# Inteligencia artificial en la empresa biotecnológica europea: clasificación jurídica, obligaciones de conformidad y modelo de gobernanza bajo el Reglamento (UE) 2024/1689

## De la investigación *in silico* al diagnóstico, la fabricación avanzada y la inteligencia artificial generativa

*José M. López, BSc, MD, PhD et al.*

*Departamento Técnico y Científico de ND Pharma - Intabiotech*

**Resumen**

La inteligencia artificial se ha incorporado con especial intensidad a las empresas biotecnológicas, farmacéuticas, de diagnóstico, de dispositivos médicos, de nutrición avanzada y de fabricación biológica. Su utilización abarca desde el descubrimiento de moléculas, el cribado virtual, la predicción de estructuras proteicas y la selección de biomarcadores hasta la interpretación de datos ómicos, esto es, *conjuntos masivos de información molecular biológica que incluyen disciplinas como la genómica, transcriptómica, proteómica y metabolómica*, la estratificación de pacientes, la automatización de procesos fermentativos, el control de calidad, la vigilancia poscomercialización y la generación de documentación científica o regulatoria.

Esta expansión tecnológica coincide con la entrada progresiva en aplicación del Reglamento (UE) 2024/1689, conocido como Reglamento Europeo de Inteligencia Artificial o *AI Act*. La nueva norma no regula la inteligencia artificial como una categoría tecnológica homogénea, sino atendiendo a la función desempeñada por cada sistema, su finalidad prevista, su integración en productos sometidos a legislación armonizada, las personas afectadas y la magnitud de los riesgos para la salud, la seguridad y los derechos fundamentales.

El presente trabajo analiza la aplicación del Reglamento a la empresa biotecnológica desde una perspectiva técnico-jurídica. Se examinan la delimitación entre investigación científica y explotación operacional, la clasificación de los sistemas de alto riesgo, la interacción con los Reglamentos de productos sanitarios y diagnóstico *in vitro*, la normativa farmacéutica, el Reglamento General de Protección de Datos, el Espacio Europeo de Datos de Salud, la ciberseguridad, la responsabilidad por productos defectuosos y el régimen de inteligencia artificial de propósito general. En el presente trabajo, se sostiene que el cumplimiento no puede reducirse a una declaración de principios éticos ni a la adquisición contractual de herramientas supuestamente conformes. Mucho más allá, exige inventariar los sistemas, fijar su finalidad prevista, distribuir formalmente responsabilidades, controlar los datos y modelos, validar su rendimiento en el contexto real de uso, mantener supervisión humana efectiva, documentar cambios y establecer vigilancia poscomercialización o posdespliegue.La tesis central es que, en biotecnología, el riesgo jurídico de la inteligencia artificial no depende únicamente de la sofisticación del algoritmo, sino de su capacidad para condicionar decisiones científicas, clínicas, industriales, laborales o comerciales. Por ello, una gobernanza madura debe integrar el Reglamento de Inteligencia Artificial con los sistemas de calidad, validación, gestión de riesgos, protección de datos, farmacovigilancia, tecnovigilancia y ciberseguridad ya existentes en la organización.

***Palabras clave:*** *inteligencia artificial; biotecnología; Reglamento (UE) 2024/1689; productos sanitarios; diagnóstico in vitro; medicamentos; datos genéticos; gobernanza algorítmica; sistemas de alto riesgo; cumplimiento regulatorio.*

## 1. Introducción: la inteligencia artificial como infraestructura decisoria de la biotecnología

La inteligencia artificial ha dejado de ser una herramienta experimental periférica para convertirse en una infraestructura transversal de la empresa biotecnológica. Los modelos algorítmicos intervienen hoy en la identificación de dianas terapéuticas, el diseño molecular, la ingeniería de proteínas, el análisis genómico, la interpretación de imágenes, la optimización de ensayos, la selección de pacientes, la predicción de estabilidad, la automatización de cultivos celulares, el control de bioprocesos y la elaboración de documentación técnica.

Sin embargo, desde el punto de vista jurídico, el afirmar que una empresa *«utiliza inteligencia artificial»* aporta muy poca información, y se configura como un extremo que debe ser analizado de manera profunda. La cuestión jurídicamente relevante es determinar qué función cumple el sistema, con qué grado de autonomía opera, sobre qué datos ha sido entrenado, cuál es su finalidad prevista, quién controla sus resultados, qué personas pueden verse afectadas y si el sistema forma parte de un producto sujeto a evaluación de conformidad.

El Reglamento (UE) 2024/1689 establece un marco horizontal destinado a promover una inteligencia artificial centrada en el ser humano y fiable, garantizando al mismo tiempo un elevado nivel de protección de la salud, la seguridad y los derechos fundamentales. Su ámbito de aplicación comprende tanto a los proveedores que introducen sistemas o modelos en el mercado europeo como a los responsables del despliegue establecidos en la Unión y, en determinadas circunstancias, a operadores de terceros países cuando el resultado producido por el sistema se utiliza en territorio europeo.

La regulación adopta un enfoque graduado. No todas las aplicaciones de inteligencia artificial están sometidas a idénticas obligaciones. La norma distingue, esencialmente, entre prácticas prohibidas, sistemas de alto riesgo, sistemas sujetos a obligaciones específicas de transparencia, modelos de inteligencia artificial de propósito general y aplicaciones que, aun siendo lícitas, permanecen sujetas a la legislación sectorial, contractual, laboral, de protección de datos, propiedad intelectual, ciberseguridad o responsabilidad civil. Y sucede que en la empresa biotecnológica, esta arquitectura regulatoria se superpone a un entorno ya altamente normativizado. Un mismo sistema puede quedar sometido simultáneamente al Reglamento de Inteligencia Artificial, al Reglamento General de Protección de Datos, a la normativa sobre medicamentos, productos sanitarios o diagnóstico *in vitro*, a las buenas prácticas de fabricación, laboratorio o clínica, a las reglas de ensayos clínicos, a la legislación de ciberseguridad y a las normas sobre responsabilidad por productos defectuosos.

La consecuencia esencial es el carácter acumulativo, y no sustitutivo, de estos regímenes. La conformidad con el Reglamento de Inteligencia Artificial no convierte automáticamente en lícito el tratamiento de datos personales ni acredita el cumplimiento de la normativa sanitaria. De igual modo, la certificación de un producto sanitario no exonera de las obligaciones específicamente algorítmicas relativas a datos, transparencia, supervisión humana, robustez o seguimiento poscomercialización.

## 2. La singularidad regulatoria de la inteligencia artificial biotecnológica

La biotecnología presenta características que intensifican los riesgos de la inteligencia artificial.

En primer lugar, trabaja frecuentemente con datos de alta dimensionalidad: secuencias genómicas, transcriptómica, proteómica, metabolómica, microbiomas, imágenes histopatológicas, registros clínicos, datos de laboratorio, señales fisiológicas y parámetros de fabricación. La complejidad matemática de estos conjuntos de datos puede crear una apariencia de objetividad que no siempre se corresponde con su calidad científica.

En segundo lugar, los datos biomédicos presentan importantes problemas de representatividad. Una cohorte limitada geográfica, étnica, clínica o socioeconómicamente puede

generar modelos aparentemente precisos en validación interna, pero incapaces de generalizar a poblaciones distintas. Los sesgos pueden originarse en la selección de pacientes, los criterios diagnósticos, la disponibilidad de muestras, la práctica clínica previa, la instrumentación utilizada o la propia estructura del sistema sanitario.

En tercer lugar, el resultado algorítmico puede insertarse en decisiones de elevada trascendencia: diagnóstico, pronóstico, elegibilidad para un tratamiento, diseño de un ensayo clínico, liberación de un lote, modificación de un proceso de fabricación o determinación de la seguridad de un producto.

En cuarto lugar, muchos sistemas biotecnológicos evolucionan. Pueden ser reentrenados, recalibrados o adaptados a nuevos conjuntos de datos. Esta capacidad de cambio genera una tensión evidente con los modelos regulatorios tradicionales, construidos en torno a productos definidos y versiones técnicamente delimitadas.

