resposta correto é "**controle herdado do provedor + evidência**", não "N/A, somos pequenos".

Legenda: [ok] Plataforma (KlinikSys / nuvem) · [info] Organização (ONG) · [parcial] Compartilhado.

Área	Resp.	Plataforma (herdado)	Organização (ONG)
Hospedagem / infra / hardening	[ok]	Supabase + Vercel; sem servidor da ONG. Cabeçalhos CSP/HSTS/COOP/CORP.	:
Criptografia em trânsito	[ok]	HTTPS forçado, com HSTS.	:
Criptografia em repouso	[ok]	At-rest do Supabase + cache local AES-GCM-256 (PBKDF2).	:
Autorização / isolamento de dados	[ok]	RLS no banco em 100% das tabelas; isolamento multi-tenant.	:
MFA de admin	[parcial]	TOTP obrigatório para admin, verificado server-side (aal2) .	Cadastrar o TOTP e não compartilhar o segredo.
Gestão de acesso / menor privilégio	[parcial]	RBAC + RLS; expiração de voluntário; auto-lock por inatividade.	Definir quem é admin , revisar acessos, remover quem saiu (offboarding).
Senhas	[parcial]	Política de senha forte + verificação HIBP; bcrypt (Supabase).	Escolher senha forte; não reutilizar/compartilhar.
Logs / auditoria	[ok]	audit_logs/system_logs, ações negadas (*_DENIED), aba de revisão.	Revisar periodicamente (a UI facilita).
Gestão de vulnerabilidades	[ok]	CI: npm audit (gate) + Dependabot + Semgrep (SAST) + OSV + ZAP (DAST).	:
Secure SDLC / gestão de mudança	[ok]	TDD, PR + branch protection + all-checks; nada vai a prod sem CI verde.	:
Backup	[parcial]	Managed backup (Supabase) + backup local cifrado .enc.json + script de restore + DR doc.	Guardar o backup exportado em local seguro; testar a restauração.
Anti-malware / e-mail / navegação	[info]	App é PWA no browser; sem servidor da ONG p/ proteger.	Manter dispositivos/navegadores atualizados ; antivírus básico no tablet.
Conscientização / treinamento	[info]	Docs e material de apoio.	Treinar a equipe (LGPD + uso seguro); material curto sugerido.

Área	Resp.	Plataforma (herdado)	Organização (ONG)
Base legal LGPD (dado de saúde)	[info]	Ferramentas de direitos do titular (export/anonimização), ROPA/DPIA templates.	Definir a base legal (Art. 11) , preencher a política de privacidade, indicar encarregado (DPO).
DPA com subprocessadores	[parcial]	KlinikSys documenta os subprocessadores.	Assinar o DPA do Supabase (plano pago) e aceitar/recusar a IA (Google).
Transferência internacional (IA)	[parcial]	IA é opt-in, desligada por padrão ; áudio deletado pós-uso.	Decidir se liga a IA (transferência p/ EUA) e documentar a base.
Retenção / descarte	[parcial]	Soft-delete + anonimização + view de retenção (CFM 20 anos).	Acionar anonimização quando cabível; solicitar purga ao encerrar.
Resposta a incidente	[parcial]	INCIDENT_RUNBOOK.md + Sentry (erros redigidos).	Acionar o runbook; notificar as partes (ANPD/titulares) quando exigido.
Continuidade / DR (RTO/RPO)	[parcial]	Managed backups + restore documentado.	Definir a tolerância aceitável e validar o teste de restauração.

1 O "checklist mínimo da ONG" (a parte que é de fato sua)

Se você é uma ONG adotando o KlinikSys, sua parte na diligência é pequena e **não exige TI**:

- **Definir quem é admin** (poucas pessoas) e habilitar o **TOTP** de cada admin.
- **Remover acesso** de quem sai (a UI de usuários faz isso; a de revisão de acesso ajuda a auditar).
- **Base legal LGPD** documentada + política de privacidade preenchida + encarregado indicado.
- **DPA do Supabase** assinado (requer plano pago), decisão de custo.
- **Decidir sobre a IA** (Google/EUA): ligar só se aceitar e documentar; senão, deixar desligada.
- **Treinar a equipe** (LGPD + não compartilhar senha + dispositivos atualizados).
- **Guardar/testar o backup** exportado.

Tudo o mais (cripto, RLS, MFA server-side, hardening, vuln mgmt, CI seguro, logs) é **herdado** da plataforma, ver SECURITY_WHITEPAPER.md.

CONTROLE DE DISTRIBUIÇÃO

A versão vigente deve permanecer no repositório oficial da KlinikSys. Impressões e arquivos exportados não são controlados; valide sempre o código e a versão antes do uso.

CÓDIGO	KS-GOV-003	VERSÃO	1.0
CLASSIFICAÇÃO	Público	PROPRIETÁRIO	Segurança e Privacidade
APROVADOR	Proprietário do produto	PRÓXIMA REVISÃO	Anual

FIM DO DOCUMENTO