

Dossier de seguridad y cumplimiento.

Resumen ejecutivo de las medidas de seguridad, protección de datos y cumplimiento normativo aplicadas por ClinicMate al tratamiento de información clínica, fiscal y personal de tus pacientes.

VERSIÓN

2026.05.01

VIGENCIA

12 meses

DIRIGIDO A

DPO · gerencia ·
aseguradora

PÁGINAS

18

CONFIDENCIAL

CLINICMATE TECHNOLOGIES S.L. · NIF B12345678 · PALMA DE MALLORCA

● CÓMO LEER ESTE DOCUMENTO

Índice del dossier

Este dossier resume las medidas técnicas, organizativas y legales que aplica ClinicMate. Cada apartado incluye la norma de referencia y el control concreto que aplicamos.

01	Sobre ClinicMate y alcance del servicio	p. 3
02	Marco normativo aplicable	p. 4
03	Verifactu — facturación electrónica (RD 1007/2023)	p. 5
04	Sistema anti-marca — Ley 29/2006 del Medicamento	p. 7
05	Tratamiento de datos personales (RGPD / LOPDGDD)	p. 8
06	Datos clínicos y Ley 41/2002 de autonomía del paciente	p. 10
07	Hosting, localización y subprocesadores	p. 11
08	Cifrado, control de acceso y trazabilidad	p. 12
09	Backups, continuidad y respuesta a incidentes	p. 14
10	Derechos del interesado y procedimiento de ejercicio	p. 15
11	Pentests, auditorías y mejora continua	p. 16
12	Matriz resumen de controles	p. 17
13	Contacto del DPO y aceptación	p. 18

NOTA

Este documento es un resumen no contractual. Las obligaciones formales se rigen por el Contrato de Tratamiento de Datos (DPA) firmado entre cliente y ClinicMate Technologies S.L., disponible en el área de facturación de tu cuenta.

01

Sobre ClinicMate y alcance del servicio

ClinicMate es una plataforma SaaS de gestión integral para clínicas estéticas, médicas y profesionales sanitarios autónomos. Reemplaza las herramientas tradicionalmente fragmentadas — agenda, ficha de paciente, historia clínica, consentimientos, facturación, booking online — en un único sistema.

Entidad responsable

RAZÓN SOCIAL	ClinicMate Technologies S.L.
NIF	B-12345678
DOMICILIO SOCIAL	Palma de Mallorca, Illes Balears, España
REGISTRO	Registro Mercantil de Palma de Mallorca
ROL RGPD	Encargado del tratamiento — el cliente (la clínica) es el Responsable
DPO	dpo@clinicmate.eu

Alcance del servicio

Las medidas descritas en este dossier aplican a todos los productos comercializados bajo la marca ClinicMate:

- **CRM y agenda** — gestión diaria de la clínica, ficha de paciente, historia clínica.
- **Booking online** — widget de reservas embebido en la web de la clínica.
- **Web de clínica** — sitio público administrado, incluido sin coste con cualquier plan de pago.
- **Chatbot IA** — asistente conversacional con captura de leads y reserva automática.
- **Portal del paciente** — área privada para consultar citas, fotos, consentimientos y facturas.

Estadísticas operativas

UE	99,98 %	< 24 h
----	---------	--------

HOSTING · MADRID Y
FRÁNCFORT

UPTIME REAL EJERCICIO
2025

NOTIFICACIÓN DE
INCIDENTES

02 Marco normativo aplicable

ClinicMate cumple con la totalidad del marco jurídico español y europeo que afecta al tratamiento de datos personales, datos sanitarios, facturación y publicidad sanitaria.