Finalmente, las empresas dependen a menudo de terceros: proveedores de modelos fundacionales, servicios de computación en nube, plataformas bioinformáticas, bases de datos externas, laboratorios contratados y desarrolladores especializados. La cadena de suministro algorítmica puede dificultar el acceso a la información necesaria para demostrar la conformidad.

La Agencia Europea de Medicamentos ha subrayado que los riesgos asociados a la inteligencia artificial deben valorarse atendiendo al contexto de uso y al grado de influencia que el sistema ejerce sobre las decisiones, y no únicamente a la tecnología empleada. También ha atribuido a promotores, fabricantes y titulares de autorizaciones la responsabilidad de garantizar que los algoritmos, modelos, conjuntos de datos y procesos utilizados sean adecuados para su finalidad, científicamente sólidos, legalmente admisibles y compatibles con las buenas prácticas aplicables.

## 3. Calendario de aplicación y situación normativa a 11 de julio de 2026

El Reglamento (UE) 2024/1689 entró en vigor el 1 de agosto de 2024. Su aplicación se articula progresivamente. Las disposiciones generales y las prácticas prohibidas comenzaron a aplicarse el 2 de febrero de 2025. Las reglas sobre modelos de inteligencia artificial de propósito general, gobernanza y determinadas sanciones comenzaron a aplicarse el 2 de agosto de 2025. Conforme al texto actualmente publicado, la aplicación general se produce el 2 de agosto de 2026, mientras que determinadas obligaciones relativas a sistemas de alto riesgo integrados en productos regulados se proyectaron inicialmente hasta el 2 de agosto de 2027.

Esta exposición requiere, no obstante, una precisión temporal importante. El 7 de mayo de 2026, el Consejo y el Parlamento Europeo alcanzaron un acuerdo político provisional dentro del denominado paquete *Digital Omnibus*. El acuerdo prevé desplazar la aplicación de los requisitos correspondientes a sistemas de alto riesgo del anexo III al 2 de diciembre de 2027 y la de los sistemas vinculados a productos del anexo I al 2 de agosto de 2028.

A la fecha de cierre de este artículo, el acuerdo provisional todavía debe ser formalmente adoptado por el Parlamento Europeo y el Consejo y publicado como *norma modificativa*. El procedimiento legislativo figura aún como pendiente en EUR-Lex. Por consiguiente, las fechas del Reglamento vigente conservan formalmente su eficacia hasta que la modificación sea aprobada y publicada, aunque las empresas deben considerar el calendario 2027-2028 como el escenario regulatorio políticamente más probable. Esta situación no justifica paralizar los programas de cumplimiento. Las obligaciones de alfabetización en inteligencia artificial se encuentran ya vigentes; las prohibiciones son plenamente aplicables; las obligaciones relativas a modelos de propósito general están operativas; y la construcción de expedientes técnicos, sistemas de calidad, procesos de validación y estructuras contractuales exige normalmente meses o años.

## 4. El concepto jurídico de sistema de inteligencia artificial y la necesidad de delimitar el objeto regulado

El Reglamento define el sistema de inteligencia artificial como un sistema basado en máquinas diseñado para funcionar con distintos niveles de autonomía y que, a partir de las entradas recibidas, infiere cómo generar resultados tales como predicciones, contenidos, recomendaciones o decisiones capaces de influir en entornos físicos o virtuales. Pero esta definición no comprende cualquier programa informático. Un cálculo determinista basado exclusivamente en reglas fijas, sin capacidad inferencial relevante, puede quedar fuera del concepto. Tampoco todo análisis estadístico convencional debe calificarse automáticamente como inteligencia artificial.

La delimitación debe realizarse atendiendo a la arquitectura real, y no al nombre comercial. Las empresas deben evitar dos errores contrapuestos:

1. **Sobreclasificación:** tratar como inteligencia artificial cualquier automatización, hoja de cálculo, sistema de control o programa estadístico.
2. **Infraclasificación:** presentar como simple programa de apoyo una herramienta que aprende de datos, produce recomendaciones individualizadas o modifica de forma material una decisión humana.

La correcta delimitación exige documentar, al menos, las entradas, los métodos de inferencia, los resultados generados, la autonomía funcional, la capacidad de adaptación, el entorno de uso y la influencia efectiva sobre las decisiones.

Debe distinguirse, además, entre el modelo matemático, el sistema completo y el producto final. Un modelo fundacional adquirido a un tercero puede ser solo un componente. El sistema regulado puede incluir interfaces, reglas de procesamiento, bases de conocimiento, mecanismos de recuperación documental, controles humanos y conexiones con otros equipos. La evaluación jurídica debe recaer sobre el sistema desplegado en su contexto real.

**5. La exclusión de la investigación científica: alcance y límites**

El Reglamento excluye de su ámbito los sistemas y modelos desarrollados y puestos en servicio *exclusivamente para fines de investigación y desarrollo científicos*. También excluye, con determinados límites, las *actividades de investigación, ensayo y desarrollo* realizadas antes de la introducción del sistema en el mercado o de su puesta en servicio. La exclusión no alcanza a los ensayos en condiciones reales, y las restantes normas de la Unión -entre ellas las de protección de datos, ensayos clínicos o bioética- continúan siendo aplicables.

Esta exclusión debe interpretarse restrictivamente. No convierte a un departamento de investigación en una zona exenta de derecho. Para que resulte aplicable es necesario que la finalidad sea genuinamente científica y que el sistema no haya sido introducido en el mercado ni utilizado operacionalmente para adoptar decisiones con efectos reales. Por ejemplo, un modelo empleado únicamente para explorar relaciones entre variables moleculares en un proyecto interno podría encontrarse dentro de la exclusión. Pero la situación cambia cuando el resultado se utiliza para seleccionar pacientes, liberar lotes, recomendar tratamientos, determinar la continuación de un programa clínico o prestar un servicio a terceros.

La frontera entre investigación y despliegue se vuelve especialmente problemática en los denominados sistemas de aprendizaje continuo. Una empresa puede alegar que sigue «experimentando» con un sistema que, en realidad, ya interviene en operaciones ordinarias. La etiqueta de prototipo no prevalece sobre el uso efectivo.

En consecuencia, toda organización debería definir formalmente:

- cuándo un proyecto se encuentra en fase exploratoria;
- qué restricciones impiden utilizar sus resultados en decisiones reales;
- qué criterios determinan el paso a validación;
- quién autoriza el despliegue;

- qué documentación debe completarse antes de ese despliegue;
- cómo se separan los entornos de desarrollo, ensayo y producción.

La ausencia de estas barreras favorece el denominado *shadow deployment*: herramientas experimentales utilizadas de hecho por científicos, técnicos o directivos sin evaluación regulatoria ni autorización formal.

## 6. Sujetos responsables: proveedor, responsable del despliegue y cadena de valor

El régimen de obligaciones depende del papel que desempeña la empresa.

### 6.1. Proveedor

Es proveedor quien desarrolla un sistema de inteligencia artificial —o encarga su desarrollo— y lo introduce en el mercado o lo pone en servicio bajo su nombre o marca. Una empresa biotecnológica puede ser proveedor, aunque no comercialice software de forma independiente. Bastará con que integre el sistema en un producto o servicio propio y lo ofrezca bajo su denominación.

También puede convertirse en proveedor quien:

- coloque su nombre o marca en un sistema ya comercializado;
- modifique sustancialmente un sistema;
- cambie la finalidad prevista de un sistema de manera que pase a considerarse de alto riesgo.

Estas reglas impiden eludir responsabilidades mediante contratos que designen formalmente al desarrollador externo como único responsable. La distribución contractual de riesgos puede producir efectos entre las partes, pero no modifica por sí sola la calificación regulatoria.

### 6.2. Responsable del despliegue

Es responsable del despliegue quien utiliza el sistema bajo su autoridad, salvo cuando se emplea en una actividad personal no profesional.

La mayoría de las empresas biotecnológicas serán responsables del despliegue respecto de herramientas adquiridas para selección de personal, análisis de datos, optimización industrial, vigilancia regulatoria, redacción asistida o atención al cliente.

Sus obligaciones incluyen utilizar el sistema conforme a las instrucciones, asignar la supervisión a personas competentes, controlar la pertinencia de los datos de entrada, vigilar el funcionamiento y suspender el uso cuando existan riesgos razonables.

