



KLINIKSYS / GOVERNANÇA E PRIVACIDADE

Subprocessadores: KlinikSys

Lista de subprocessadores

CÓDIGO	KS-GOV-004	VERSÃO	1.2
VIGÊNCIA	16/09/2026	PRÓXIMA REVISÃO	Semestral
CLASSIFICAÇÃO	Público	PROPRIETÁRIO	Segurança e Privacidade

USO E CONFIDENCIALIDADE

Público. Pode ser compartilhado livremente.

Sumário

1 Obrigatórios (base da plataforma)

1.1 Supabase: Auth, Banco (PostgreSQL), Storage

1.2 Vercel: Hospedagem estática / Edge (CDN)

1.3 Resend: entrega dos e-mails transacionais de autenticação

2 Opcionais (só com a feature habilitada pelo admin da org)

2.1 Google: Gemini API (IA: Scribe de voz + "Analisar com IA")

2.2 Sentry: Monitoramento de erros (observabilidade)

3 Não são subprocessadores de PHI (contexto)

4 Resumo para a diligência

3

3

3

3

4

4

5

5

5

NOTA

Lista dos terceiros que processam dados em nome de uma organização usuária do KlinikSys, com localização, o que processam, certificações e o link direto para a página de segurança / trust center (onde o relatório SOC 2 / ISO é obtido, normalmente mediante solicitação/NDA). **Como ler:** os subprocessadores **obrigatórios** (Supabase, Vercel, Resend) sustentam a plataforma. Os **opcionais** só entram em cena se o **admin da organização habilitar** a feature correspondente: vêm **desligados por padrão**.

Última revisão: 2026-09-16. Confirme sempre a versão atual do relatório no trust center de cada fornecedor (o relatório SOC 2 muda a cada período de auditoria).

NOTA

Revisão de 16/09/2026. A lista anterior afirmava que o Sentry pode ser desligado por organização, o que o código não permite, e descrevia o que é enviado à IA de forma incompleta. **Nenhum contrato de tratamento está assinado** com qualquer fornecedor desta lista; o bloqueio é a ausência de pessoa jurídica para assiná-los.

1 Obrigatórios (base da plataforma)

1.1 Supabase: Auth, Banco (PostgreSQL), Storage

- **O que processa:** todos os dados da aplicação (pacientes, consultas, etc.), autenticação e arquivos (fotos, assinaturas). É a **fonte de verdade**.
- **Localização:** região **sa-east-1 (São Paulo, Brasil)**: dado em repouso no Brasil.
- **Certificações:** SOC 2 Type II, **ISO 27001**. HIPAA disponível em planos pagos.
- **Segurança / Trust center:** <https://supabase.com/security>
- **SOC 2 (visão geral):** <https://supabase.com/docs/guides/security/soc-2-compliance>
- **DPA (Acordo de Tratamento de Dados):** <https://supabase.com/legal/dpa> *A assinatura do DPA e o acesso ao relatório SOC 2 completo exigem plano pago.*

1.2 Vercel: Hospedagem estática / Edge (CDN)

- **O que processa:** serve **apenas os arquivos estáticos** do app (HTML/JS/CSS) e aplica os cabeçalhos de segurança (CSP/HSTS). **Não armazena PHI**, nenhum dado de paciente passa/reside na Vercel.
- **Hosts:** o aplicativo em app.kliniksys.com; o site institucional, que não tem login nem toca dado pessoal, em kliniksys.com como **projeto separado** (ver ADR-022). O DNS é do Cloudflare em modo DNS only, sem proxy: o Cloudflare resolve o nome e não termina a conexão, portanto **não é subprocessador de conteúdo**.
- **Localização:** edge global; sem persistência de dados pessoais.
- **Certificações:** SOC 2 Type II, **ISO 27001**.
- **Segurança / Trust center:** <https://vercel.com/security> · <https://security.vercel.com>
- **DPA:** <https://vercel.com/legal/dpa> *Conta hoje no plano **Hobby**, cujos Termos proíbem uso comercial. Migração para o Pro decidida para antes de qualquer cobrança ao adotante (risco R24).*

1.3 Resend: entrega dos e-mails transacionais de autenticação

- **Situação (29/08/2026): ativo.** É o SMTP custom do Supabase Auth desde 29/08/2026, verificado de ponta a ponta com um fluxo real de redefinição de senha. Domínio kliniksys.com verificado com DKIM, SPF e MX de retorno no subdomínio send.kliniksys.com, mais DMARC em p=none.
- **O que processará:** o **endereço de e-mail** do profissional de saúde e o corpo dos e-mails de autenticação (confirmação de conta, convite, redefinição de senha). **Não processa dado de paciente:** nenhum e-mail transacional carrega PHI, e o conteúdo é gerado pelos templates do Supabase Auth.
- **Titulares afetados:** usuários do sistema (profissionais e administradores), **não pacientes**.
- **Localização:** envio na região **sa-east-1 (São Paulo, Brasil)**, escolhida na criação do domínio. A Resend é empresa americana, e **não está confirmado com o fornecedor onde ficam os logs** com os 3 dias de retenção. Portanto: o envio não é transferência internacional; a retenção de log **pode ser**, e é ponto de auditoria em aberto. Em qualquer hipótese, o dado é cadastral (endereço de e-mail de profissional), nunca dado sensível de saúde.
- **Certificações:** SOC 2 Type II, GDPR.
- **Segurança / Trust center:** <https://resend.com/security>
- **DPA:** <https://resend.com/legal/dpa>, **a assinar**, bloqueado pela mesma ausência de entidade jurídica que trava o pacote contratual.
- **Retenção:** o plano Pro retém o conteúdo do e-mail por **3 dias** para depuração de entrega. Isso é retenção de endereço de e-mail em servidor estrangeiro e precisa constar do aviso de privacidade ao usuário.