NORMA	REFERENCIA	APLICACIÓN EN CLINICMATE
Reglamento General de Protección de Datos	UE 2016/679	Base jurídica del tratamiento, derechos del interesado, registro de actividades, EIPD cuando procede.
Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales	LO 3/2018	Adaptación al RGPD en España, derechos digitales, sanciones AEPD.
Ley básica reguladora de la autonomía del paciente	Ley 41/2002	Historia clínica, consentimiento informado, retención mínima 5 años, derecho de acceso.
Ley de garantías y uso racional del medicamento	Ley 29/2006	Prohibición de publicidad de marcas registradas de medicamentos sujetos a prescripción. Aplicado mediante el sistema anti-marca (sección 4).
Reglamento de facturación electrónica	RD 1007/2023	Verifactu. Encadenado de facturas, envío a la AEAT, QR oficial. Detalle en sección 3.
Reglamento eIDAS de firma electrónica	UE 910/2014	Firma digital de consentimientos y sesiones clínicas con validez jurídica.
Directiva NIS2 de ciberseguridad	UE 2022/2555	Medidas técnicas y organizativas, notificación de incidentes < 24 h.
Estándar de seguridad para pagos con tarjeta	PCI-DSS	Procesamiento delegado en Stripe (nivel 1) y Redsys. ClinicMate no almacena PAN.

RESUMEN

Toda factura emitida desde ClinicMate cumple Verifactu de origen. Todo dato personal se trata bajo RGPD con base jurídica documentada. Toda historia clínica se conserva al menos 5 años conforme a la Ley 41/2002. Ninguna marca registrada de medicamento sujeto a prescripción puede publicarse en canales públicos.

03

Verifactu — facturación electrónica

● RD 1007/2023 · OBLIGATORIO EN 2027

A partir del 1 de enero de 2027, todo empresario o profesional en España deberá emitir facturas mediante un sistema informático que cumpla con el Reglamento Verifactu. ClinicMate ya cumple, sin coste extra para el cliente.

Consecuencia de no cumplir

La AEAT podrá sancionar con **150 € por cada factura incorrecta** y hasta **50 000 € por cada ejercicio** a quienes utilicen un sistema no homologado. Para una clínica que emita ~100 facturas/mes, el riesgo anual supera fácilmente los **15 000 €**.

Cómo cumplimos

REQUISITO VERIFACTU	IMPLEMENTACIÓN EN CLINICMATE
Encadenado criptográfico	Cada factura referencia el hash SHA-256 de la anterior. Cualquier modificación rompe la cadena.
Tipos de factura	F1 (completa), F2 (simplificada, ≤ 3 000 €), R1 (rectificativa completa), R5 (rectificativa simplificada).
Envío a la AEAT	Automático en el momento de emisión. El acuse de recibo con CSV se almacena junto a la factura.
QR oficial	Generado en cada PDF según especificación AEAT. Permite la verificación pública por el receptor.
Flujo de fianzas	Doble factura — fianza inicial + factura final con línea de deducción — conforme a la consulta vinculante DGT V0091-24.
Retención	Mínimo 4 años desde la emisión, accesible incluso tras baja del servicio.
Inmutabilidad	Las facturas emitidas no se editan. Cualquier corrección genera una rectificativa (R1/R5) trazable.

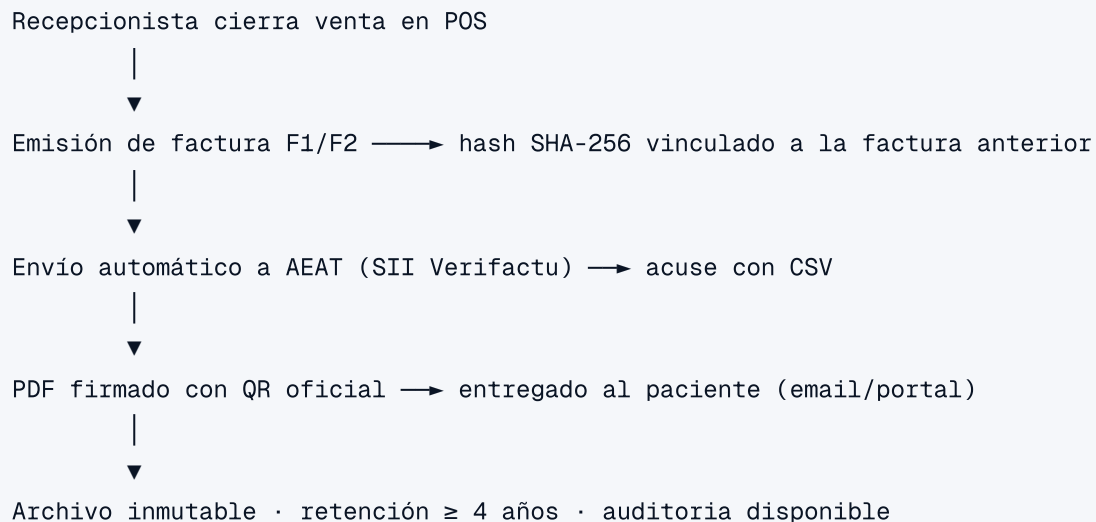
Series documentales

Series por defecto: `A-{año}-{secuencial}` para facturas, `R-{año}-{secuencial}` para rectificativas.
Configurables por clínica.