### 6.3. Importador y distribuidor

Las empresas que introduzcan en la Unión sistemas procedentes de terceros países o los distribuyan también deben verificar determinados elementos de conformidad, documentación, marcado e identificación del proveedor.

### 6.4. Proveedor de modelos de propósito general

Las entidades que desarrollan modelos de propósito general deben elaborar documentación técnica, proporcionar información a los proveedores que los incorporan a otros sistemas, establecer una política de respeto de los derechos de autor y publicar un

resumen suficientemente detallado del contenido utilizado para el entrenamiento. Los modelos que presenten riesgo sistémico soportan obligaciones adicionales de evaluación, mitigación, notificación y ciberseguridad.

La empresa biotecnológica usuaria de un modelo fundacional normalmente no será proveedor del modelo, pero sí puede convertirse en proveedor del sistema final construido sobre él.

## 7. Clasificación jurídica de los sistemas utilizados en biotecnología

La clasificación no depende de que la tecnología sea innovadora, compleja o costosa. Depende de su finalidad prevista, su función y su contexto de uso.

### 7.1. Prácticas prohibidas

El artículo 5 prohíbe determinadas prácticas consideradas incompatibles con los valores de la Unión. Entre ellas se incluyen técnicas manipuladoras o engañosas capaces de alterar sustancialmente la conducta y causar perjuicios significativos, la explotación de vulnerabilidades, determinadas modalidades de puntuación social, la creación de bases de reconocimiento facial mediante extracción indiscriminada de imágenes y, salvo excepciones médicas o de seguridad, la inferencia de emociones en el lugar de trabajo.

En una empresa biotecnológica pueden plantearse riesgos, por ejemplo, cuando se utilizan sistemas de análisis facial o vocal para inferir emociones, compromiso, estrés o sinceridad de empleados y candidatos. Una herramienta comercializada como sistema de «bienestar laboral» no deja de estar prohibida si su verdadera función consiste en inferir estados emocionales en el trabajo y no concurre una excepción legítima de carácter médico o de seguridad.

También serían problemáticos los sistemas diseñados para explotar vulnerabilidades asociadas a una enfermedad, discapacidad o situación socioeconómica con fines comerciales, especialmente cuando se dirigen a pacientes o consumidores.

### 7.2. Sistemas de alto riesgo integrados en productos regulados

Un sistema se considera de alto riesgo por la vía del artículo 6.1 cuando concurren cumulativamente dos condiciones:

1. que constituya un componente de seguridad de un producto regulado por la legislación del anexo I o sea él mismo uno de esos productos; y
2. que el producto deba someterse a una evaluación de conformidad por un tercero antes de su introducción en el mercado o puesta en servicio.

El anexo I incluye expresamente el Reglamento (UE) 2017/745 sobre productos sanitarios y el Reglamento (UE) 2017/746 sobre productos sanitarios para diagnóstico *in vitro*.

Entendido lo anterior, hay que reseñar que no toda inteligencia artificial médica es automáticamente de alto riesgo. Es necesario comprobar la clasificación del producto y si requiere intervención de un organismo notificado. Un software médico de clase I sin intervención de un tercero podría no entrar por esta vía, aunque seguiría sometido al Reglamento de productos sanitarios, al RGPD y a otras obligaciones.

Por el contrario, un sistema que interprete imágenes para detectar lesiones, calcule un riesgo clínico, determine la presencia de un biomarcador o clasifique resultados genómicos

puede ser alto riesgo cuando forme parte de un producto sanitario o diagnóstico *in vitro* sujeto a evaluación de conformidad por un organismo notificado.

### 7.3. Sistemas de alto riesgo del anexo III

El anexo III contempla usos determinados en ámbitos como empleo, educación, acceso a servicios esenciales, aplicación de la ley, migración o administración de justicia.

En la empresa biotecnológica, la categoría más frecuente será la relativa al empleo. Los sistemas utilizados para reclutar, seleccionar, filtrar candidaturas, evaluar candidatos, asignar tareas, adoptar decisiones sobre promoción o terminación, o vigilar y evaluar el rendimiento de los trabajadores pueden ser considerados de alto riesgo.

El Reglamento permite que ciertos sistemas incluidos formalmente en el anexo III no se consideren de alto riesgo cuando no presenten un riesgo significativo para la salud, la seguridad o los derechos fundamentales y se limiten a tareas procedimentales, preparatorias o de apoyo muy restringido. La excepción debe justificarse y documentarse. Además, un sistema que realice perfiles de personas físicas se considera siempre de alto riesgo dentro de estos supuestos.

### 7.4. Inteligencia artificial en medicamentos y descubrimiento de fármacos

Los medicamentos no están incluidos, como tales, en la lista de productos del anexo I del Reglamento de Inteligencia Artificial. Por consiguiente, un modelo utilizado en descubrimiento de moléculas, predicción toxicológica o diseño de ensayos no se convierte automáticamente en sistema de alto riesgo por la vía del artículo 6.1.

Esta conclusión no equivale a una ausencia de regulación. El uso puede quedar sometido a la normativa farmacéutica, a las buenas prácticas de laboratorio, clínica o fabricación y a los requisitos de integridad, trazabilidad y validación de datos.

La Agencia Europea de Medicamentos ha señalado que la inteligencia artificial puede afectar a la seguridad del paciente, la integridad de los estudios y la evaluación de la relación beneficio-riesgo. Los titulares, promotores y fabricantes deben gestionar los riesgos desde el desarrollo inicial hasta la retirada o desmantelamiento del sistema y solicitar interacción regulatoria temprana cuando su uso pueda influir de manera significativa en la evaluación del medicamento.

### 7.5. Sistemas de control industrial

Un sistema utilizado para controlar un biorreactor, una línea de producción o una instalación puede ser de alto riesgo cuando actúe como componente de seguridad de una máquina u otro producto del anexo I y concurra la exigencia de evaluación por terceros.

Si su función se limita a optimizar productividad o eficiencia, sin controlar funciones de seguridad, puede quedar fuera de la categoría de alto riesgo. No obstante, si su resultado afecta a parámetros críticos de calidad, esterilidad, potencia, pureza o liberación de lotes, deberá ser validado conforme a la normativa sectorial y al sistema de calidad de la empresa.

### 7.6. Sistemas sujetos a transparencia

El artículo 50 impone obligaciones específicas en determinados supuestos. Las personas deben ser informadas cuando interactúan directamente con un sistema de

inteligencia artificial, salvo que resulte evidente por las circunstancias. Los proveedores deben permitir la identificación en formato legible por máquina de los contenidos sintéticos. Los sistemas de reconocimiento de emociones o categorización biométrica deben ser objeto de información específica. Los contenidos manipulados o artificiales que constituyan *deepfakes* deben revelarse como tales.

No existe, sin embargo, una obligación general de declarar públicamente que cualquier texto empresarial ha recibido asistencia de inteligencia artificial. La transparencia debe analizarse conforme al supuesto concreto. Un informe científico, material comercial o artículo de interés público generado o alterado sustancialmente por inteligencia artificial puede exigir especial cautela, sobre todo si no existe revisión humana ni responsabilidad editorial efectiva.

## 8. Obligaciones esenciales aplicables a los sistemas de alto riesgo

### 8.1. Gestión continua de riesgos

El artículo 9 exige un sistema de gestión de riesgos continuo, iterativo y mantenido durante todo el ciclo de vida. No se trata de elaborar una matriz inicial y archivarla. La organización debe identificar riesgos conocidos y previsibles, valorar usos indebidos razonablemente previsibles, analizar la información procedente del seguimiento poscomercialización y adoptar medidas de mitigación.

En biotecnología, la evaluación debería abarcar, entre otros:

- falsos positivos y falsos negativos;
- errores de clasificación clínica;
- sesgos poblacionales;
- deriva de datos y de concepto;
- utilización fuera de la población validada;
- degradación del rendimiento por cambios instrumentales;
- errores de interoperabilidad;
- automatización excesiva de la decisión;
- vulnerabilidades de ciberseguridad;
- extracción o reconstrucción de datos sensibles;
- uso adversarial de modelos biológicos;
- consecuencias de una indisponibilidad del sistema;
- impacto de reentrenamientos y actualizaciones.

