RESPONSABILIDAD JURÍDICA POR DECISIONES ALGORÍTMICAS EN LA INDUSTRIA ALIMENTARIA

Quién responde cuando la inteligencia artificial falla: fabricante, proveedor tecnológico, laboratorio, Director Técnico, operador alimentario o Administración

José M. López, BSc, MD, PhD

Serie: Inteligencia artificial en la industria alimentaria · Publicación n.º 7

Estado normativo analizado: 6 de agosto de 2026

INTABIOTECH

RESPONSABILIDAD JURÍDICA POR DECISIONES ALGORÍTMICAS EN LA INDUSTRIA ALIMENTARIA

Quién responde cuando la inteligencia artificial falla: fabricante, proveedor tecnológico, laboratorio, director técnico, operador alimentario o Administración

Serie: Inteligencia artificial en la industria alimentaria · Publicación n.º 7

José M. López · Dirección Técnica INTABIOTECH

Edición revisada y consolidada · Agosto de 2026

Ficha editorial

Título: Responsabilidad jurídica por decisiones algorítmicas en la industria alimentaria
Subtítulo: Quién responde cuando la inteligencia artificial falla
Serie: Inteligencia artificial en la industria alimentaria — Publicación n.º 7
Autor: José Manuel López Pérez
Entidad: INTABIOTECH
Cierre normativo: 6 de agosto de 2026
Edición: Versión consolidada, revisada y maquetada para publicación

Nota de alcance

Este trabajo ofrece un análisis jurídico-técnico general. No sustituye el asesoramiento jurídico, pericial o regulatorio adaptado a un incidente, producto, contrato o procedimiento concreto.

Criterio editorial y metodología

La obra se ha reconstruido a partir del manuscrito acumulado de la serie completa, unificando la terminología y reordenando el contenido en una arquitectura temática, de cara a facilitar su comprensión. El análisis combina Derecho alimentario, responsabilidad civil y contractual, Derecho administrativo sancionador, Derecho penal, gobierno corporativo, tecnología de los alimentos, validación de modelos y gestión de evidencias digitales. Las afirmaciones normativas se han contrastado con los textos oficiales vigentes al cierre indicado. Cuando una regla depende de la clasificación del sistema, de la función efectivamente desempeñada o de la fecha de aplicación de una obligación, se evita presentar conclusiones automáticas y se exige el examen del caso concreto.

Resumen ejecutivo

La inteligencia artificial ya interviene en decisiones que inciden directamente en la seguridad, la legalidad y la calidad de los alimentos: selección de materias primas, control de procesos, interpretación analítica, predicción de vida útil, generación de etiquetado, liberación de lotes y gestión de retiradas. La tecnología puede mejorar la capacidad preventiva de la empresa, pero también introduce nuevas dependencias, nuevas asimetrías informativas y nuevas dificultades probatorias.

La tesis central de esta obra es que la decisión puede automatizarse, pero la responsabilidad jurídica no. El algoritmo carece de personalidad jurídica, patrimonio y capacidad penal. Por ello, cuando el sistema falla, el análisis debe reconstruir qué personas y entidades diseñaron, suministraron, integraron, validaron, configuraron, utilizaron y supervisaron la herramienta, y quién tenía la capacidad real de impedir el resultado.

El operador alimentario conserva una posición central porque controla el proceso y decide la introducción del producto en el mercado. Esa centralidad no convierte, sin embargo, su responsabilidad en exclusiva. El proveedor tecnológico puede responder por defectos de diseño, documentación o actualización; el integrador, por una configuración inadecuada; el laboratorio, por fallos de muestreo, método o interpretación; el Director Técnico y otros responsables, cuando sus funciones reales, su conocimiento y su capacidad de actuación permitan una imputación personal; y la Administración, por sus propias actuaciones automatizadas cuando concurran los presupuestos de invalidez o responsabilidad patrimonial.

La prevención eficaz exige integrar la inteligencia artificial en el APPCC, en el sistema de calidad, en el compliance y en el gobierno corporativo. Deben existir inventario, clasificación de criticidad, validación contextual, supervisión humana efectiva, control de versiones, vigilancia de deriva, derechos contractuales de acceso a registros, plan de contingencia y protocolo de preservación de evidencias. La empresa no necesita prometer infalibilidad, pero sí demostrar que conocía los límites del sistema y gestionó el riesgo con una diligencia proporcionada a sus consecuencias.