VENTAJA

Verifactu está incluido en todos los planes, también el Free. No es un módulo de pago aparte. No requiere instalación. No requiere cambio de gestoría. La clínica sigue facturando como hasta ahora; el sistema se encarga del cumplimiento.

Diagrama del flujo Verifactu



Casos especiales documentados

- **Fianza de booking** — al cobrar la fianza online se emite F1 de anticipo; al cerrar la cita se emite F1 final con línea negativa de deducción. Cumple consulta DGT V0091-24.
- **Anulación de cita** — si no se prestó el servicio, se anula la factura de fianza mediante R1 con motivo «anulación de operación».
- **Rectificación parcial** — la línea original queda intacta; se emite R1 con la corrección. Trazabilidad completa.
- **Bonos y packs** — emisión diferida: F1 al consumir cada sesión, no al vender el pack.

Verificación independiente

Cualquier persona — la AEAT, el cliente final, un inspector — puede verificar una factura escaneando el QR. La respuesta del servicio AEAT confirma o desmiente que la factura fue declarada por el emisor.

04 Sistema anti-marca — Ley 29/2006

● MULTAS DE HASTA 90 000 €

La Ley 29/2006 del Medicamento prohíbe la publicidad dirigida al público de medicamentos sujetos a prescripción y de sus marcas comerciales. La sanción puede alcanzar 90 000 € por publicar servicios con marcas registradas prohibidas. La Comunidad de Madrid sancionó a 58 clínicas estéticas entre 2020 y 2023 por este motivo.

Marcas afectadas

Forman parte de la lista interna 20+ marcas registradas activamente bloqueadas en canales públicos, entre ellas:

Botox · Vistabel · Azzalure · Bocouture

Juvederm · Restylane · Belotero · Teosyal

CoolSculpting · Morpheus8 · Ulthera · HIFU

Lista completa disponible bajo NDA y actualizada trimestralmente.

Arquitectura dual: nombre interno + nombre público

CONTEXTO	TRATAMIENTO
Uso interno Equipo, ficha de paciente, notas clínicas	Sin restricciones. El profesional puede escribir «Botox 30 UI en frontal» en su historia clínica. Es el lenguaje técnico del sector y no constituye publicidad.
Canales públicos Web, booking, WhatsApp, email automatizado, ticket	El sistema sustituye automáticamente al nombre genérico: «toxina botulínica», «ácido hialurónico», «criolipólisis». La marca registrada nunca abandona el dominio interno.

Aviso preventivo en formularios

Cuando un miembro del equipo escribe una marca bloqueada en un campo destinado a un canal público (nombre de servicio, descripción de la web, plantilla de WhatsApp), el sistema:

- Bloquea el guardado con un mensaje claro: «"Botox" es una marca registrada. La Ley 29/2006 impide publicitarla; usa "toxina botulínica".»
- Ofrece la alternativa segura preconfigurada.

3. Registra el intento en el log de auditoría, sin penalizar al usuario.

ADVERTENCIA LEGAL

El sistema anti-marca es una **capa de protección**, no un sustituto del criterio profesional. ClinicMate no presta asesoramiento legal y recomienda a la clínica disponer de protocolo propio y/o asesor especializado para campañas publicitarias.

05 Tratamiento de datos personales

El Cliente (la clínica) es el **Responsable del tratamiento**. ClinicMate actúa como **Encargado del tratamiento** en los términos del artículo 28 del RGPD, mediante Contrato de Tratamiento de Datos (DPA) firmado en el alta del servicio.

