Security Brief Institucional

Kimun.pro · Capa operativa trazable para equipos de salud

Jun 2026 · Trust Center público

Kimun coordina entregas de turno, interconsultas, Ley de Urgencia, camas, pabellones y mensajería segura sin reemplazar el HIS ni la ficha clínica oficial. Datos clínicos operacionales en Postgres con RLS; KV queda limitado a sesiones, rate limits, caches y flujos transitorios no clínicos. OAuth institucional, archivos privados, trazabilidad de acciones sensibles, controles de IA y DPA enterprise disponible para revisión institucional.

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

- Separación lógica por institución y dominio organizacional
- Datos clínicos operacionales en Postgres con RLS
- KV limitado a sesiones, rate limits, caches y flujos transitorios no clínicos
- Rol de aplicación sin privilegios de bypass en producción

Comunicación clínica

- Video-interconsulta 1:1: sala privada Daily.co, token OAuth, sin grabación
- Máx. 2 participantes verificados; salas efímeras con auditoría
- App y push reducen dependencia de WhatsApp personal
- Mensajería de turno con contexto clínico y adjuntos privados

Defensa en profundidad

- HTTPS + HSTS + CSP en toda la plataforma
- Webhooks de pagos y mensajería con firma o secreto obligatorio
- Rate limiting en login, APIs sensibles y rutas admin
- Rutas privadas protegidas por sesión y permisos por módulo

IA responsable

- IA restringida por permiso, módulo y configuración institucional
- Funciones de IA pueden enviar fragmentos a proveedores externos autorizados
- No entrenamos modelos propios con datos institucionales

COMPLIANCE CHILE

- Ley 19.628 / 20.584: institución = responsable; Kimun = encargado
- Trust Center, privacidad, términos y DPA enterprise disponible
- Ley de Urgencia: reportes a jefatura con logs (usuario, IP, timestamp)
- Códigos de verificación firmados (HMAC) en IC, LU y entrega de turno
- Subencargados documentados: Vercel, Neon, Daily.co, Twilio, Google, OpenAI, Resend, Sentry, PostHog y pagos
- Retención referencial: mensajes 90d; IA, IC, LU y entregas 365d; pabellón 730d

CONTROLES VERIFICADOS

- Revisión técnica jun 2026: hallazgos remediados y controles reforzados
- Aislamiento por organización validado con pruebas de RLS y rol app restringido
- Smoke post-deploy, pruebas de rutas clínicas y monitoreo de aislamiento
- Trust Center público con stack, controles, DPA y security brief descargable
- Rutas E2E bloqueadas en producción y webhooks sin secreto rechazados

PREGUNTAS FRECUENTES

¿Dónde están los datos? Datos clínicos operacionales en Postgres (Neon) con RLS; KV queda limitado a sesiones, rate limits, caches y flujos transitorios no clínicos. Archivos clínicos en blob privado con controles de acceso.

¿Pentest / certificación? Revisión técnica jun 2026 cerrada; pentest externo planificado como siguiente hito enterprise.

¿Es historia clínica legal? No. Kimun complementa el HIS y la ficha oficial como capa operativa trazable.

francisco@kimun.pro
Trust Center · DPA · Privacidad · Seguridad

Documento Kimun.pro — 29 Jun 2026. No sustituye asesoría legal, DPA firmado ni contrato institucional.