Tesis de la obra

La responsabilidad algorítmica en la industria alimentaria no es la responsabilidad de una máquina, sino la imputación jurídica de los fallos humanos, técnicos y organizativos que permitieron que una decisión automatizada produjera consecuencias ilícitas.

Resumen

La incorporación de sistemas de inteligencia artificial a la industria alimentaria está desplazando progresivamente decisiones que hasta ahora dependían de técnicos, laboratorios y responsables de calidad. Algoritmos de visión artificial clasifican materias primas, modelos predictivos determinan la vida útil, sistemas de aprendizaje automático identifican desviaciones microbiológicas, aplicaciones generativas proponen formulaciones y etiquetados, y plataformas automatizadas deciden sobre la liberación de lotes, la aceptación de proveedores o la retirada de productos.

Esta transformación no crea, sin embargo, una zona de irresponsabilidad jurídica. Cuando una decisión algorítmica provoca la comercialización de un alimento inseguro, un etiquetado incorrecto, la omisión de un alérgeno, un falso resultado analítico o una retirada tardía, la pregunta jurídicamente relevante no es quién «tomó» materialmente la decisión, sino quién tenía el deber de diseñar, validar, supervisar, corregir o impedir el resultado.

El presente trabajo analiza la posible concurrencia de responsabilidades del fabricante del sistema, el proveedor tecnológico, el integrador, el laboratorio, el Director Técnico, el operador de empresa alimentaria, sus administradores y la Administración pública. Se examinan el Reglamento Europeo de Inteligencia Artificial, el Derecho alimentario de la Unión, la nueva Directiva sobre responsabilidad por productos defectuosos, el Derecho civil y contractual español, el régimen sancionador alimentario, la responsabilidad penal por delitos contra la salud pública, la responsabilidad de las personas jurídicas y la responsabilidad patrimonial de las Administraciones públicas.

La conclusión principal es clara: la utilización de inteligencia artificial no desplaza la responsabilidad del operador alimentario ni convierte al algoritmo en sujeto responsable. La responsabilidad puede distribuirse y acumularse entre distintos participantes, pero no desaparecer. La empresa que introduce una herramienta algorítmica en una decisión relevante para la seguridad alimentaria asume un deber reforzado de selección, validación, vigilancia, trazabilidad y supervisión humana efectiva.

Palabras clave: inteligencia artificial; industria alimentaria; responsabilidad jurídica; operador alimentario; Director Técnico; producto defectuoso; laboratorio; Reglamento de Inteligencia Artificial; seguridad alimentaria; decisiones algorítmicas; trazabilidad probatoria.

Abreviaturas y conceptos de uso recurrente

Término	Significado
APPCC	Análisis de Peligros y Puntos de Control Crítico.
CAPA	Acciones correctivas y preventivas.
IA	Inteligencia artificial.
RIA / AI Act	Reglamento (UE) 2024/1689, modificado por el Reglamento (UE) 2026/1744.
OEA	Operador de empresa alimentaria.
PCC	Punto de control crítico.
RACI	Responsible, Accountable, Consulted, Informed.
Log	Registro automático de acontecimientos o eventos del sistema.
Deriva	Pérdida o modificación del rendimiento del modelo por cambios en datos, entorno o proceso.

Tabla preliminar 1. Abreviaturas esenciales.

Contenido

CAPÍTULO 1. FUNDAMENTOS DE LA IMPUTACIÓN ALGORÍTMICA

Este capítulo fija la tesis general del trabajo: la inteligencia artificial no crea una zona de irresponsabilidad. La imputación jurídica sigue el control del riesgo, el deber de actuación y la capacidad de evitar el resultado. El propósito no es encontrar un culpable automático, sino reconstruir la cadena de decisiones que convirtió una salida técnica en una consecuencia jurídica.

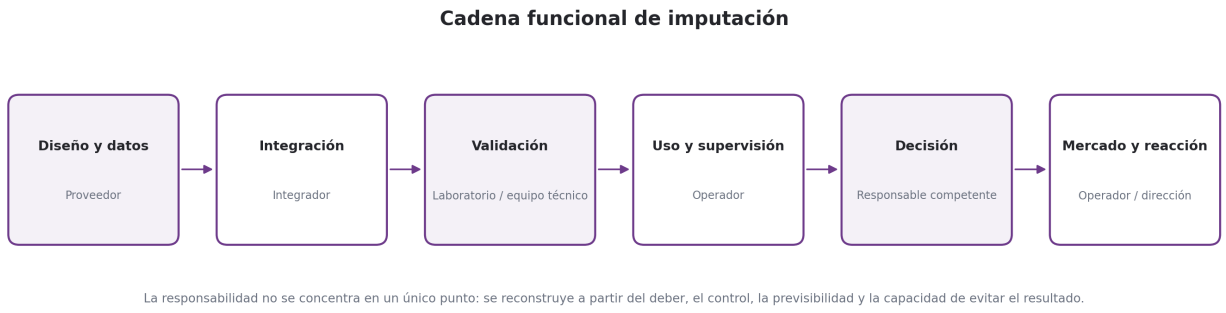


Figura 1. Cadena funcional de imputación de responsabilidad.

