MEDAI · TOOLDATA SPA

Dossier de seguridad

Diseño de seguridad y arquitectura de referencia de MedAI

Activo de confianza · MedAI en pre-lanzamiento · julio de 2026

Naturaleza del documento. Este dossier describe el **diseño de seguridad objetivo** de MedAI y su **arquitectura de referencia** de despliegue en la infraestructura del cliente. Está dirigido al equipo de seguridad (CISO / TI) de una clínica u hospital que realiza *due-diligence*. MedAI se encuentra en **pre-lanzamiento**: algunos componentes están en construcción y las cifras técnicas son **referenciales**, ajustables en cada implementación. Es el documento que la Arquitectura de Referencia de Despliegue referencia en su §6 (Seguridad). No describe implementaciones en producción con clientes ni constituye una certificación.

Campo	Valor
Producto	MedAI — plataforma de apoyo a la decisión clínica con IA
Proveedor (encargado de tratamiento)	Tooldata SpA, RUT 76.963.629-3 — Concón, Región de Valparaíso, Chile
Estado	Pre-lanzamiento (diseño de referencia)
Modalidades de despliegue	On-premise · Nube privada dedicada (VPC) · Híbrido · Air-gapped
Versión del documento	1.0 — julio de 2026
Documentos relacionados	Arquitectura de Referencia de Despliegue · DPA (Ley 21.719) · Plantilla EIPD · Guía de dimensionamiento

1. Alcance y naturaleza

1.1 Qué cubre este documento

Cubre el diseño de seguridad de **MedAI como producto** desplegado en la infraestructura del cliente, y aclara la separación con el **sitio web corporativo** de Tooldata. La distinción es central para entender el modelo de amenazas y el papel de terceros.

Superficie	Qué es	Dónde se ejecuta	Datos que maneja
Producto MedAI	Software de apoyo clínico (orquestador, inferencia local, conectores, auditoría)	**Infraestructura del cliente** (on-premise / VPC)	Datos clínicos sensibles del cliente
Sitio web (`medai.tooldata.io`)	Sitio de marketing y formulario de contacto	Hosting de Tooldata	Datos de contacto de *leads* (nombre, correo, mensaje). **Sin datos clínicos.**

Consecuencia de diseño: **los datos clínicos solo existen dentro del perímetro del producto, en la infraestructura del cliente.** El sitio web no toca datos de pacientes.

1.2 Principio rector: apoyo, no autonomía

MedAI genera **borradores** (epicrisis, resúmenes, propuestas de codificación CIE-10, apoyo a la lectura de imágenes). Toda salida es un borrador que un **profesional habilitado revisa, edita, valida y firma** (arquitectura *human-in-the-loop*). MedAI **no emite diagnóstico autónomo** ni reemplaza el juicio clínico; la responsabilidad de la decisión permanece en el profesional. Este encuadre es también un control de seguridad y de calidad: ninguna salida se considera definitiva sin validación humana registrada.

1.3 Naturaleza pre-lanzamiento

Los controles descritos corresponden al **diseño objetivo**. Cuando un control está en construcción o depende del entorno del cliente, se indica. Este documento no afirma tracción, uso en producción ni certificaciones vigentes.

2. Modelo de amenazas (resumen)

2.1 Activos a proteger

- **Datos clínicos sensibles** (Ley 21.719): identificación de pacientes, datos de salud, imágenes médicas (DICOM), y los **borradores** generados.
- **Registros de auditoría y trazabilidad** (autoría, versión de modelo/plantilla, marcas de tiempo).
- **Integridad del modelo y de las plantillas/prompts** (que la versión que genera un borrador sea la esperada y verificable).
- **Credenciales, secretos y claves** de integración (HIS/EMR, PACS/RIS, IdP).
- **Disponibilidad** del servicio para la operación clínica.