La aceptabilidad del riesgo debe vincularse a criterios previamente establecidos. No basta con afirmar que el modelo «funciona bien». Deben definirse métricas, umbrales, intervalos de confianza, poblaciones, condiciones de exclusión y consecuencias de los errores.

### 8.2. Gobernanza de datos

El artículo 10 exige que los conjuntos de datos de entrenamiento, validación y prueba se sometan a prácticas apropiadas de gobernanza. Estas deben comprender el origen de los datos, su obtención, preparación, limpieza, etiquetado, formulación de supuestos, evaluación de su disponibilidad, adecuación y representatividad, análisis de posibles sesgos y detección de lagunas.

Los conjuntos de datos deben ser pertinentes, suficientemente representativos y, en la medida de lo posible, estar libres de errores y ser completos para la finalidad prevista. Deben considerar las características geográficas, contextuales o conductuales específicas del entorno en el que el sistema será utilizado.

En biomedicina, la representatividad no debe confundirse con el tamaño. Un conjunto masivo de datos procedentes de una única institución, plataforma analítica o población puede ser menos generalizable que otro más pequeño, pero adecuadamente estratificado.

Así, la separación entre datos de entrenamiento, validación y prueba resulta esencial. La Agencia Europea de Medicamentos ha advertido sobre el riesgo de fugas de información entre conjuntos, sobreajuste, validación insuficiente y pérdida de generalización. También recomienda conservar registros trazables y disponer de información suficiente sobre modelos suministrados por terceros. Y finalmente, decir que el artículo 10.5 permite, con carácter excepcional, tratar categorías especiales de datos personales para detectar y corregir sesgos cuando sea estrictamente necesario y se apliquen garantías adecuadas. Esta disposición no constituye una autorización general para utilizar datos de salud, genéticos o biométricos. Debe existir, además, una base jurídica válida conforme al RGPD y cumplirse los principios de necesidad, minimización y seguridad.

### 8.3. Documentación técnica y trazabilidad

El proveedor debe disponer de documentación técnica suficiente antes de introducir el sistema en el mercado o ponerlo en servicio. La documentación debe permitir demostrar el cumplimiento y proporcionar a las autoridades la información necesaria para evaluar el sistema.

La trazabilidad debe abarcar:

- versiones del modelo y del código;
- fuentes y versiones de los conjuntos de datos;
- criterios de inclusión y exclusión;
- transformaciones realizadas;
- parámetros e hiperparámetros;
- resultados de validación;
- limitaciones conocidas;
- cambios introducidos;
- incidentes y desviaciones;
- decisiones de aprobación;
- responsables de cada etapa.

El Reglamento exige conservar determinada documentación durante diez años. Los registros generados automáticamente deben mantenerse, por regla general, durante un período adecuado a la finalidad y no inferior a seis meses cuando estén bajo el control del proveedor, salvo que otra normativa disponga un plazo distinto.

En entornos GxP, estos plazos pueden verse superados por las obligaciones sectoriales de conservación. La regla prudente consiste en aplicar el período más exigente y documentar la política de retención.

### 8.4. Transparencia e instrucciones de uso

Los sistemas de alto riesgo deben diseñarse de modo que su funcionamiento sea suficientemente transparente para permitir al responsable del despliegue interpretar los resultados y utilizarlos adecuadamente.

Las instrucciones deben incluir, entre otros elementos:

- identidad y datos del proveedor;
- finalidad prevista;

- nivel de precisión y métricas relevantes;
- limitaciones conocidas;
- grupos o situaciones respecto de los cuales puede disminuir el rendimiento;
- riesgos previsibles;
- requisitos de datos de entrada;
- medidas de supervisión humana;
- recursos computacionales necesarios;
- mantenimiento y actualización;
- mecanismos de registro.

La explicación debe ser funcional. No es necesario revelar todos los detalles matemáticos del modelo, pero sí proporcionar información suficiente para comprender cuándo resulta fiable, cuándo no debe utilizarse y qué consecuencias puede tener un error.

**8.5. Supervisión humana**

La supervisión humana no consiste en colocar a una persona al final del proceso para ratificar automáticamente el resultado. Debe ser real, competente y materialmente capaz de alterar la decisión.

El supervisor debe:

- comprender las capacidades y limitaciones del sistema;
- detectar anomalías y sesgos;
- evitar una confianza automática en los resultados;
- interpretar correctamente las salidas;
- decidir no utilizar el sistema;
- ignorar, revertir o interrumpir su funcionamiento;
- activar procedimientos de escalado.

En una aplicación clínica, la supervisión debería recaer en profesionales con competencia clínica y formación específica sobre el sistema. En fabricación, deberá corresponder a personal capaz de comprender tanto el proceso como el significado de la predicción algorítmica.

Cuando el volumen, la velocidad o la complejidad del sistema hacen imposible revisar efectivamente las decisiones, la mera presencia formal de un humano no cumple la finalidad de la norma.

**8.6. Precisión, robustez y ciberseguridad**

Los sistemas de alto riesgo deben alcanzar niveles adecuados de precisión, robustez y ciberseguridad y mantenerlos durante todo su ciclo de vida.

La ciberseguridad algorítmica excede la protección convencional de redes. Incluye:

- envenenamiento de datos;
- manipulación de etiquetas;
- ejemplos adversariales;
- extracción del modelo;
- inversión del modelo;
- reconstrucción de datos de entrenamiento;
- secuestro de interfaces;
- inyección de instrucciones;
- contaminación de bases documentales;

- exfiltración de información mediante respuestas generadas;
- alteración de modelos o parámetros;
- ataques a la cadena de suministro.

La robustez debe verificarse en condiciones que reproduzcan razonablemente el entorno real. Un modelo preciso sobre datos históricos perfectamente curados puede fallar en presencia de ruido, datos incompletos, cambios instrumentales o variaciones poblacionales.

### 8.7. Sistema de gestión de la calidad

Los proveedores de sistemas de alto riesgo deben establecer un sistema de gestión de la calidad documentado. Este debe abarcar estrategia de cumplimiento, diseño, desarrollo, verificación, validación, gestión de datos, gestión de riesgos, seguimiento poscomercialización, comunicación con autoridades, gestión documental, recursos y responsabilidades.

Las empresas sometidas al Reglamento de productos sanitarios, al Reglamento de diagnóstico *in vitro* o a buenas prácticas farmacéuticas no deberían construir un sistema paralelo e inconexo. El artículo 17 permite integrar los requisitos en sistemas de calidad ya existentes.

En términos prácticos, una empresa podría incorporar el gobierno de inteligencia artificial a su sistema ISO 13485, GMP o equivalente mediante:

- procedimientos específicos de clasificación;
- control de datos y modelos;
- validación algorítmica;
- gestión de cambios;
- calificación de proveedores;
- revisión periódica;
- gestión de desviaciones;
- auditoría;
- vigilancia;
- acciones correctivas y preventivas.

### 8.8. Evaluación de conformidad y marcado

Antes de introducir un sistema de alto riesgo en el mercado, el proveedor debe someterlo al procedimiento de evaluación de conformidad aplicable, emitir la declaración UE de conformidad, colocar el marcado CE cuando proceda y registrar el sistema.

Cuando la inteligencia artificial forme parte de un producto sanitario o de diagnóstico *in vitro*, la evaluación debe articularse con el procedimiento sectorial correspondiente. La finalidad es evitar duplicidades, pero no reducir el alcance de la comprobación.

### 8.9. Seguimiento poscomercialización e incidentes

El proveedor debe establecer un sistema de seguimiento poscomercialización proporcional a la naturaleza del sistema y sus riesgos. Debe recopilar y analizar de forma activa y sistemática datos sobre rendimiento durante toda la vida útil.

Los incidentes graves deben notificarse a la autoridad competente, normalmente en un plazo máximo de quince días desde que se establece la relación causal o resulta razonablemente probable. Existen plazos más breves para determinados incidentes críticos y para aquellos que causen la muerte.

En biotecnología, la vigilancia debería integrar:

- quejas de usuarios;
- discrepancias entre resultado y referencia;
- errores de laboratorio;
- eventos clínicos;
- desviaciones de proceso;
- cambios en la prevalencia;
- cambios en dispositivos de medición;
- alertas de ciberseguridad;
- degradación estadística;
- resultados de auditorías.