Introducción: el algoritmo decide, pero el Derecho imputa

La inteligencia artificial no contamina un alimento, no firma una declaración de conformidad, no libera jurídicamente un lote y no comparece ante una autoridad sanitaria. Tampoco posee patrimonio con el que indemnizar a las víctimas ni capacidad penal para responder por un delito contra la salud pública.

El sistema algorítmico constituye una herramienta tecnológica integrada en una organización humana y empresarial. Por tanto, cuando su utilización produce un daño, el ordenamiento jurídico debe reconstruir qué personas físicas o jurídicas intervinieron en su diseño, suministro, integración, entrenamiento, validación, utilización y supervisión.

La cuestión no puede resolverse mediante una respuesta única. En un mismo incidente pueden coexistir:

- responsabilidad administrativa del operador alimentario;
- responsabilidad civil del fabricante o proveedor tecnológico;
- responsabilidad contractual del laboratorio o integrador;
- responsabilidad personal de determinados técnicos o directivos;
- responsabilidad societaria de los administradores;
- responsabilidad penal de personas físicas;
- responsabilidad penal de la persona jurídica;
- responsabilidad patrimonial de una Administración;
- obligaciones regulatorias específicas derivadas del Reglamento de Inteligencia Artificial.

Estas responsabilidades no son necesariamente excluyentes. Pueden ser concurrentes, solidarias, sucesivas o sujetas a acciones de repetición entre los participantes.

La inteligencia artificial añade complejidad causal y probatoria, pero no altera el principio esencial del Derecho alimentario europeo: los operadores de empresas alimentarias deben garantizar, en las actividades sometidas a su control, que los alimentos cumplen la legislación aplicable y deben verificar efectivamente dicho cumplimiento. Así lo establece el artículo 17 del Reglamento (CE) n.º 178/2002.

El Reglamento (CE) n.º 852/2004 refuerza este principio al declarar que la responsabilidad principal de la seguridad alimentaria corresponde al operador y al exigir procedimientos permanentes basados en los principios APPCC.

Por ello, una empresa no puede defenderse simplemente afirmando:

«El algoritmo indicó que el lote era conforme».

Esa afirmación podrá servir para identificar un fallo del proveedor o fundamentar posteriormente una reclamación contractual, pero, por sí sola, no elimina la responsabilidad primaria del operador que comercializó el alimento.

Tesis central: la IA no sustituye la posición jurídica de garante

La responsabilidad no se atribuye atendiendo únicamente a quién ejecutó físicamente la última acción. Se examina quién:

1. creó o suministró el sistema;
2. definió su finalidad;
3. seleccionó los datos;
4. configuró sus parámetros;
5. decidió integrarlo en el proceso;
6. estableció el grado de automatización;
7. interpretó o aceptó su resultado;
8. disponía de capacidad para intervenir;
9. conocía o debía conocer sus limitaciones y
10. podía evitar razonablemente el daño.

En términos jurídicos, la pregunta decisiva es:

¿Quién controlaba el riesgo y tenía el deber de impedir su materialización?

Esto conduce a una ***primera regla*** de imputación:

Regla de control

Cuanto mayor sea la capacidad de una persona o entidad para diseñar, modificar, supervisar o detener el sistema, mayor será su exposición jurídica.

Y a una ***segunda***:

Regla de dependencia

Cuanto mayor sea la dependencia empresarial respecto del resultado algorítmico, más intenso debe ser el sistema de validación y supervisión.

Una herramienta meramente informativa no genera el mismo riesgo que un sistema que libera automáticamente un lote. La responsabilidad se intensifica cuando el resultado algorítmico:

- se ejecuta sin revisión;
- produce efectos irreversibles;
- afecta directamente a la salud;
- reemplaza una verificación legalmente exigible;
- opera con datos insuficientes;
- no conserva registros;
- no permite explicar la decisión;
- no dispone de mecanismos de parada;
- ha sido modificado después de su validación;
- continúa utilizándose pese a la aparición de señales de deriva.