Categorías de datos tratados

CATEGORÍA	DATOS	BASE JURÍDICA
Identificativos	Nombre, DNI/NIE, teléfono, email, dirección, fecha de nacimiento	Ejecución de contrato · art. 6.1.b
Categorías especiales (salud)	Historia clínica, anamnesis, alergias, fotografías clínicas, prescripciones	Consentimiento explícito · art. 9.2.a · y Ley 41/2002
Económicos	Facturas, métodos de pago, importes, deudas pendientes	Obligación legal · art. 6.1.c · normativa fiscal
Comunicaciones	Emails, SMS, WhatsApp, conversaciones del chatbot	Ejecución de contrato e interés legítimo
Marketing	Segmentos, campañas, consentimientos comerciales	Consentimiento revocable · art. 6.1.a

Principios aplicados

- **Minimización** — se solicita exclusivamente lo necesario para cada finalidad. Los formularios son configurables por la clínica.
- **Exactitud** — el paciente puede actualizar sus datos desde el portal con magic link.
- **Limitación del plazo** — retención según norma (4 años fiscal, 5 años clínico mínimo). Anonimización al expirar.
- **Integridad y confidencialidad** — cifrado AES-256 en reposo y TLS 1.3 en tránsito (sección 8).
- **Responsabilidad proactiva** — registro de actividades, EIPD para tratamientos de alto riesgo, evaluación anual.

Segregación clínico ↔ fiscal

Los datos de salud **nunca** aparecen en facturas, recibos ni en cualquier documento de circulación fiscal. La factura describe el servicio en términos genéricos («tratamiento facial») sin diagnóstico ni producto sanitario asociado. Esta segregación protege al paciente frente a la divulgación accidental a contables, asesores fiscales o auditores.

06 Datos clínicos · Ley 41/2002

La Ley básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica establece obligaciones específicas sobre historia clínica, consentimiento informado y conservación documental.

Historia clínica

- **Estructura SOAP** — Motivo, Anamnesis, Exploración, Diagnóstico, Plan, Evolución.
- **Editor enriquecido** con anclas a sesiones previas y a la galería de fotos del paciente.
- **Flujo de estados** — Borrador → Completada → Firmada → Rectificada. La rectificación deja la versión original visible en histórico.
- **Firma digital del profesional y del paciente** conforme eIDAS, con sello de tiempo.
- **Trazabilidad de lotes** — cada producto inyectable consumido se registra con número de lote y caducidad, obligación de farmacovigilancia.

Consentimiento informado

El sistema detecta automáticamente cuando un servicio reservado requiere consentimiento (configurable por servicio) y desencadena el siguiente flujo:

1. Envío al paciente del enlace al formulario por email y SMS.
2. El paciente firma desde su móvil (sin login, magic link de un solo uso, validez 7 días).
3. Alternativa presencial: la recepción muestra un QR; el paciente lo escanea con su móvil y firma desde su dispositivo, o utiliza la tablet de la clínica.
4. El consentimiento firmado queda vinculado a la sesión clínica y a la versión exacta del texto del consentimiento (versionado inmutable).

Anamnesis con autocumplimentación

El cuestionario médico de 10 secciones (identificación, antecedentes, medicaciones y alergias, antecedentes ginecológicos cuando proceda, hábitos, dermatología, evaluación cutánea, antecedentes familiares, consentimientos, firma) se envía al paciente **antes de la primera cita** mediante magic link. Cuando el paciente llega a la clínica su ficha ya está completa, lo que reduce el tiempo medio de recepción en aproximadamente 15 minutos por paciente nuevo.

Retención y acceso del paciente

- Mínimo de 5 años desde el alta del proceso asistencial. Algunas comunidades autónomas exigen más (Cataluña 15 años, Galicia 5 años desde el alta); el sistema soporta la configuración por comunidad.
- El paciente puede solicitar copia de su historia clínica completa en formato PDF firmado mediante el portal o por solicitud al DPO.
- Tras baja del servicio, el cliente (clínica) puede exportar la totalidad de las historias clínicas en formato CSV + PDF para cumplir su obligación de conservación.

07 Hosting, localización y subprocesadores

Toda la infraestructura productiva de ClinicMate reside dentro del Espacio Económico Europeo. Ninguna transferencia internacional de datos fuera del EEE forma parte del flujo normal de operación.