## 9. Interacción con el Reglamento General de Protección de Datos

### 9.1. Datos genéticos, biométricos y de salud

Los datos genéticos, biométricos destinados a identificar de manera unívoca y los datos relativos a la salud constituyen categorías especiales de datos. Su tratamiento requiere una base jurídica del artículo 6 del RGPD y una excepción válida a la prohibición del artículo 9.

El consentimiento no es la única base posible ni siempre la más adecuada. En investigación clínica, asistencia sanitaria, salud pública o cumplimiento de obligaciones legales pueden resultar aplicables otras bases, sujetas a condiciones específicas.

La empresa debe distinguir entre:

- base jurídica del tratamiento;
- finalidad científica o asistencial;
- compatibilidad de usos posteriores;
- anonimización real;
- seudonimización;
- transferencias internacionales;
- plazos de conservación;
- derechos de los interesados;
- decisiones automatizadas.

### 9.2. Un modelo entrenado con datos personales no es necesariamente anónimo

La Opinión 28/2024 del Comité Europeo de Protección de Datos rechaza que un modelo entrenado con datos personales pueda considerarse automáticamente anónimo. La evaluación debe realizarse caso por caso, atendiendo a la probabilidad de extraer, reconstruir o inferir información relativa a personas concretas. Esta advertencia es especialmente relevante para modelos genómicos. La información genética posee una capacidad identificativa extraordinaria y está relacionada biológicamente con familiares del interesado. Eliminar nombres o identificadores directos no convierte necesariamente el conjunto en anónimo.

### 9.3. Evaluación de impacto

El uso de inteligencia artificial sobre datos genéticos, clínicos o biométricos exigirá frecuentemente una evaluación de impacto relativa a la protección de datos, especialmente

cuando implique nuevas tecnologías, tratamiento a gran escala, perfiles, decisiones automatizadas o monitorización sistemática.

La evaluación debe preceder al despliegue y coordinarse con la gestión de riesgos del Reglamento de Inteligencia Artificial. No son documentos intercambiables. La evaluación de impacto del RGPD se centra en los derechos y libertades de las personas; el sistema de gestión de riesgos del *AI Act* incluye también salud, seguridad, rendimiento y uso indebido.

### 9.4. Decisiones automatizadas

El artículo 22 del RGPD protege frente a decisiones basadas únicamente en tratamientos automatizados que produzcan efectos jurídicos o afecten significativamente de modo similar. La excepción aparente consistente en introducir una revisión humana carece de eficacia cuando la persona se limita a aceptar sistemáticamente el resultado. La intervención debe ser significativa, informada y capaz de modificar la decisión.

### 9.5. Espacio Europeo de Datos de Salud

El Reglamento (UE) 2025/327 crea el Espacio Europeo de Datos de Salud y establece una estructura común para el uso primario y secundario de datos sanitarios. Su desarrollo puede facilitar el acceso regulado a datos para investigación, innovación y entrenamiento de sistemas, pero no elimina las exigencias del RGPD ni autoriza una reutilización indiscriminada.

Los proyectos deberán respetar las finalidades autorizadas, los permisos de acceso, los entornos seguros de tratamiento, las prohibiciones de uso y las garantías frente a una eventual re-identificación.

## 10. Productos sanitarios y diagnóstico *in vitro*

La inteligencia artificial puede formar parte de un producto sanitario, constituir software médico independiente o integrarse en un dispositivo físico.

La calificación depende de la finalidad prevista declarada por el fabricante. Un software destinado a proporcionar información utilizada para tomar decisiones diagnósticas o terapéuticas puede constituir un producto sanitario. Un sistema destinado al examen *in vitro* de muestras humanas para obtener información sobre estados fisiológicos, patológicos, predisposición, compatibilidad o respuesta terapéutica puede quedar comprendido en el Reglamento de diagnóstico *in vitro*.

La finalidad prevista no puede redactarse de forma artificialmente limitada para evitar una clasificación superior cuando las funciones, materiales comerciales o instrucciones revelan un uso más amplio.

### 10.1. Integración de evaluaciones

La documentación debería coordinar:

- clasificación como producto sanitario o IVD;
- clasificación como sistema de IA de alto riesgo;
- gestión de riesgos conforme a la normativa de producto;
- gestión de riesgos algorítmicos;
- evaluación clínica o del rendimiento;
- validación analítica;

- usabilidad;
- ciberseguridad;
- vigilancia poscomercialización;
- control de modificaciones.

### 10.2. Cambios y aprendizaje continuo

Un cambio en el modelo puede alterar el rendimiento, la finalidad o el perfil de riesgo. Debe existir una política que distinga:

- mantenimiento sin impacto clínico;
- recalibración;
- reentrenamiento;
- incorporación de nuevas variables;
- ampliación de población;
- cambio de indicación;
- cambio sustancial.

No debe permitirse que un sistema desplegado aprenda autónomamente de datos reales y modifique su comportamiento sin un mecanismo de control, validación y liberación de versiones.

### 10.3. Evidencia clínica

La validación algorítmica no sustituye la evaluación clínica. Una elevada sensibilidad o especificidad en un conjunto de prueba no acredita por sí sola utilidad clínica.

Deben analizarse:

- población diana;
- prevalencia;
- comparador;
- estándar de referencia;
- diseño prospectivo o retrospectivo;
- centros participantes;
- variabilidad interobservador;
- valores predictivos;
- calibración;
- utilidad clínica;
- consecuencias de los errores;
- generalización.

## 11. Medicamentos, ensayos clínicos y buenas prácticas

El uso de inteligencia artificial en medicamentos debe analizarse desde la perspectiva del ciclo de vida completo: descubrimiento, desarrollo no clínico, ensayos clínicos, fabricación, autorización, farmacovigilancia y seguimiento.

### 11.1. Descubrimiento y diseño molecular

Los modelos pueden priorizar dianas, generar estructuras, estimar afinidad, predecir toxicidad o proponer nuevas indicaciones. Aunque estos usos no sean automáticamente de alto riesgo conforme al *AI Act*, deben documentarse suficientemente cuando sus resultados influyan en decisiones regulatorias.

Una empresa debería poder explicar:

- de dónde proceden los datos;
- qué criterios de calidad se aplicaron;
- qué sesgos pueden contener;
- cómo se validaron las predicciones;
- qué incertidumbre existe;
- qué comprobación experimental se realizó;
- qué parte de la decisión correspondió al modelo.

### 11.2. Ensayos clínicos

La inteligencia artificial puede utilizarse para selección de centros, reclutamiento, estratificación, identificación de criterios de inclusión, análisis de imágenes, monitorización remota o detección de señales.

Los riesgos incluyen exclusión discriminatoria de participantes, introducción de sesgos en la muestra, pérdida de representatividad, decisiones automatizadas no transparentes y afectación de la integridad del estudio.

Cuando una herramienta determine la elegibilidad de pacientes, la empresa debe asegurar validación en la población diana, trazabilidad, revisión humana y mecanismos para detectar exclusiones incorrectas.

### 11.3. Fabricación y control de calidad

Los modelos de mantenimiento predictivo, control multivariable, detección de anomalías, visión artificial y liberación paramétrica pueden mejorar la eficiencia, pero también comprometer atributos críticos de calidad.

En entornos regulados, el sistema debe evaluarse conforme a un enfoque basado en riesgos y a los principios de integridad de datos. Debe existir evidencia documentada de que:

- el sistema es adecuado para su uso;
- los datos de entrada son fiables;
- los resultados son reproducibles;
- los accesos están controlados;
- los cambios son autorizados;
- los registros son íntegros;
- las excepciones se revisan;
- existe capacidad de recuperación;
- la supervisión humana es efectiva.

### 11.4. Farmacovigilancia

La inteligencia artificial puede identificar señales en informes espontáneos, literatura, redes sociales o bases de datos clínicas. Su uso puede reducir cargas, pero los errores de clasificación pueden omitir señales o generar falsos positivos.