2.2 Actores y superficies consideradas

Actor / amenaza	Superficie	Mitigación de diseño
Atacante externo por internet	Egress / exfiltración	On-premise: sin exposición pública por defecto; en modo **air-gapped, sin salida a internet**. VPC: entorno dedicado y aislado, sin exposición pública por defecto.
Movimiento lateral desde la red del cliente	Red interna	Segmentación, mínimo privilegio, gateway único con TLS + SSO.
Usuario interno malintencionado o negligente	Acceso a la aplicación	RBAC, *necesidad de conocer*, registros de auditoría, versionado de salidas.
Compromiso de la cadena de suministro (dependencias, imágenes)	SDLC / actualizaciones	Releases **firmados** (cosign/sigstore) verificados antes de aplicar; importación controlada; sin cambios silenciosos.
Acceso indebido de personal del proveedor	Soporte/mantenimiento	Acceso del encargado limitado y autorizado por el cliente (DPA); operación bajo control del cliente.
Fuga por servicios de terceros / nube pública	Procesamiento externo	**Inferencia local**: los datos no se envían a servicios de terceros ni a modelos públicos.

2.3 Cómo el despliegue en la infraestructura del cliente reduce la superficie

La decisión arquitectónica más relevante es **dónde se procesan los datos**. Al ejecutarse dentro del perímetro del cliente:

- En **on-premise**, los datos clínicos **no salen de la red del cliente**; en modo air-gapped no existe conexión saliente a internet.
- En **nube privada (VPC)**, los datos permanecen en un **entorno dedicado bajo el control del cliente**, sin infraestructura compartida con otros clientes.
- En ambos modos los datos clínicos permanecen **bajo el control del cliente** y **no se usan para entrenar** modelos de uso general ni de terceros.

Esto elimina, por diseño, categorías completas de riesgo asociadas al envío de datos sensibles a servicios externos.

3. Controles de seguridad técnica

3.1 Cifrado

- **En tránsito:** TLS en el punto de ingreso (API Gateway) y en las comunicaciones entre servicios; certificados provistos y controlados por el cliente.
- **En reposo:** cifrado **AES** de la base de datos (PostgreSQL), del almacenamiento de objetos y de los respaldos. Puede combinarse con el cifrado a nivel de disco/volumen del cliente.

3.2 Identidad y accesos (IAM)

- **RBAC** (control de acceso por rol) con **principio de mínimo privilegio** y **necesidad de conocer**.
- **SSO** federado con el IdP del cliente vía **SAML / OIDC** (Active Directory / Entra ID / Keycloak). MedAI no busca ser un almacén paralelo de identidades.
- Separación de roles operativos (administración, uso clínico, auditoría).

3.3 Segmentación de red y *hardening*

- **Gateway único de ingreso** (reverse proxy) con TLS, autenticación SSO y *rate limiting*.
- **Segregación de entornos** y de componentes; el servidor de inferencia y la base de datos no se exponen directamente.
- Modo **air-gapped** sin egress a internet como configuración soportada.
- *Hardening* del SO Linux base, imágenes de contenedor minimizadas y superficie de servicios reducida (referencia de plataforma en la Guía de dimensionamiento y en `docker-compose`/Helm de referencia).

3.4 Gestión de secretos

- Credenciales de integración (HIS/EMR, PACS/RIS, IdP), claves y certificados gestionados como **secretos**, fuera del código y de las imágenes, con acceso restringido por rol.
- Integrable con el gestor de secretos del cliente (por ejemplo, el nativo del orquestador Kubernetes o una bóveda del cliente).

4. Tratamiento de datos

- **No entrenamiento con datos del cliente.** Política categórica y **contractual** (DPA, cláusula 5.2): los datos del cliente no se usan para entrenar modelos de uso general o de terceros, ni se comparten fuera de lo pactado.
- **Minimización.** Se tratan solo los datos necesarios para la finalidad (documentación clínica, codificación, apoyo a imagenología).
- **Retención configurable.** Plazos de conservación de artefactos temporales y metadatos parametrizables por el cliente; borrado según su política y la normativa de ficha clínica (Ley 20.584).
- **Anonimización / enmascaramiento** donde aplique, para reducir el riesgo de reidentificación.

- **Trazabilidad y versionado de salidas.** Cada borrador y cada salida validada queda registrada con **autor/validador, versión de modelo y de plantilla, y marca de tiempo**, permitiendo saber siempre *qué versión generó qué resultado y quién lo firmó*.