Centro de datos primario y secundario

ROL	PROVEEDOR	UBICACIÓN	CERTIFICACIÓN
Producción	Hetzner Online GmbH	Helsinki (FI), Núremberg (DE)	ISO 27001 · ISO 9001
Réplica fría	Hetzner Online GmbH	Falkenstein (DE)	ISO 27001
CDN / almacenamiento	Bunny.net	EU edge (FR, DE, ES)	ISO 27001

Subprocesadores autorizados

SUBPROCESADOR	FINALIDAD	DATOS	UBICACIÓN
Hetzner Online GmbH	Hosting de aplicación y base de datos	Todos los datos productivos	UE
Stripe Payments Europe	Suscripciones y pagos online	Identificativos · pago	Irlanda
Redsys Servicios de Procesamiento	Pagos con tarjeta y fianzas	Identificativos · pago	España
Resend Inc.	Envío de email transaccional	Email · contenido	UE (region EU)
Meta Platforms Ireland Ltd.	WhatsApp Business API, Instagram DM	Mensajes · teléfono	Irlanda
Google Ireland Ltd.	Google Calendar, Maps, Business Reviews	Citas · ubicación	Irlanda
OpenAI Ireland Ltd.	Modelos LLM del chatbot	Conversaciones chatbot	Irlanda (DPA «zero retention»)

El listado actualizado de subprocesadores y sus cláusulas contractuales se publica en clanicmate.eu/subprocesadores. Los cambios se notifican con 30 días de antelación; el cliente puede oponerse y, si fuera incompatible con el servicio, rescindir sin penalización.

Transferencias internacionales

No se realizan transferencias internacionales de datos personales fuera del EEE en el flujo normal del servicio. Los subprocesadores indicados con sede en Irlanda son entidades intra-EEE. OpenAI Ireland procesa con DPA específico que excluye el reentrenamiento de modelos con los datos del cliente.

08

Cifrado, control de acceso y trazabilidad

Cifrado

ESTADO DEL DATO	PROTECCIÓN
En tránsito	TLS 1.3 con cifras AEAD (AES-GCM, ChaCha20-Poly1305). HSTS preload. Certificados gestionados automáticamente.
En reposo (BD)	AES-256 a nivel de disco (LUKS). Cifrado adicional por columna en datos especialmente sensibles (DNI, número de tarjeta sanitaria).
En reposo (archivos)	AES-256 server-side por objeto. Clave única por clínica derivada de KMS interno.
Backups	Cifrado AES-256 con clave distinta a la de producción. Almacenados en zona geográfica separada.
Tránsito interno	mTLS entre microservicios. Red privada virtual con segmentación por entorno.

Control de acceso basado en roles (RBAC)

El sistema implementa **42 permisos granulares** agrupados en 13 dominios (Agenda, Pacientes, Clínica, Consentimientos, Finanzas, Packs, Leads, Servicios, Inventario, Equipo, Configuración, Marketing, Informes) sobre **6 roles base**:

ROL	ALCANCE TÍPICO
Owner	Bypass de permisos. Único capaz de eliminar la cuenta.
Admin	Gestión completa salvo facturación y baja de servicio.
Staff	Operativa diaria, sin acceso a histórico financiero.
Profesional / Doctor	Historia clínica de sus pacientes. No accede a finanzas.
Recepcionista	Agenda, ficha básica, POS. Sin acceso a historia clínica.
Comercial	Leads, campañas. Sin acceso a datos clínicos.

Roles personalizados disponibles en plan Business y superior.

Autenticación

- Contraseñas con verificación contra repositorio de filtraciones conocidas (HIBP).
- **Segundo factor obligatorio** para roles Owner y Admin; opcional configurable para el resto.
- SSO SAML 2.0 disponible en plan Clinic.
- Sesiones de 12 h con renovación silenciosa. Bloqueo tras 5 intentos fallidos.

Log de auditoría

Toda acción sensible queda registrada con: usuario, rol, IP de origen, user-agent, timestamp UTC, recurso afectado, valor anterior, valor nuevo. El log es **inmutable** (append-only) y se conserva durante **5 años**. Está disponible para consulta del cliente desde el panel de administración y puede exportarse en formato CSV o JSON firmado.

09

Backups, continuidad y respuesta a incidentes

Política de backups

TIPO	FRECUENCIA	RETENCIÓN	UBICACIÓN
Backup incremental	Cada hora	30 días	Réplica fría (DE)
Snapshot diario completo	03:00 UTC	1 año	Réplica fría (DE)
Snapshot anual	Anual	5 años	Almacenamiento frío offline
Backup de configuración	Cada despliegue	90 días	Repositorio cifrado

Objetivos de continuidad

RTO

< 4 h

Tiempo máximo para restablecer el servicio tras una caída total.