El sistema no debería cerrar automáticamente casos relevantes ni descartar señales sin criterios validados y revisión competente. La responsabilidad en el área de farmacovigilancia permanece en el titular. La Agencia Europea de Medicamentos considera prioritario reforzar la alfabetización en inteligencia artificial, la evaluación de riesgos y la capacidad regulatoria en su plan de trabajo 2026-2028.

## 12. Inteligencia artificial generativa en la empresa biotecnológica

La inteligencia artificial generativa merece un análisis específico porque su facilidad de uso puede ocultar riesgos relevantes.

### 12.1. Usos admisibles

Puede utilizarse para:

- búsqueda y síntesis documental;
- preparación de borradores;
- traducción;
- estructuración de informes;
- generación de código;
- elaboración de materiales formativos;
- apoyo a consultas internas;
- exploración de hipótesis.

### 12.2. Riesgos característicos

Los principales riesgos son:

- invención de datos o referencias;
- atribución incorrecta de fuentes;
- omisión de información crítica;
- revelación de secretos empresariales;
- tratamiento ilícito de datos personales;
- incorporación de contenidos protegidos;
- contaminación de documentos regulados;
- automatización acrítica;
- persistencia de información en servicios externos;
- vulnerabilidades por inyección de instrucciones;
- extracción de datos a través de bases de conocimiento conectadas.

### 12.3. Documentación regulatoria

La generación de borradores de expedientes técnicos, procedimientos normalizados, informes clínicos, respuestas a autoridades o evaluaciones de riesgos puede ser legítima. No obstante, el modelo no debe actuar como autor autónomo ni como fuente de evidencia.

Toda afirmación técnica debe verificarse contra la fuente primaria. Las referencias deben comprobarse individualmente. Los cálculos, unidades, límites, tablas y conclusiones deben revisarse por personal competente.

La empresa debería prohibir expresamente:

- introducir datos clínicos identificables en herramientas no autorizadas;
- cargar formulaciones o procesos confidenciales sin garantías contractuales;
- utilizar referencias no verificadas;
- aprobar automáticamente documentos GxP;
- modificar procedimientos mediante salidas generativas sin control de cambios;
- presentar contenido generado como evidencia experimental.

### 12.4. Sistemas de recuperación aumentada

Los sistemas que combinan modelos generativos con bases documentales internas pueden reducir errores, pero no los eliminan. La organización debe controlar:

- documentos autorizados;
- versiones vigentes;
- permisos de acceso;
- segmentación de información;
- trazabilidad de las fuentes;
- actualización de índices;
- eliminación de documentos obsoletos;
- resistencia a instrucciones maliciosas;
- registro de consultas y respuestas.

La respuesta generada debe citar el documento exacto y permitir que el usuario acceda a la fuente original.

**13. Propiedad intelectual, secretos empresariales y datos de terceros**

El uso de modelos externos plantea problemas de propiedad intelectual y confidencialidad. Antes de contratar un servicio deben examinarse al menos las siguientes áreas o extremos:

- titularidad de entradas y salidas;
- utilización de datos para reentrenamiento;
- conservación de instrucciones;
- sub-encargados;
- localización de servidores;
- transferencias internacionales;
- garantías de eliminación;
- derechos de auditoría;
- responsabilidad por infracción;
- continuidad del servicio;
- acceso a documentación;
- restricciones de exportación.

La introducción de secuencias, formulaciones, resultados experimentales, protocolos, expedientes de patentes o estrategias clínicas en una herramienta pública puede comprometer su consideración como secreto empresarial y afectar a la novedad patentable.

El Reglamento exige a los proveedores de modelos de propósito general establecer una política de respeto de la legislación europea sobre derechos de autor, incluidas las reservas formuladas por los titulares frente a la minería de textos y datos.

Estas obligaciones del proveedor no sustituyen la diligencia del usuario empresarial. La empresa debe verificar que dispone de derechos suficientes sobre los datos introducidos y que el resultado no reproduce indebidamente material protegido.

**14. Ciberseguridad, continuidad y resiliencia operacional**

La inteligencia artificial debe integrarse en la estrategia general de ciberseguridad.

La Directiva NIS2 establece obligaciones reforzadas para determinadas entidades esenciales e importantes. El Reglamento de Ciber-resiliencia introduce requisitos horizontales para productos con elementos digitales. Su aplicación concreta dependerá de la naturaleza de la empresa, el producto y la actividad.

Una evaluación específica debería considerar:

- dependencia de servicios externos;

- indisponibilidad del proveedor;
- manipulación de modelos;
- pérdida de datos;
- credenciales comprometidas;
- ataques a interfaces;
- vulnerabilidades de bibliotecas;
- cambios no comunicados;
- degradación del servicio;
- fallos de conectividad;
- capacidad de operar manualmente.

En procesos críticos debe existir un plan de contingencia. La organización debe saber qué ocurrirá si el sistema no está disponible, devuelve resultados incoherentes o debe suspenderse de inmediato.

El riesgo de concentración merece particular atención. Una empresa puede depender de un único proveedor de nube, modelo, base de datos o plataforma bioinformática. Esta dependencia debe analizarse desde la continuidad de negocio, portabilidad, interoperabilidad y recuperación.

**15. Responsabilidad civil y contractual**

El cumplimiento administrativo no elimina la responsabilidad civil, antes al contrario, pues ya desde la Directiva (UE) 2024/2853 sobre responsabilidad por productos defectuosos se incluye el software dentro del concepto de producto y adapta el régimen a los productos digitales y a las actualizaciones. El perjudicado deberá demostrar, con las reglas y presunciones aplicables, el defecto, el daño y la relación causal.

La propuesta de Directiva específica sobre responsabilidad en materia de inteligencia artificial fue retirada formalmente en 2025. Por tanto, no existe actualmente una directiva europea autónoma de responsabilidad civil por IA equivalente al Reglamento de Inteligencia Artificial.

Ello no crea un vacío. Pues pueden resultar aplicables:

- responsabilidad por productos defectuosos;
- responsabilidad contractual;
- responsabilidad extracontractual;
- responsabilidad profesional;
- responsabilidad sanitaria;
- normativa de consumo;
- normativa laboral;
- regímenes sectoriales de productos sanitarios y medicamentos.

Los contratos con proveedores tecnológicos deben distribuir responsabilidades, pero no deben contener una confianza ilusoria en cláusulas genéricas. Estos deberían regular:

- finalidad autorizada;
- documentación de conformidad;
- niveles de servicio;
- métricas de rendimiento;
- acceso a registros;
- gestión de cambios;
- notificación de incidentes;
- seguridad;
- subcontratación;
- auditoría;

- cooperación regulatoria;
- indemnidad;
- terminación;
- devolución o eliminación de datos;
- continuidad y migración.

Una cláusula según la cual el proveedor no garantiza la exactitud de las salidas puede ser incompatible con el uso de la herramienta en decisiones críticas. Si no existe garantía suficiente, la conclusión no debe ser simplemente aceptar el riesgo, sino limitar o prohibir el caso de uso.

**16. Alfabetización en inteligencia artificial**

El artículo 4 obliga a proveedores y responsables del despliegue a adoptar medidas para garantizar un nivel suficiente de alfabetización en inteligencia artificial de su personal y de otras personas que operen los sistemas por cuenta de la organización. La formación debe adaptarse a los conocimientos, experiencia, contexto y personas afectadas. Esta obligación se aplica desde el 2 de febrero de 2025.

La alfabetización no equivale a una sesión genérica sobre ventajas y riesgos. Debe estructurarse por funciones.

El consejo de administración y la alta dirección necesitan comprender:

- exposición regulatoria;
- asignación de responsabilidades;
- riesgos estratégicos;
- recursos necesarios;
- consecuencias sancionadoras;
- impacto reputacional.

El personal científico y técnico necesita formación en:

- calidad de datos;
- sesgos;
- validación;
- generalización;
- reproducibilidad;
- trazabilidad;
- incertidumbre.

Los usuarios operativos deben saber:

- para qué puede utilizarse el sistema;
- cuando no debe utilizarse;
- cómo interpretar resultados;
- cómo detectar anomalías;
- cuando escalar;
- cómo informar de incidentes.

Los departamentos: jurídico, de calidad, regulatorio, protección de datos y ciberseguridad deben comprender tanto la tecnología como su integración en los sistemas de cumplimiento. La formación debe documentarse, actualizarse y evaluarse. La asistencia a un curso no demuestra por sí sola competencia.