> Nota sobre alcance clínico: la trazabilidad y el versionado son controles de auditoría e integridad. MedAI **no** clasifica ni prioriza automáticamente casos por criticidad clínica; toda interpretación corresponde al profesional que valida y firma.

5. Ciclo de vida seguro del software (SDLC)

- **Control de dependencias.** Inventario de componentes de terceros; las imágenes de contenedor se construyen a partir de bases controladas y minimizadas.
- **Gestión de vulnerabilidades.** Análisis de vulnerabilidades sobre dependencias e imágenes como parte del proceso de publicación; corrección priorizada por severidad (proceso en maduración durante el pre-lanzamiento).
- **Actualizaciones versionadas y firmadas.** Cada *release* se publica como **imágenes de contenedor versionadas** acompañadas de su **firma criptográfica (cosign / sigstore)**.
- **Importación controlada, incluso air-gapped.** El cliente recibe el *bundle* (descarga controlada o medio físico), **verifica la firma** contra la cadena de confianza **antes** de importar y aplicar, y puede **revertir** a la versión anterior. No se requiere conexión saliente a internet.
- **Sin cambios silenciosos en producción.** Los cambios de modelo o de plantilla son **explícitos, versionados y aprobados por el cliente** en despliegues on-premise/air-gapped; no se aplican actualizaciones automáticas no consentidas.

Este flujo protege la integridad de la cadena de suministro (§2.2) y garantiza que la versión en ejecución sea siempre conocida, verificable y reversible.

6. Operación

- **Registros de auditoría.** Registro estructurado de accesos, acciones y salidas, con trazabilidad de autoría y versión, disponible para el equipo de seguridad del cliente y para dar soporte a la notificación de brechas (§7).
- **Observabilidad dentro del perímetro.** Logs, métricas y salud de servicios (referencia: Prometheus / Grafana) **dentro de la infraestructura del cliente**; la telemetría clínica no se envía a Tooldata.
- **Respaldos y recuperación (DR).** Respaldos cifrados de base de datos y artefactos; plan de recuperación ante desastres. La arquitectura de alta disponibilidad (redundancia, réplica) se dimensiona por contrato (ver Guía de dimensionamiento; los tiempos de recuperación y disponibilidad se acuerdan por caso, sin comprometer cifras de *uptime* sin un diseño de HA validado).
- **Rollback por versión.** Al ser releases versionados y firmados, se puede revertir a una versión previa conocida ante una regresión.

7. Respuesta a incidentes y notificación de brechas

7.1 Reparto de responsabilidades (Ley 21.719)

- El **Responsable** del tratamiento es la **institución de salud** (clínica/hospital): determina fines y medios, y le corresponde el deber de **notificar a la Agencia** y, cuando proceda, a los titulares.
- **Tooldata SpA** actúa como **Encargado**: trata datos por cuenta y según instrucciones documentadas del Responsable.

7.2 Flujo de notificación

Conforme al DPA (cláusula 8), ante una **vulneración de seguridad** que afecte datos personales tratados por cuenta del Responsable, el Encargado notificará al Responsable **sin dilación indebida** tras tener conocimiento, para que este cumpla su deber de notificación dentro de los **plazos legales** (referencialmente **72 horas**, a confirmar con el texto vigente de la Ley 21.719 y las guías de la Agencia).

La notificación incluirá, en la medida disponible: naturaleza de la vulneración, categorías y volumen aproximado de datos y titulares afectados, consecuencias probables y medidas adoptadas o propuestas.

7.3 Consideración de perímetro

En despliegues on-premise/VPC, la **detección y respuesta de primer nivel** ocurre dentro del perímetro y bajo control del cliente; Tooldata asiste según lo pactado en el DPA y el contrato de soporte. El plan de respuesta a incidentes específico (roles, contactos, tiempos) se acuerda en la implementación.

8. Subprocesadores (subencargados)

Ámbito	Subprocesadores de datos	Detalle
Producto MedAI (on-premise / VPC)	**Ninguno externo de datos clínicos**	La inferencia y el tratamiento ocurren en la infraestructura del cliente. Los datos clínicos no se transfieren a terceros ni fuera de dicha infraestructura.
Sitio web corporativo	**Resend** (correo transaccional)	Envía las notificaciones del formulario de contacto; procesa **datos de contacto de *leads*, no datos clínicos**. Almacenamiento en EE. UU. (transferencia regida por el contrato del proveedor).