Responsabilidades concurrentes y distribución interna del riesgo

La presencia de varios participantes no obliga a elegir un único responsable. La responsabilidad jurídica puede acumularse por títulos diferentes.

Un proveedor tecnológico puede responder porque suministró un sistema defectuoso. El laboratorio puede responder porque utilizó ese sistema sin validarlo. El Director Técnico puede responder porque aprobó su uso pese a conocer sus limitaciones. El operador alimentario puede ser sancionado por comercializar el producto. Los administradores pueden responder si omitieron controles estructurales. Y la Administración puede incurrir en responsabilidad si su propio sistema automatizado causó un daño antijurídico.

Los contratos entre las partes pueden distribuir costes y establecer indemnizaciones, pero no permiten neutralizar las obligaciones imperativas frente a consumidores, autoridades o terceros perjudicados.

Una cláusula conforme a la cual «el proveedor no garantiza la exactitud de los resultados» puede ser relevante en una controversia contractual entre empresas, pero difícilmente legitima que el operador utilice el sistema para adoptar decisiones críticas sin validación independiente.

Del mismo modo, una cláusula por la que el proveedor asume toda la responsabilidad no libera automáticamente al operador de sus obligaciones legales de seguridad alimentaria.

Distribución interna no equivale a exoneración externa

El contrato puede decidir quién soportará finalmente el coste económico entre proveedor y cliente. No puede modificar libremente quién es responsable ante la autoridad sanitaria, el consumidor lesionado o el órgano jurisdiccional penal.

Síntesis: la imputación sigue al deber incumplido

La imputación jurídica exige evitar dos extremos:

1. atribuir toda la responsabilidad al operador, ignorando defectos tecnológicos o analíticos;
2. trasladar toda la responsabilidad al proveedor, ignorando que la empresa decidió utilizar el sistema y comercializar el producto.

La solución correcta consiste en reconstruir la cadena completa:

diseño → suministro → integración → validación → configuración → uso → supervisión → decisión → comercialización → vigilancia → reacción

En cada eslabón debe determinarse:

- qué obligación existía;
- quién debía cumplirla;
- qué riesgo era previsible;
- qué información estaba disponible;
- qué control se omitió;
- qué relación causal tuvo la omisión con el daño;
- qué evidencia permite demostrarlo.

La tesis que vertebra este trabajo puede formularse del siguiente modo:

La responsabilidad algorítmica en la industria alimentaria no es la responsabilidad de una máquina, sino la imputación jurídica de los fallos humanos, técnicos y organizativos que permitieron que una decisión automatizada produjera consecuencias ilícitas.

El algoritmo no rompe la cadena de responsabilidad. Simplemente añade nuevos eslabones, nuevos deberes y nuevas dificultades probatorias.

CAPÍTULO 2. MARCO NORMATIVO EUROPEO Y SECTORIAL

El marco aplicable no se agota en el Reglamento de Inteligencia Artificial. El análisis exige superponer el Derecho alimentario, la higiene y el APPCC, la responsabilidad por productos defectuosos, el Derecho de consumo y las normas nacionales de responsabilidad. La clasificación del sistema conforme al Reglamento de IA es importante, pero no decide por sí sola la diligencia exigible al operador alimentario.

2.1. Estado normativo y calendario de aplicación

El Reglamento (UE) 2024/1689 entró en vigor el 1 de agosto de 2024 y su fecha general de aplicación es el 2 de agosto de 2026. El Reglamento (UE) 2026/1744, en vigor desde el 27 de julio de 2026, modificó el calendario de las secciones 1, 2 y 3 del capítulo III: las reglas correspondientes a los sistemas de alto riesgo del artículo 6.2 y

anexo III se aplicarán desde el 2 de diciembre de 2027, mientras que las referidas a los sistemas del artículo 6.1 y anexo I lo harán desde el 2 de agosto de 2028.

La Directiva (UE) 2024/2853 sobre responsabilidad por productos defectuosos debe transponerse antes del 9 de diciembre de 2026. Tras la corrección de errores publicada el 7 de mayo de 2026, su artículo 2.1 establece que se aplicará a los productos introducidos en el mercado o puestos en servicio después del 8 de diciembre de 2026; en términos prácticos, a partir del 9 de diciembre de 2026.

