CIBER EN TACONES

Gobernanza y cumplimiento de IA

Riesgos, responsabilidades y controles para el uso de inteligencia artificial en el entorno sanitario.

CASO DE ESTUDIO SIMULADO

PYME SANITARIA MEDITERRÁNEA

Índice

1. Clasificación y fundamento del riesgo de IA....3

2. Responsabilidades del proveedor y del hospital....4

3. Análisis de conflictos entre RGPD y AI Act....5

4. Supervisión regulatoria y gestión de incidentes....8

5. Modelo operativo de AI Compliance....9

Perfil profesional — Gobernanza, riesgo y cumplimiento....11

Bibliografía....11

1. Clasificación y fundamento del riesgo de IA

Sistema: IA de apoyo al diagnóstico y triaje de pacientes. **Entidad:** PYME Sanitaria Mediterránea, hospital privado de 220 empleados. **Clasificación de gobernanza adoptada: ALTO RIESGO.**

El sistema puede influir en la valoración clínica y en la prioridad asistencial. La presencia de datos de salud (art. 9 RGPD) **no lo convierte, por sí sola, en IA de alto riesgo**: el encaje depende de su finalidad prevista y de las condiciones del art. 6 del Reglamento (UE) 2024/1689.

Análisis de los cuatro niveles del AI Act

Nivel	Conclusión y fundamento
Riesgo inaceptable · art. 5	No se identifican funciones prohibidas como puntuación social, manipulación ilícita o determinados usos biométricos.
ALTO RIESGO · art. 6	**Nivel de gobernanza asignado.** El Anexo III, 5.d, contempla el triaje sanitario **de urgencia**. El diagnóstico asistido puede ser alto riesgo bajo el art. 6.1 y el Anexo I si el software es producto sanitario y exige evaluación de conformidad por tercero.
Riesgo limitado · art. 50	Sus deberes de transparencia no reemplazan las exigencias del nivel alto cuando concurren sus presupuestos legales.
Riesgo mínimo	Sin obligaciones específicas por ese nivel; no se adopta porque el uso clínico requiere verificar los supuestos de alto riesgo.

Fundamento, límite y decisión

Dos vías legales distintas. Para el triaje, confirmar que se presta en urgencias (art. 6.2 y Anexo III, 5.d). Para el diagnóstico, obtener la finalidad prevista, clasificación como producto sanitario y modalidad de evaluación de conformidad (art. 6.1, Anexo I y Reglamento UE 2017/745). **El expediente no acredita todavía esos extremos**; no procede presentarlos como hechos.

Dirección: registrar AI-01 como alto riesgo a efectos preventivos y solicitar al fabricante la documentación que determine su clasificación jurídica definitiva antes de aprobar cambios o ampliaciones. La gestión incluirá supervisión humana, riesgos, registros y protección de datos clínicos.

Aplicación temporal vigente: tras el Reglamento (UE) 2026/1744, los requisitos del capítulo III, secciones 1–3, se aplican desde el **2-12-2027** para Anexo III y el **2-8-2028** para Anexo I, con las disposiciones transitorias que correspondan. Los controles propuestos anticipan ese cumplimiento; el RGPD sigue siendo exigible.

2. Responsabilidades del proveedor y del hospital

Rol asignado: DESPLEGADOR (art. 3.4 AI Act). El hospital usa la IA en su asistencia sanitaria y no consta que la desarrolle ni la comercialice bajo su marca. Dirección debe confirmarlo mediante contrato y ficha del producto; el proveedor externo aún no está identificado en la documentación.

Quién responde de qué

Proveedor: conformidad del producto	Hospital: utilización segura
Diseño y riesgos · arts. 9 y 10. Identifica peligros y documenta calidad y representatividad de datos de desarrollo.	**Instrucciones** · art. 26.1. Limita el uso a la finalidad y condiciones del fabricante; conserva instrucciones accesibles al equipo clínico.
Documentación · art. 11 y Anexo IV. Prepara expediente técnico, información de capacidades, límites y requisitos de supervisión (art. 14).	**Control clínico** · art. 26.2. Designa profesionales competentes que comprueben, corrijan o rechacen recomendaciones.
Conformidad · art. 16 y obligaciones aplicables de evaluación y registro. Acredita la conformidad antes de su puesta en servicio cuando sea exigible.	**Datos, registros y vigilancia** · arts. 26.4–26.6. Controla pertinencia de datos de entrada, conserva logs bajo su control y comunica riesgos e incidentes.

