Security Brief — Reuniones clínicas

Auditoría Jun 2026 · Multi-tenant RLS enforced

Kimun.pro · Plataforma y app iOS para equipos de salud

SaaS clínico con seguridad en capas: OAuth profesional, datos aislados por organización en PostgreSQL (Neon) con RLS strict en producción y rol app sin bypass (`kimun_app`), archivos privados, permisos por rol/módulo y auditoría externa con 7 hallazgos cerrados.

5 PILARES DE SEGURIDAD

Autenticación

- Google, Apple o Microsoft — sin contraseñas Kimun
- Sesiones httpOnly + secure en producción; revocables
- Dashboard y APIs bloqueados sin sesión válida

Aislamiento de datos

- Cada organización en su propio tenant (orgDomain)
- RLS Postgres Fase 3 strict + ola remaining (0044) en prod
- Rol `kimun_app` sin BYPASSRLS — enforcement en capa DB
- Postgres fuente única; KV clínico legacy eliminado

Archivos clínicos

- Almacenamiento privado — no URLs públicas directas
- Descarga tras verificar propiedad y tenant del archivo
- Adjuntos mensajería: ownership blob validado server-side

Defensa en profundidad

- HTTPS + HSTS + CSP en toda la plataforma
- Webhooks Twilio/Mercado Pago: firma obligatoria o rechazo
- Rate limiting en login, APIs sensibles y rutas admin
- Fail-closed RLS en app (`withTenantSql` + sin fallback Drizzle)

IA responsable

- IA restringida por permiso de usuario
- Documentos acotados (máx. 3 PDF, 5 MB c/u por consulta)
- No entrenamos modelos con datos de pacientes

COMPLIANCE CHILE

- Ley 19.628 / 20.584: institución = responsable; Kimun = encargado
- Política de privacidad, términos y Trust Center en kimun.pro
- Checklist DPA 1 página para pilotos clínicos
- Ley de Urgencia con logs de auditoría (usuario, IP, timestamp)
- Subencargados: Vercel, Neon, Twilio, Google, Sentry

AUDITORÍA CERRADA (JUN 2026)

- Auditoría externa jun 2026: 7 hallazgos (1 crítico) — todos cerrados
- Middleware auth en /api/*; tokens OAuth no expuestos en URL
- Webhooks sin secreto configurado → rechazo automático
- RLS Fase 3 + remaining (0044) promovido en prod; rol kimun_app enforced
- Smoke post-deploy + clinical-auth 8/8; monitor:rls 4/4
- Rutas bootstrap E2E bloqueadas en producción

PREGUNTAS FRECUENTES

¿Dónde están los datos? PostgreSQL (Neon) + blobs privados. RLS strict por tenant; rol app sin bypass en prod.

¿Pentest / certificación? Auditoría jun 2026 cerrada. Trust Center público. Pentest externo: planificado.

¿Es historia clínica legal? No reemplaza la ficha oficial del establecimiento.

contacto@kimun.pro
Trust Center · Privacidad · Seguridad