La propuesta de Directiva específica sobre responsabilidad extracontractual en materia de inteligencia artificial, COM(2022) 496, fue retirada formalmente el 6 de octubre de 2025. La responsabilidad debe reconstruirse, por tanto, mediante el Reglamento de Inteligencia Artificial, la normativa de productos defectuosos, el Derecho nacional y las reglas sectoriales alimentarias.

Instrumento	Hito relevante	Fecha
Reglamento (UE) 2024/1689	Entrada en vigor	1 de agosto de 2024
Reglamento (UE) 2024/1689	Aplicación general, con excepciones	2 de agosto de 2026
Reglamento (UE) 2026/1744	Entrada en vigor	27 de julio de 2026
Sistemas de alto riesgo: art. 6.2 y anexo III	Aplicación de cap. III, secciones 1 a 3	2 de diciembre de 2027
Sistemas de alto riesgo: art. 6.1 y anexo I	Aplicación de cap. III, secciones 1 a 3	2 de agosto de 2028
Directiva (UE) 2024/2853	Fecha límite de transposición	9 de diciembre de 2026
Directiva (UE) 2024/2853	Productos comprendidos	Introducidos o puestos en servicio después del 8 de diciembre de 2026

Tabla 2. Calendario normativo relevante al cierre de la obra.

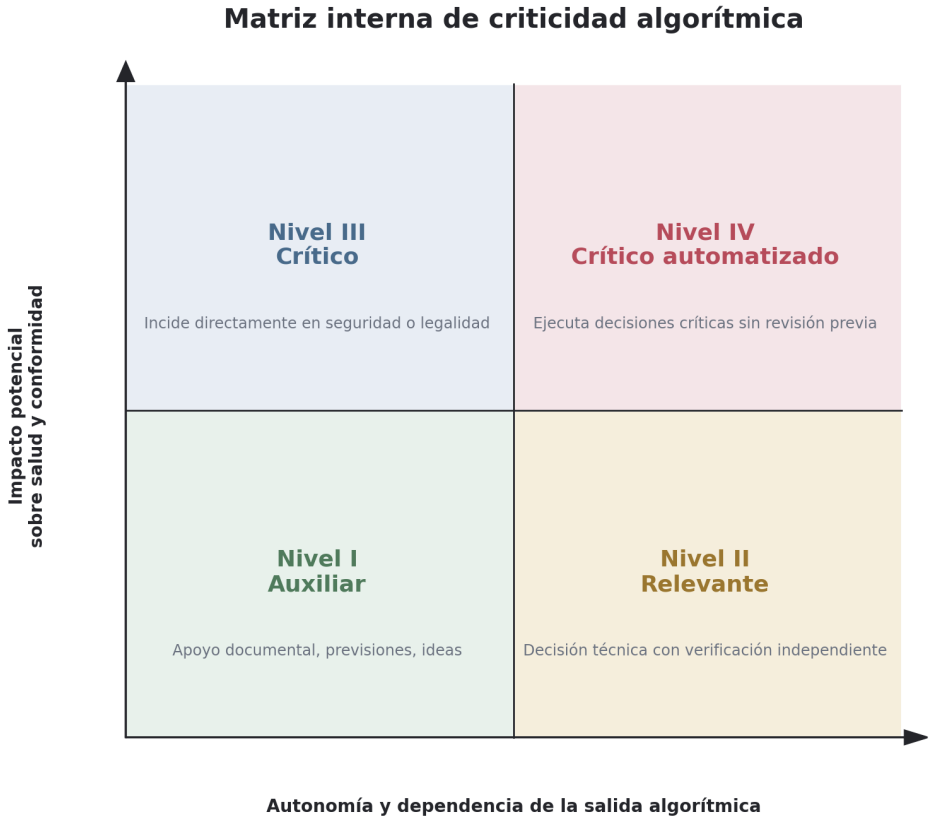


Figura 2. Matriz interna de criticidad algorítmica.

Primera precisión: no toda IA alimentaria es de «alto riesgo» conforme al AI Act

Uno de los errores jurídicos más frecuentes consiste en asumir que cualquier sistema de inteligencia artificial utilizado en seguridad alimentaria será automáticamente un sistema de alto riesgo conforme al Reglamento (UE) 2024/1689. Esto no es así.

La clasificación de alto riesgo depende de los criterios del artículo 6 y de los anexos I y III del Reglamento. Un sistema puede ser de alto riesgo cuando actúa como componente de seguridad de determinados productos regulados por la legislación armonizada europea y el producto está sujeto a evaluación de conformidad por terceros, o cuando se utiliza en alguno de los ámbitos sensibles expresamente recogidos en el anexo III.