Cambio de rol: riesgo jurídico que debe evitarse

El art. 25 puede atribuir al hospital obligaciones de proveedor si pone su marca al sistema, introduce una modificación sustancial o altera la finalidad en los supuestos de la norma. **Cualquier adaptación clínica relevante exige revisión de GRC y del fabricante antes de producción.**

Decisión para Dirección

Solicitar identificación del proveedor, instrucciones y evidencia de conformidad aplicable; aprobar un protocolo de supervisión a cargo de Dirección Médica, custodia técnica de registros por Sistemas y control documental por Seguridad/GRC. El DPO asesorará y supervisará la dimensión de privacidad; **la responsabilidad de cumplir corresponde al hospital**, no al DPO.

Resultado esperado: proveedor responsable de la conformidad del sistema; hospital responsable de su uso autorizado, vigilancia, supervisión humana y gestión de datos. La contratación no traslada al fabricante las obligaciones del desplegador.

3. Análisis de conflictos entre RGPD y AI Act

Para AI-01 se examina **la tensión jurídica, su consecuencia asistencial y la medida verificable** que permite cumplir simultáneamente ambos marcos. No se atribuyen al hospital obligaciones de desarrollo que corresponden al proveedor.

Base jurídica y gobernanza de datos

Tensión. Los arts. 6 y 9 RGPD exigen legitimación para cada tratamiento de datos de salud. El art. 10 AI Act obliga al proveedor a gobernar sus datos de desarrollo; esa obligación **no crea una base legal** para reutilizar historias clínicas.

Caso. El RAT T01 documenta historia clínica y asistencia sanitaria con las bases del art. 6.1.b/c, según la operación, y art. 9.2.h para datos de salud. Introducir datos necesarios para apoyar la asistencia puede quedar comprendido en esa finalidad. **Ceder historiales al fabricante para reentrenamiento no queda legitimado automáticamente por T01.**

Control y evidencia. Antes de un tratamiento secundario, el hospital documentará finalidad, base del art. 6, excepción del art. 9, minimización y destinatarios; actualizará el RAT y evaluará EIPD y art. 28 cuando corresponda. El **DPO asesora**; Dirección autoriza o rechaza; GRC verifica documentación de proveedor. **Dictamen:** no ceder datos para mejorar modelos sin justificación y autorización documentadas.

Decisiones automatizadas y supervisión humana

Tensión. El art. 22 RGPD protege frente a decisiones exclusivamente automatizadas con efectos jurídicos o similarmente significativos, salvo excepciones. Los arts. 14 y 26.2 AI Act exigen supervisión humana; **una firma automática del profesional no evita por sí sola una decisión automatizada**. El art. 9.2.h RGPD tampoco constituye por sí solo excepción al art. 22.4.

Caso. Un triaje equivocado podría retrasar la atención de un paciente. Si el profesional acepta la prioridad sin poder contrastarla, la supervisión sería aparente.

Control y evidencia. Antes de decidir, el sanitario verifica los datos y la recomendación, puede corregir o rechazar el resultado y registra discrepancias relevantes. Dirección Médica designa supervisores y establece una alternativa asistencial ante fallo. GRC revisa las trazas y recurrencia de errores. **Dictamen:** ninguna recomendación se aplicará autónomamente cuando pueda afectar significativamente al paciente.

Calidad y representatividad frente a minimización

Tensión central. El art. 10.2–10.4 AI Act exige datos de entrenamiento, validación y prueba pertinentes, representativos y sometidos a controles de calidad. El art. 5.1.c RGPD exige tratar solo los datos personales necesarios para una finalidad. **Más datos no significan necesariamente mejores resultados y pueden multiplicar los riesgos de confidencialidad.**

Caso del hospital. AI-01 debe funcionar para los casos clínicos comprendidos en su finalidad. Si la herramienta ofrece peor rendimiento en determinados grupos de edad, patologías o situaciones de urgencia, una prioridad incorrecta puede comprometer la atención. Sin embargo, detectar ese sesgo no justifica entregar historias clínicas completas e identificables al proveedor.

Resolución operativa: calidad demostrable con mínima exposición

- **Definir la validación.** Dirección Médica documentará los grupos y tipos de casos relevantes, las variables necesarias y el criterio clínico de aceptación; no incluirá datos por mera disponibilidad.
- **Exigir pruebas al fabricante.** GRC solicitará documentación sobre representatividad, limitaciones, sesgos conocidos y rendimiento (arts. 10 y 13 AI Act), sin asumir el desarrollo ni exigir acceso irrestricto a conjuntos identificables.
- **Elegir datos proporcionales.** Para pruebas locales se usarán datos anónimos o sintéticos cuando mantengan utilidad clínica. Si se necesitan datos personales, se acotarán variables, accesos y conservación. La seudonimización **no elimina** la aplicación del RGPD.
- **Separar prueba de reentrenamiento.** Ningún dato usado para validar el servicio se destinará automáticamente a entrenar al proveedor; cada reutilización exigirá evaluación jurídica y contractual propia.
- **Vigilar resultados.** Dirección Médica revisará errores y diferencias de rendimiento clínicamente relevantes; si afectan a la seguridad, limitará o suspenderá el uso y abrirá acción correctiva documentada.