RPO

< 1 h

Pérdida máxima de datos en escenario peor.

UPTIME OBJETIVO

99,9 %

Excluyendo ventanas de mantenimiento anunciadas.

Procedimiento de respuesta a incidentes

- Detección** — sistemas de monitorización 24/7, alertas a guardia de seguridad.
- Contención** — aislamiento del componente afectado, rotación de credenciales si procede.
- Evaluación** — clasificación de severidad y determinación si hay brecha de datos personales.
- Notificación al cliente** — comunicación al Responsable del tratamiento **en menos de 24 horas** desde el conocimiento de los hechos (mejor que el mínimo legal de 72 h del art. 33 RGPD).
- Notificación a la AEPD** — coordinada con el cliente cuando se cumplen los supuestos del art. 33 RGPD.
- Resolución y postmortem** — informe técnico al cliente. Medidas correctoras incorporadas al ciclo de mejora continua.

NOTIFICACIÓN REFORZADA

ClinicMate notifica al cliente **todo incidente que afecte a la disponibilidad o confidencialidad del servicio**, incluso cuando no haya brecha de datos personales — para que el cliente pueda informar proactivamente a su propio equipo y pacientes si lo considera oportuno.

Pruebas de recuperación

Trimestralmente se ejecuta un simulacro completo de restauración de backup en entorno aislado, verificando integridad y RTO real. El resultado de los simulacros está disponible bajo NDA.

10 Derechos del interesado

Los pacientes (interesados) pueden ejercer en cualquier momento los derechos reconocidos por el RGPD. ClinicMate ofrece herramientas para que la clínica (Responsable) atienda estas solicitudes en plazo.

DERECHO	CÓMO SE EJERCE	PLAZO DE RESPUESTA
Acceso	Solicitud al DPO de la clínica. Exportación con un clic desde el panel.	1 mes (ampliable 2 meses motivado)
Rectificación	El paciente puede modificar sus datos desde el portal con magic link.	Inmediato
Supresión («derecho al olvido»)	Anonimización irreversible de los datos identificativos. Se preserva la historia clínica anonimizada por obligación legal (Ley 41/2002).	1 mes
Limitación	Marcado del paciente como «restringido»: solo accesible por DPO y profesional asignado.	72 h
Portabilidad	Exportación en JSON y CSV con esquema documentado.	1 mes
Oposición	Revocación de consentimientos comerciales desde el portal o por solicitud.	Inmediato
No ser objeto de decisión automatizada	ClinicMate no toma decisiones jurídicas individualizadas mediante perfilado automatizado.	—

Reclamación a la autoridad de control

El interesado puede en cualquier momento presentar reclamación ante la Agencia Española de Protección de Datos (AEPD), www.aepd.es, sin perjuicio del derecho a obtener tutela judicial efectiva.

Petición al DPO de ClinicMate

Si el interesado considera que su solicitud no ha sido atendida por la clínica, puede contactar con el Delegado de Protección de Datos de ClinicMate en **dpo@clinicmate.eu**. Las solicitudes recibidas se reenvían al cliente correspondiente y se acompaña al interesado en su tramitación.

11 Pentests, auditorías y mejora continua

Pruebas de penetración externas

Anualmente se contrata a una empresa externa independiente para ejecutar un test de intrusión sobre el entorno productivo (caja gris). El alcance cubre la aplicación web, la API REST, la autenticación, los flujos de pago y los webhooks. Los hallazgos se priorizan según CVSS v3.1:

- **Crítico (9-10)** — corregido en ≤ 48 h.
- **Alto (7-8,9)** — corregido en ≤ 14 días.
- **Medio (4-6,9)** — corregido en ≤ 60 días.
- **Bajo (< 4)** — incorporado al backlog priorizado.

El informe ejecutivo del último pentest está disponible para clientes en planes Business y Clinic mediante NDA.

Programa de divulgación responsable

Aceptamos reportes de vulnerabilidades en security@clinicmate.eu con clave PGP publicada en clinicmate.eu/well-known/security.txt. Compromiso de respuesta inicial en 72 h. Reconocimiento público de investigadores con su autorización.