La lista de subencargados y sus garantías se formaliza en el **Anexo III del DPA**, con derecho del Responsable a ser informado y a oponerse por motivos fundados ante cambios. El punto clave para *due-diligence*: **el producto que trata datos clínicos no depende de subprocesadores externos de datos.**

9. Cumplimiento y estándares

MedAI se **diseña alineado con las familias de controles** de estándares reconocidos de seguridad de la información, **sin afirmar certificación alguna**. El siguiente mapeo es de diseño, no una atestación:

Familia de controles	Cómo lo aborda MedAI (diseño)
Control de acceso e identidad	RBAC, SSO SAML/OIDC, mínimo privilegio, necesidad de conocer
Criptografía	TLS en tránsito, AES en reposo, respaldos cifrados, firma de releases
Seguridad de operaciones	Registros de auditoría, observabilidad en el perímetro, gestión de vulnerabilidades, gestión de cambios versionada
Continuidad y resiliencia	Respaldos, plan de recuperación (DR), rollback por versión, opción de HA

Familia de controles	Cómo lo aborda MedAI (diseño)
Seguridad del desarrollo / cadena de suministro	Control de dependencias, releases firmados (cosign/ sigstore), importación verificada
Relación con proveedores	DPA (Ley 21.719), gobierno de subencargados, notificación de brechas

Marco normativo chileno considerado: - **Ley 21.719** (protección de datos personales) — **plena vigencia el 1 de diciembre de 2026**; los **datos de salud son datos sensibles** con régimen reforzado (la Ley 19.628 rige hasta esa fecha). - **Ley 20.584** — derechos del paciente, **ficha clínica** y secreto médico. - **Ley 21.668** — **interoperabilidad** del sistema de salud (estándares **HL7 FHIR**). - **ISP / dispositivos médicos (SaMD):** Chile está incorporando el software como dispositivo médico al régimen de control sanitario del ISP; el alcance se evalúa por caso de uso con asesoría regulatoria. La arquitectura *human--in-the-loop* (apoyo, no diagnóstico autónomo) define el encuadre.

Estándares internacionales como referencia de diseño (no certificación): el diseño se orienta con los controles de marcos como **ISO/IEC 27001/27002**, y considera prácticas de resguardo de datos de salud del tipo **HIPAA/SOC 2** como referencia de controles, sin declarar cumplimiento certificado de ninguno de ellos.

> **ISO 27001:** en **roadmap / en diseño**. Tooldata construye su sistema de gestión de seguridad de la información alineado con estos controles; **MedAI/Tooldata no está certificado ISO 27001** a la fecha de este documento.

10. Contacto de seguridad y solicitud de información

- **Contacto:** `hola@tooldata.io` — asunto sugerido: **«Seguridad — MedAI»** (consultas de *due-diligence*, cuestionarios de seguridad, solicitud de este dossier, DPA o plantilla EIPD).
- **Divulgación responsable:** las notificaciones de posibles vulnerabilidades pueden dirigirse al mismo correo con el asunto **«Seguridad — Divulgación»**; se acusará recibo y se coordinará el tratamiento.
- **Entidad:** Tooldata SpA, RUT 76.963.629-3, Avenida Concón Reñaca 4000, oficina 1603, Concón, Región de Valparaíso, Chile.

Documentación complementaria disponible bajo solicitud: Arquitectura de Referencia de Despliegue, Guía de dimensionamiento, DPA modelo (Ley 21.719) y plantilla de EIPD/DPIA. Para escenarios específicos (air-gapped, HA, integración con un IdP o PACS/HIS concreto), la definición se acuerda en la fase de implementación.

> **Aviso.** Documento de **diseño de seguridad en pre-lanzamiento**. Describe la arquitectura y los controles **objetivo** de MedAI; algunos están en construcción y las cifras son referenciales. **No constituye una certificación, una garantía contractual ni asesoría legal**, y está **sujeto a evolución** del producto. Las obligaciones vinculantes se establecen en el contrato de servicio y en el DPA. Julio de 2026 — versión 1.0.