Límite reconocido. Los datos anónimos o sintéticos pueden ocultar grupos minoritarios o factores necesarios para detectar sesgos: no se prescriben en exclusiva. La medida correcta es **justificar cada categoría de datos y verificar que la validación sigue siendo representativa**. Las peticiones de supresión (art. 17 RGPD) se atenderán conforme al alcance del tratamiento y a las obligaciones de conservación clínica; no se promete un «desentrenamiento» automático.

Dictamen: aprobar únicamente conjuntos suficientes para un objetivo de validación concreto, con criterios clínicos, informe del proveedor y revisión de minimización por el DPO. **Evidencias:** protocolo de validación, informe de rendimiento, controles de acceso, registro de reutilizaciones y acciones correctivas.

Transparencia para pacientes y profesionales

Tensión. Los arts. 13–14 RGPD exigen explicar al paciente el tratamiento de sus datos. El art. 13 AI Act exige al **proveedor** ofrecer al hospital instrucciones y límites comprensibles. Cuando aplique el art. 26.11, el **desplegador** informará además a las personas afectadas de la utilización de determinados sistemas del Anexo III. Los destinatarios y finalidades informativas son distintos.

Caso. Un paciente debe conocer el apoyo de IA en el diagnóstico o triaje, sin recibir un manual técnico; el personal sanitario necesita entender cuándo confiar y cuándo apartarse de la recomendación.

Solución. Aprobar aviso breve en admisión y capa ampliada de privacidad, más instrucciones clínicas revisadas por Dirección Médica. **Aviso propuesto:** «En su atención podemos utilizar IA como apoyo al diagnóstico y al triaje. Sus recomendaciones son revisadas por profesionales sanitarios, responsables de las decisiones clínicas. Consulte nuestra información de privacidad para conocer cómo tratamos sus datos y ejercer sus derechos».

La información ampliada recogerá responsable, finalidad, base jurídica, destinatarios, conservación, derechos y contacto del DPO. **Evidencias:** texto aprobado, canal de publicación, instrucciones del proveedor y formación clínica.

Independencia del DPO y coordinación de AI Compliance

Tensión. Los arts. 37–39 RGPD garantizan independencia del DPO y evitan conflictos de intereses. El AI Act **no exige un puesto general reglado** denominado AI Compliance Officer. La coordinación puede integrarse en GRC, pero el DPO no debe convertirse en quien decide los fines y medios que después supervisa.

Caso. La revisión organizativa del hospital detectó funciones de DPO asumidas de hecho por el responsable de Sistemas, pese a intervenir en decisiones técnicas. Concentrar también AI Compliance en ese puesto intensificaría el conflicto.

Función	Responsabilidad concreta
Seguridad/GRC	Coordina clasificación y cumplimiento AI Act; mantiene expediente AI-01, controles y evidencias.
DPO independiente	Asesora y supervisa legitimación, EIPD, transparencia y derechos, sin decidir la operación.
Dirección Médica y Sistemas	La primera dirige supervisión asistencial; Sistemas administra accesos, cambios y registros.
Dirección	Aprueba usos, recursos y respuesta ante riesgos no aceptables.

Dictamen integrado: separar supervisión independiente y ejecución. GRC reportará a Dirección, el DPO conservará acceso directo y las decisiones quedarán en actas y matriz de responsabilidades. Estas cinco áreas se gestionarán con **autorizaciones, controles y pruebas**, no con declaraciones de cumplimiento.

4. Supervisión regulatoria y gestión de incidentes

AI-01 implica dos planos de supervisión: seguridad y cumplimiento del sistema de IA, y licitud y protección de los historiales clínicos. **La autoridad de vigilancia de IA depende del encaje regulatorio definitivo; la AEPD mantiene sus competencias sobre datos personales.**

Autoridad competente según la clasificación acreditada

Supuesto	Supervisión y criterio
Triaje de urgencias · Anexo III, 5.d	Autoridad de vigilancia del AI Act dentro de la distribución nacional de competencias, con **AESIA como autoridad de referencia general**; comprobar la designación aplicable al sistema.
Diagnóstico como producto sanitario · art. 6.1, Anexo I	Autoridad sectorial de vigilancia conforme al **art. 74.3 AI Act**; en España debe examinarse la competencia de **AEMPS** y la normativa de productos sanitarios.
Datos personales de pacientes	**AEPD:** legitimidad, confidencialidad, EIPD, derechos y brechas (arts. 33–34, 51–58 RGPD).