**17. Modelo de gobernanza para la empresa biotecnológica**

Una organización madura debería implantar un sistema de gobernanza algorítmica proporcional a su actividad.

### 17.1. Política corporativa

La política debe definir principios, ámbito, responsabilidades y usos prohibidos. Debe ser aprobada por la alta dirección y aplicarse a sistemas desarrollados internamente, adquiridos, integrados o utilizados informalmente.

### 17.2. Inventario de sistemas

El inventario debería contener:

- nombre y versión;
- propietario interno;
- proveedor;
- finalidad prevista;
- usuarios;
- personas afectadas;
- datos utilizados;
- integración con otros sistemas;
- papel regulatorio de la empresa;
- clasificación de riesgo;
- base jurídica de datos;
- estado de validación;
- fecha de aprobación;
- fecha de revisión;
- incidentes;
- dependencia de terceros.

No puede gobernarse lo que no se conoce. Deben incluirse herramientas gratuitas, complementos, cuentas individuales y automatizaciones creadas por empleados.

### 17.3. Clasificación previa

Antes de adquirir o desarrollar un sistema debe realizarse una clasificación preliminar que responda, como mínimo, a las siguientes preguntas:

1. ¿Es jurídicamente un sistema de inteligencia artificial?
2. ¿Se encuentra excluido por investigación científica?
3. ¿incurre en una práctica prohibida?
4. ¿forma parte de un producto del anexo I?
5. ¿requiere evaluación de conformidad por terceros?
6. ¿está incluido en el anexo III?
7. ¿realiza perfiles?
8. ¿está sujeto a transparencia?
9. ¿utiliza un modelo de propósito general?
10. ¿trata datos personales o categorías especiales?
11. ¿afecta a decisiones clínicas, industriales, laborales o comerciales?
12. ¿qué normativa sectorial resulta aplicable?

### 17.4. Comité multidisciplinar

La evaluación no debe quedar exclusivamente en manos del departamento informático. Deben participar, según el caso:

- dirección;
- investigación y desarrollo;
- calidad;
- asuntos regulatorios;
- clínico o médico;
- protección de datos;
- jurídico;
- ciberseguridad;
- recursos humanos;
- propiedad intelectual;
- fabricación;
- farmacovigilancia o tecnovigilancia.

El comité debe tener autoridad para condicionar, limitar o rechazar proyectos.

**17.5. Gestión de proveedores**

La evaluación del proveedor debe abarcar como mínimo:

- identidad y solvencia;
- papel conforme al Reglamento;
- documentación técnica;
- certificaciones;
- datos de entrenamiento;
- métricas;
- limitaciones;
- historial de incidentes;
- procesos de actualización;
- seguridad;
- subcontratistas;
- acceso a registros;
- cooperación en auditorías;
- estrategia de salida.

Las declaraciones comerciales de «IA ética», «cumplimiento europeo» o «modelo privado» no deben aceptarse sin evidencia.

**17.6. Validación basada en contexto**

La validación debe realizarse sobre el caso de uso concreto. El rendimiento publicado por el proveedor no sustituye la validación local.

Debe comprobarse:

- población o proceso real;
- representatividad;
- calidad de entradas;
- métricas relevantes;
- umbral operativo;
- desempeño por subgrupos;
- falsos positivos y negativos;
- estabilidad temporal;
- robustez;
- utilidad;
- supervisión;

- comportamiento ante datos incompletos.

### 17.7. Gestión de cambios

Todo cambio debe evaluarse antes de su despliegue:

- actualización del modelo;
- cambio de proveedor;
- nueva versión;
- nuevos datos;
- nuevas integraciones;
- modificación de indicación;
- ampliación de usuarios;
- variación de umbrales;
- cambio de infraestructura.

La organización debe determinar si el cambio requiere revalidación, nueva evaluación de conformidad o comunicación a autoridades.

### 17.8. Vigilancia y auditoría

La gobernanza debe incluir indicadores como:

- tasa de errores;
- discrepancias con expertos;
- rendimiento por subgrupos;
- anulaciones humanas;
- incidentes;
- reclamaciones;
- deriva;
- disponibilidad;
- alertas de seguridad;
- cambios del proveedor.

Las auditorías deben revisar no solo documentación, sino el uso real. Es frecuente que los procedimientos describan una supervisión que no se produce en la práctica.

## 18. Casos prácticos de calificación

### 18.1. Modelo interno de descubrimiento de moléculas

Una empresa desarrolla un modelo para priorizar compuestos y realizar ensayos posteriores.

En fase puramente exploratoria puede resultar aplicable la exclusión de investigación científica. El sistema no será automáticamente de alto riesgo. Sin embargo, deberán cumplirse las normas sobre datos, propiedad intelectual, seguridad e integridad científica. Y cuando sus resultados formen parte de un expediente regulatorio, la empresa deberá conservar trazabilidad, justificar la metodología y demostrar validación experimental.

### 18.2. Sistema de selección de pacientes para un ensayo

Un modelo analiza historias clínicas para identificar candidatos. También puede tratar categorías especiales de datos, requerir evaluación de impacto y afectar al acceso a un ensayo. Si actúa como producto sanitario o modifica decisiones clínicas, podría quedar sometido al MDR y, en su caso, al régimen de alto riesgo.

Aunque se presente como herramienta de apoyo, debe analizarse si el investigador puede revisar efectivamente la decisión.

### 18.3. Algoritmo de interpretación genética

Un sistema interpreta variantes y genera una clasificación de riesgo clínico. Si está destinado a proporcionar información diagnóstica o predictiva a partir de muestras humanas, puede constituir un producto de diagnóstico *in vitro*. Si su clase requiere intervención de un organismo notificado, será previsiblemente un sistema de alto riesgo por la vía del artículo 6.1.

La validación deberá contemplar rendimiento analítico, evidencia clínica, representatividad poblacional y gestión de variantes inciertas.

### 18.4. Control predictivo de fermentación

Un algoritmo ajusta automáticamente temperatura, oxígeno, alimentación y pH de un biorreactor. Si controla funciones de seguridad de una máquina sometida a evaluación por terceros, puede quedar incluido como alto riesgo. Si su función principal es optimizar calidad o rendimiento, podría no estarlo, pero seguirá sujeto al sistema de calidad, validación, integridad de datos y gestión de cambios.

La posibilidad de que una salida errónea comprometa un lote exige límites operativos independientes y capacidad de intervención manual.

### 18.5. Herramienta de selección de personal científico

Un sistema clasifica candidatos según currículos, entrevistas grabadas y pruebas. Y este puede ser de alto riesgo conforme al anexo III. La empresa debe examinar sesgos, accesibilidad, datos de entrenamiento, supervisión humana, información a candidatos y derechos de protección de datos.

Si además infiere emociones durante entrevistas, podría incurrir en una práctica prohibida.

### 18.6. Modelo generativo para expedientes regulatorios

Una empresa utiliza un modelo para redactar partes de un expediente técnico. Normalmente este no será un sistema de alto riesgo por ese uso aislado. No obstante, presenta riesgos de confidencialidad, errores, referencias inventadas y pérdida de integridad documental. Sin embargo, debe utilizarse únicamente como herramienta de asistencia, bajo revisión cualificada, trazabilidad de fuentes y control de versiones.

### 18.7. Asistente conversacional para pacientes

Si un sistema responde preguntas sobre tratamientos o interpreta síntomas, entonces debe analizarse si proporciona información diagnóstica o terapéutica, en cuyo caso podría constituir software médico. Debe informar al usuario de que interactúa con una máquina, controlar contenidos, establecer límites y derivar situaciones urgentes. Y desde luego, una

cláusula genérica afirmando que «no sustituye al médico» no neutraliza una finalidad médica revelada por su funcionamiento real.

## 19. Régimen sancionador y consecuencias empresariales

Las infracciones relativas a prácticas prohibidas pueden sancionarse con multas administrativas de hasta 35 millones de euros o, para empresas, hasta el 7 % del volumen de negocio mundial total anual del ejercicio anterior, aplicándose el importe que corresponda conforme a las reglas del Reglamento.