Revisión continua del código

- Análisis estático automático en cada pull request (SAST).
- Análisis de dependencias diario con alertas CVE.
- Revisión humana obligatoria por dos personas antes de despliegue a producción.
- Despliegue continuo con rollback automático ante anomalías.

Formación del equipo

Todo el personal de ClinicMate con acceso a sistemas productivos firma compromiso de confidencialidad y recibe formación obligatoria en protección de datos sanitarios, OWASP Top 10 e ingeniería social. La formación se renueva anualmente.

12 Matriz resumen de controles

Resumen consolidado de los controles aplicados, mapeados al estándar ISO/IEC 27002:2022 y al Esquema Nacional de Seguridad (ENS) categoría media.

ID	CONTROL	ISO 27002	IMPLEMENTACIÓN
C-01	Política de seguridad de la información	5.1	Documento interno revisado anualmente
C-02	Gestión de identidad y acceso	5.15 / 5.16	RBAC 42 permisos, MFA Owner/Admin
C-03	Clasificación de la información	5.12	Tres niveles: pública, interna, restringida (salud)
C-04	Cifrado de datos en reposo	8.24	AES-256 LUKS + columna sensible
C-05	Cifrado de datos en tránsito	8.24	TLS 1.3 obligatorio, HSTS preload
C-06	Gestión de claves criptográficas	8.24	KMS interno, rotación anual
C-07	Registro de actividades	8.15	Log inmutable, 5 años de retención
C-08	Gestión de vulnerabilidades	8.8	SAST en CI, escaneo dependencias diario
C-09	Pruebas de penetración	8.8	Pentest anual externo
C-10	Gestión de incidentes	5.24-5.28	Notificación cliente < 24 h
C-11	Continuidad de negocio	5.29 / 5.30	RTO 4 h, RPO 1 h, simulacros trimestrales
C-12	Copia de seguridad	8.13	Hourly + daily + yearly
C-13	Segregación de entornos	8.31	Dev / staging / pro aislados
C-14	Desarrollo seguro	8.25-8.28	Revisión 4 ojos, despliegue controlado
C-15	Concienciación del personal	6.3	Formación anual obligatoria
C-16	Gestión de proveedores	5.19-5.23	DPA firmado con todos los subprocesadores
C-17	Protección física	7.1-7.14	Delegada en CPD certificado ISO 27001

ID	CONTROL	ISO 27002	IMPLEMENTACIÓN
C-18	Protección frente a malware	8.7	Análisis automático de archivos subidos
C-19	Prevención de fuga de datos	8.12	Sistema anti-marca + segregación clínica/fiscal
C-20	Cumplimiento legal	5.31-5.36	Verifactu, RGPD, Ley 41/2002, Ley 29/2006

13 Contacto y aceptación

Delegado de Protección de Datos (DPO)

EMAIL	dpo@clinicmate.eu
POSTAL	ClinicMate Technologies S.L. — Att. DPO — Palma de Mallorca, Illes Balears, España
IDIOMAS	Español, catalán, inglés
PLAZO DE RESPUESTA	10 días hábiles

Seguridad y vulnerabilidades

EMAIL	security@clinicmate.eu
PGP	Publicado en clinicmate.eu/well-known/security.txt
RESPUESTA INICIAL	72 h

Estado del servicio

Página pública de estado en **status.clinicmate.eu** con histórico de los últimos 90 días.

Aceptación del cliente

La descarga de este dossier no constituye contrato. La relación jurídica se rige por las Condiciones Generales y el DPA aceptados al alta del servicio. Si desea constancia formal de recepción y archivo, complete y devuelva firmado el siguiente bloque:

RECEPCIÓN DEL DOSIER · USO INTERNO

NOMBRE Y FIRMA DEL RESPONSABLE DE LA
CLÍNICA

FECHA

CLÍNICA · RAZÓN SOCIAL

NIF

PRÓXIMA REVISIÓN

Este dossier se actualiza al menos una vez al año, o de forma extraordinaria cuando se produzca un cambio sustancial en la infraestructura, en los subprocesadores o en la normativa aplicable. La versión vigente está siempre disponible en clinicmate.eu/dossier-seguridad.