Protocolo dual ante un incidente

Supuesto de control: la IA asigna una prioridad asistencial incorrecta y se descubre además acceso indebido a la historia clínica. Dirección Médica contendrá el riesgo; Sistemas preservará pruebas; GRC y DPO abrirán **dos evaluaciones paralelas**, sin presumir que todo fallo clínico es incidente grave ni que todo incidente implica brecha.

Vía	Actuación, obligado y plazo
IA de alto riesgo · arts. 26.5 y 73	El **hospital** comunica **inmediatamente** el incidente grave al proveedor y después, cuando proceda, a importador/distribuidor y autoridad de vigilancia. El **proveedor** notifica formalmente en cuanto concurran las condiciones legales: máximo general **15 días**, **10** si hay fallecimiento y **2** en los supuestos del art. 73.3. Sin contacto con el proveedor, se aplica al hospital el art. 73 por remisión. Para productos sanitarios, verificar art. 73.10 y régimen sectorial.
Datos personales · arts. 33–34 RGPD	El **hospital** notifica a la **AEPD sin dilación indebida y, si es posible, dentro de 72 horas** desde el conocimiento, salvo improbabilidad de riesgo; si el riesgo es alto, informa también a los pacientes sin dilación indebida.

Decisión para Dirección: aprobar un expediente único de incidentes con dos hojas de decisión y destinatarios propios; **GRC coordina IA, el DPO asesora y supervisa privacidad, y el hospital presenta las notificaciones RGPD**. Registrar hora de detección, valoración, autoridad, responsable, aviso enviado y justificante.

5. Modelo operativo de AI Compliance

Objetivo operativo: integrar el cumplimiento AI Act en Seguridad/GRC sin crear un departamento paralelo. La Dirección aprobará los usos y recursos; Dirección Médica asumirá el control asistencial y el DPO mantendrá su supervisión independiente de privacidad.

Inventario y expediente de control

ID	Sistema y uso	Nivel / datos	Proveedor	Responsable
AI-01	Apoyo al diagnóstico y triaje	**Alto** (gobernanza); salud	**Identificación por acreditar**	Dirección Médica

GRC custodiará la ficha AI-01: finalidad prevista, versión, proveedor, clasificación legal acreditada, documentación de conformidad, instrucciones, tratamiento T01, riesgos, registros, revisiones y decisiones. El alcance del expediente comprende solo AI-01; cualquier otro uso exigirá su propia autorización.

Gobierno y decisión

Responsable	Función ejecutiva y evidencia
Consejo Directivo	Autoriza política, recursos, restricciones y cambios relevantes; acta de aprobación.
Seguridad/GRC	Coordina AI Compliance, comprobaciones y proveedores; expediente y reporte de desviaciones.
Dirección Médica	Define uso clínico, supervisores y respuesta asistencial; protocolo y registros.
Sistemas	Gestiona permisos, versiones y trazas; resultados de pruebas y alertas.
DPO independiente	Asesora y supervisa RAT, EIPD y derechos; informes sin asumir decisiones operativas.

El **Comité de Seguridad existente** examinará AI-01 trimestralmente y ante incidentes, con acuerdos, responsable y fecha de cierre. GRC elevará inmediatamente los riesgos clínicos o regulatorios que no puedan esperar a esa reunión.

Circuito operativo: activación, comprobación y prueba

Activación / quién	Qué se comprueba y qué se hace	Evidencia
Antes de poner en servicio o modificar · GRC, clínica y DPO	Finalidad y versión, clasificación, instrucciones, conformidad y legitimación de datos. **Si falta un requisito esencial, no autorizar.**	Ficha AI-01 y aprobación.
Cada recomendación · profesional clínico	Contrastar la propuesta con el caso del paciente; corregir o rechazar; ante riesgo, usar circuito alternativo y avisar.	Decisión y discrepancias relevantes.

Activación / quién	Qué se comprueba y qué se hace	Evidencia
En operación · Sistemas	Verificar generación, integridad y acceso a logs; investigar falta de trazas, errores y accesos anómalos; escalar alertas sin resolver.	Monitorización y cierre.
Fallo clínico · Dirección Médica	Valorar daño y pacientes afectados; contener o suspender si procede; activar circuito de notificación con GRC y DPO.	Incidente y decisiones.
Cambio de versión o finalidad · Sistemas/GRC	Detener puesta en producción hasta revisar impacto en clasificación, contrato, riesgos, privacidad y supervisión.	Cambio autorizado.
Cierre mensual · GRC/Clínica	Consolidar discrepancias, incidentes y desviaciones de rendimiento; asignar corrección, responsable y plazo; verificar su eficacia.	Informe y acciones.