2 Opcionais (só com a feature habilitada pelo admin da org)

NOTA

Estas features vêm **DESLIGADAS por padrão**. A transferência de dados a estes terceiros só ocorre se o admin da organização **ativar** a flag correspondente em Configurações da Organização. Uma ONG que não pode aceitar transferência internacional simplesmente **não liga**: o sistema funciona 100% sem eles.

2.1 Google: Gemini API (IA: Scribe de voz + "Analisar com IA")

- **Feature flag:** ai_scribe e/ou ai_consultation (opt-in). **Off por padrão**.
- **O que processa (só se ligado):** o **áudio integral da consulta** (Scribe) ou, na análise, **data de nascimento completa, sexo, histórico médico, sinais vitais, especialidade e o texto livre da queixa**. Nome, CPF e foto não são enviados, mas isso não torna o dado anônimo: numa comunidade pequena, data de nascimento e sexo permitem reidentificação, e o texto livre pode conter nomes. A Edge Function repassa o conteúdo sem filtro. **Isto é transferência internacional de dado de saúde (EUA)**, LGPD Art. 33.
- **Mitigações no produto:** opt-in por org, verificado no servidor (ADR-021); o **áudio é apagado pelo aplicativo** logo após a transcrição, com sucesso ou erro. A exclusão é feita pelo navegador, em melhor esforço: se a aba fechar no meio, o arquivo permanece no bucket e não há limpeza no servidor.
- **Certificações (Google Cloud):** SOC 1/2/3, ISO 27001/27017/27018/**27701**, HIPAA (com BAA).

- **Compliance Google Cloud:** <https://cloud.google.com/security/compliance/offerings>
- **SOC 2 (Google Cloud):** <https://cloud.google.com/security/compliance/soc-2>
- **Termos da Gemini API:** <https://ai.google.dev/gemini-api/terms> **Ponto de auditoria a confirmar:** a Gemini *Developer* API (AI Studio, camada gratuita) pode **usar o conteúdo para melhorar produtos**; o **Vertex AI** (Google Cloud, pago) oferece garantia de **não-treinamento** + DPA. Para PHI, recomenda-se o caminho com garantia contratual de não-uso, **ou manter a IA desligada**. Decisão da organização.

2.2 Sentry: Monitoramento de erros (observabilidade)

- **O que processa:** eventos de erro do frontend **com PHI removido**: um scrubber (`redact()`) remove nome, CPF, diagnóstico, telefone antes do envio.
- **Certificações:** SOC 2 Type II, **ISO 27001**.
- **Segurança / Trust:** <https://sentry.io/security/> · <https://security.sentry.io>
- **DPA:** <https://sentry.io/legal/dpa/>
- **O que envia além do erro:** o identificador (UUID) do profissional logado.
- **Ativação:** global, quando `VITE_SENTRY_DSN` está configurado na publicação do aplicativo. **Não há desligamento por organização**; a versão anterior desta lista afirmava o contrário.
- **Localização da conta:** a confirmar.

3 Não são subprocessadores de PHI (contexto)

Terceiro	Papel	Dado pessoal?
OpenStreetMap	tiles do mapa epidemiológico	Não: só coordenadas de tile são requisitadas; nenhum PHI é enviado. Tiles são cacheados offline.
GitHub / Dependabot / GitHub Actions	código-fonte e CI/CD	Não em produção: nunca processam dado de paciente.
Cloudflare	DNS autoritativo de <code>kliniksys.com</code>	Não: opera em modo <code>DNS only</code> , sem proxy. Resolve o nome e não termina a conexão TLS, portanto não vê tráfego nem conteúdo.

4 Resumo para a diligência

- **Dado de paciente em repouso:** apenas no **Supabase (Brasil, sa-east-1)**: SOC 2 + ISO 27001.
- **Transferência internacional de dado de saúde:** somente com a IA e a transcrição (Google, EUA), **desligadas por padrão**.
- **Transferência internacional de dado cadastral:** a Resend, ativa desde 29/08/2026, envia em São Paulo; a localização dos registros de 3 dias está a confirmar. Nunca envolve paciente.
- **Vercel** não vê dado de paciente (só estáticos). **Sentry** vê erros redigidos e o UUID do profissional.

- **Contratos:** nenhum assinado com qualquer fornecedor desta lista.
- Cada fornecedor mantém trust center próprio; solicite o relatório SOC 2 vigente pelos links acima.

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-004	VERSÃO	1.2
CLASSIFICAÇÃO	Público	PROPRIETÁRIO	Segurança e Privacidade
APROVADOR	Proprietário do produto	PRÓXIMA REVISÃO	Semestral

FIM DO DOCUMENTO