El incumplimiento de otras obligaciones puede alcanzar 15 millones de euros o el 3 % del volumen de negocio mundial. El suministro de información incorrecta, incompleta o engañosa puede sancionarse con hasta 7,5 millones de euros o el 1 %. Para pequeñas y medianas empresas se aplican reglas destinadas a evitar sanciones desproporcionadas.

La multa administrativa no es el único riesgo. Deben considerarse:

- retirada o suspensión de productos;
- medidas correctivas;
- pérdida de certificación;
- responsabilidad civil;
- reclamaciones laborales;
- investigaciones de protección de datos;
- pérdida de propiedad intelectual;
- incumplimiento contractual;
- exclusión de licitaciones;
- daño reputacional;
- pérdida de confianza científica.

En una empresa biotecnológica, el mayor impacto puede no ser la sanción económica, sino la imposibilidad de utilizar datos, la invalidación de resultados, la interrupción de un ensayo, la no conformidad de un lote o la pérdida de aceptación regulatoria.

## 20. Pensamiento crítico: errores frecuentes en la interpretación empresarial

### 20.1. «Nuestro sistema no toma la decisión final»

Esta afirmación no excluye la regulación. Un sistema puede influir materialmente en la decisión, aunque exista una aprobación humana formal.

### 20.2. «Solo somos usuarios»

La empresa puede convertirse en proveedor si introduce el sistema bajo su marca, lo modifica sustancialmente o altera su finalidad.

### 20.3. «El proveedor afirma que cumple el Reglamento»

La declaración comercial no sustituye la diligencia debida. El responsable del despliegue mantiene obligaciones propias.

### 20.4. «Los datos están seudonimizados, y por tanto no son personales»

La seudonimización reduce riesgos, pero no elimina por sí misma la condición de dato personal.

### 20.5. «Es un proyecto de investigación»

La exclusión científica no resulta aplicable cuando el sistema se utiliza operacionalmente o en condiciones reales con efectos sobre personas o productos.

### 20.6. «No es un producto sanitario porque lo llamamos herramienta de bienestar»

La calificación depende de la finalidad y las funciones reales, no exclusivamente de la denominación.

### 20.7. «La inteligencia artificial es más objetiva que una persona»

Los modelos reproducen las características, errores y sesgos de sus datos y de las decisiones incorporadas al proceso de desarrollo.

### 20.8. «El humano siempre puede intervenir»

La posibilidad teórica no equivale a supervisión efectiva. Deben existir tiempo, información, competencia y autoridad para intervenir.

### 20.9. «El Reglamento se ha aplazado»

Solo determinados plazos de sistemas de alto riesgo han sido objeto de un acuerdo político provisional de modificación. Otras obligaciones ya están vigentes y el cambio normativo todavía debe formalizarse.

### 20.10. «La inteligencia artificial generativa solo redacta»

La redacción puede introducir datos falsos, divulgar información confidencial, alterar decisiones y contaminar documentación regulada.

## 21. Conclusiones

El Reglamento Europeo de Inteligencia Artificial no impone una prohibición general ni una autorización previa para todo uso de inteligencia artificial. Establece una arquitectura de obligaciones graduadas que debe aplicarse caso por caso. En biotecnología, el análisis jurídico no puede partir del algoritmo de forma aislada. Debe comenzar por la finalidad prevista, la decisión condicionada, el producto en el que se integra, los datos utilizados, la población afectada y el papel asumido por cada operador. La exclusión de investigación científica es relevante, pero estrecha. No ampara usos operativos ni elimina las obligaciones derivadas de protección de datos, ensayos clínicos, propiedad intelectual, bioética o integridad científica.

Los sistemas vinculados a productos sanitarios y diagnóstico *in vitro* constituyen uno de los principales ámbitos de alto riesgo, siempre que concurra la exigencia de evaluación de conformidad por terceros. Los usos en medicamentos no son automáticamente de alto riesgo conforme al Reglamento, pero pueden tener una relevancia regulatoria muy elevada conforme a la legislación farmacéutica y las buenas prácticas.

Por otro lado, la gobernanza de datos constituye el núcleo técnico del cumplimiento. Sin datos pertinentes, representativos, trazables y legalmente obtenidos, no existe una inteligencia artificial fiable, por sofisticado que sea el modelo.

La supervisión humana debe ser efectiva. Un profesional que carece de tiempo, información o capacidad para cuestionar el resultado no constituye una garantía, sino una validación aparente. La inteligencia artificial generativa debe gestionarse como una herramienta de riesgo variable. Su uso en

documentación científica o regulatoria requiere verificación primaria, control de confidencialidad, trazabilidad y responsabilidad editorial.

La empresa biotecnológica debería integrar el cumplimiento algorítmico en sus sistemas existentes de calidad, gestión de riesgos, validación, protección de datos, ciberseguridad y vigilancia. Crear una estructura paralela aumentaría burocracia sin mejorar necesariamente el control. El principal desafío no es producir documentos formales, sino demostrar que la organización conoce qué sistemas utiliza, por qué los utiliza, con qué datos, bajo qué limitaciones, quién responde de ellos y cómo detectará que han dejado de ser seguros o fiables.

En definitiva, la inteligencia artificial jurídicamente sostenible no es la que promete sustituir la decisión científica, clínica o técnica, sino la que se integra en un proceso gobernado, verificable, reversible y sujeto a responsabilidad humana. Para la empresa biotecnológica europea, esta exigencia no debe contemplarse únicamente como una carga regulatoria. Constituye una condición de calidad científica, confianza comercial y legitimidad industrial.

**Referencias normativas, regulatorias y técnicas.**


1. ***Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo**, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial.*
2. ***Reglamento (UE) 2016/679**, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales.*
3. ***Reglamento (UE) 2017/745**, sobre los productos sanitarios.*
4. ***Reglamento (UE) 2017/746**, sobre los productos sanitarios para diagnóstico in vitro.*
5. ***Reglamento (UE) 2025/327**, relativo al Espacio Europeo de Datos de Salud.*
6. ***Reglamento (UE) 2023/2854**, sobre normas armonizadas para un acceso justo a los datos y su utilización —Reglamento de Datos—.*
7. ***Directiva (UE) 2022/2555**, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión —NIS2—.*
8. ***Reglamento (UE) 2024/2847**, relativo a los requisitos horizontales de ciberseguridad para los productos con elementos digitales.*
9. ***Directiva (UE) 2024/2853**, sobre responsabilidad por los daños causados por productos defectuosos.*
10. ***European Medicines Agency. Reflection paper on the use of artificial intelligence in the medicinal product lifecycle**, versión adoptada en septiembre de 2024.*
11. ***European Medicines Agency. Multi-annual Artificial Intelligence Workplan 2026-2028**.*
12. ***Comité Europeo de Protección de Datos. Opinión 28/2024 sobre determinados aspectos de protección de datos relacionados con el tratamiento de datos personales en el contexto de modelos de inteligencia artificial**.*
13. ***ISO/IEC 42001:2023**, Information technology — Artificial intelligence — Management system.*
14. ***ISO/IEC 23894:2023**, Information technology — Artificial intelligence — Guidance on risk management.*
15. ***ISO 13485:2016**, Medical devices — Quality management systems — Requirements for regulatory purposes.*
16. ***ISO 14971:2019**, Medical devices — Application of risk management to medical devices.*
17. ***IEC 62304:2006/Amd 1:2015**, Medical device software — Software life-cycle processes.*
18. ***ISO 14155:2020**, Clinical investigation of medical devices for human subjects — Good clinical practice.*
19. ***ISO 20916:2019**, In vitro diagnostic medical devices — Clinical performance studies using specimens from human subjects — Good study practice.*
20. ***EudraLex, volumen 4, anexo 11**, Computerised Systems.*
21. ***ISPE, GAMP 5, segunda edición**, A Risk-Based Approach to Compliant GxP Computerized Systems.*


*Las normas técnicas citadas constituyen referencias relevantes para estructurar sistemas de gestión, validación y control, pero su mera implantación no acredita automáticamente la conformidad con el Reglamento de Inteligencia Artificial. La presunción jurídica de conformidad dependerá, cuando proceda, de la publicación de las correspondientes referencias de normas armonizadas en el Diario Oficial de la Unión Europea.*