Control reforzado por evidencia previa. En la auditoría simulada del Centro 1 se detectó una modificación de historia clínica que no generaba la traza exigida. **Antes de autorizar AI-01**, Sistemas probará que resultados, usuario, hora y revisión clínica dejan registros verificables; no se presume que AI-01 padezca ese mismo fallo. Conservar los logs automáticos bajo control del hospital **al menos seis meses**, salvo plazo legal diferente (art. 26.6 AI Act).

Integración de controles existentes

SGSI, Centro 1: vincular AI-01 a accesos y permisos (A.5.15), registro (A.8.15) y monitorización (A.8.16), sin extender de oficio el perímetro definido del SGSI a otros centros. **RGPD:** asociar AI-01 al RAT T01; el hospital decidirá cambios de finalidad, contratación de encargados y EIPD con asesoramiento del DPO.

Política y terceros: permitir solo el uso clínico autorizado; prohibir datos de pacientes en herramientas externas no aprobadas. Exigir al proveedor instrucciones, evidencias de conformidad, límites, soporte, gestión de incidentes y cláusulas de tratamiento de datos cuando correspondan. **ISO/IEC 42001** será referencia voluntaria de mejora, sin presumir certificación.

Implantación: hitos internos desde la aprobación de Dirección

Hito	Entrega verificable y responsable
Día 10	Designación de GRC; expediente AI-01 abierto. **Dirección/GRC.**
Día 30	Identidad y documentación del proveedor contrastadas; ficha y condiciones de autorización revisadas. **GRC/DPO/Clínica.**
Día 60	Supervisión humana, pruebas de trazabilidad, incidencias y escalado aprobados. **Clínica/Sistemas.**
Día 90; meses 6, 9 y 12	Primer reporte al Comité y revisiones con cierre verificado de acciones. **GRC/Comité.**

Decisión para el Consejo Directivo: aprobar responsables y política, exigir la ficha AI-01 y las pruebas de supervisión y trazabilidad antes del uso o cambio autorizado. Estos hitos son **plazos de implantación propuestos**, no plazos legales del AI Act.

Perfil profesional — Gobernanza, riesgo y cumplimiento

Gobernanza, riesgos y cumplimiento | Inteligencia artificial

Mi perfil combina conocimientos de automatización con inteligencia artificial y formación especializada en **Gobierno, Riesgo y Cumplimiento (GRC)**. Me interesa ayudar a las organizaciones a utilizar estas tecnologías con responsabilidades definidas, riesgos controlados y respeto por la privacidad.

He construido un **caso continuo sobre un mismo hospital simulado**, desarrollando distintas capas de gobierno: análisis de riesgos con MAGERIT, SGSI ISO 27001, protección de datos, auditoría interna, cumplimiento integrado y gobernanza de IA conforme al AI Act y al RGPD.

Este trabajo acredita competencias vinculadas a cuatro salidas profesionales: **GRC Analyst**, en evaluación de riesgos y controles; **Auditor de Sistemas de Información**, en contraste de evidencias y hallazgos; **DPO**, en obligaciones y garantías de privacidad; y **AI Compliance Officer**, en clasificación regulatoria, supervisión y controles de cumplimiento.

Busco oportunidades en GRC y cumplimiento de inteligencia artificial, aportando una perspectiva que conecta tecnología, datos y normativa con decisiones útiles y verificables para las organizaciones.

Bibliografía

UE (2024). Reglamento (UE) 2024/1689 (AI Act), texto consolidado. EUR-Lex
UE (2026). Reglamento (UE) 2026/1744, modificación y calendario del AI Act. EUR-Lex
UE (2016). Reglamento (UE) 2016/679 (RGPD). EUR-Lex
UE (2017). Reglamento (UE) 2017/745, productos sanitarios. EUR-Lex
España (2023). Real Decreto 729/2023, Estatuto de AESIA. BOE
AEPD (2020). Adecuación al RGPD de tratamientos que incorporan IA. AEPD
AEPD (2021). Gestión del riesgo y evaluación de impacto. AEPD
ISO/IEC (2022). ISO/IEC 27001:2022, SGSI. ISO
ISO/IEC (2023). ISO/IEC 42001:2023, sistema de gestión de IA. ISO