En la industria alimentaria, pueden encontrarse sistemas de IA que no sean formalmente de alto riesgo según el Reglamento de Inteligencia Artificial, por ejemplo:

1) predicción comercial de la demanda;
2) optimización de inventarios;
3) recomendación preliminar de formulaciones;
4) clasificación no crítica de imágenes;
5) análisis de tendencias de consumidores;
6) estimación interna de costes;
7) elaboración asistida de documentación.

Otros sistemas pueden adquirir una significación jurídica mucho mayor cuando intervienen en:

a) rechazo o liberación automática de lotes;
b) detección de cuerpos extraños;
c) control de tratamientos térmicos;
d) predicción microbiológica;
e) cálculo de vida útil;
f) detección de alérgenos;
g) dosificación automática de ingredientes o aditivos;
h) determinación de condiciones de almacenamiento;
i) interpretación de resultados analíticos;
j) evaluación de proveedores críticos;
k) activación o desactivación de retiradas;
l) control automatizado de maquinaria que afecte a la seguridad.

La consecuencia es fundamental: que un sistema no sea de alto riesgo conforme al Reglamento de Inteligencia Artificial no significa que su utilización sea jurídicamente irrelevante o que quede fuera del Derecho.

Seguirán resultando aplicables, según el caso:

- el Derecho alimentario;
- las normas sobre higiene y APPCC;
- las obligaciones de trazabilidad y retirada;
- el Derecho de consumo;
- el régimen de productos defectuosos;
- el Derecho contractual;
- la normativa de protección de datos;
- el Derecho laboral;
- el Derecho administrativo sancionador;
- el Derecho penal;
- las reglas generales sobre diligencia profesional.

El Reglamento de Inteligencia Artificial entró en vigor el 1 de agosto de 2024 y una parte sustancial de sus disposiciones comenzó a aplicarse el 2 de agosto de 2026. Tras la reforma denominada AI Omnibus, en vigor desde el 27 de julio de 2026, determinadas obligaciones sobre sistemas de alto riesgo del anexo III se han desplazado hasta diciembre de 2027 y las relativas a sistemas integrados en productos del anexo I hasta agosto de 2028.

Esta aplicación escalonada no suspende las obligaciones preexistentes de seguridad alimentaria. El operador no puede esperar a que resulte plenamente aplicable el régimen de alto riesgo para implantar controles adecuados.

La nueva responsabilidad por productos defectuosos

La Directiva (UE) 2024/2853 moderniza el régimen europeo de responsabilidad objetiva por productos defectuosos e incluye expresamente el software dentro del concepto de producto. Esto permite que un sistema de inteligencia artificial defectuoso pueda generar responsabilidad del fabricante sin que la víctima tenga que demostrar necesariamente su culpa, aunque deberá acreditar el daño, el defecto y la relación causal conforme al régimen aplicable.

La Directiva también contempla:

- defectos derivados de actualizaciones;
- insuficiencia de actualizaciones de seguridad;
- servicios digitales relacionados;
- vulnerabilidades de ciberseguridad;
- modificaciones sustanciales;
- aprendizaje continuo del sistema;
- acceso judicial a determinadas pruebas;
- presunciones de defecto o causalidad en situaciones de complejidad técnica.

Una actualización, reentrenamiento o proceso de aprendizaje continuo puede constituir una modificación sustancial. Quien realiza esa modificación fuera del control del fabricante original puede ser tratado como fabricante del producto modificado.

Esta Directiva debe aplicarse a los productos introducidos en el mercado o puestos en servicio después del 8 de diciembre de 2026. A fecha de este trabajo, 6 de agosto de 2026, todavía no ha comenzado su ámbito temporal operativo, aunque las empresas deben preparar ya su documentación, contratos y sistemas de trazabilidad.

Debe aclararse también que la propuesta de Directiva específica sobre responsabilidad civil por inteligencia artificial fue formalmente retirada en 2025. No existe, por tanto, una Directiva horizontal independiente que resuelva toda responsabilidad extracontractual por IA. El marco debe reconstruirse mediante el Reglamento de Inteligencia Artificial, la Directiva de productos defectuosos, el Derecho nacional y las normas sectoriales.

CAPÍTULO 3. SUJETOS RESPONSABLES EN LA CADENA ALIMENTARIA Y TECNOLÓGICA

La cadena tecnológica y la cadena alimentaria rara vez coinciden. El fabricante del modelo, el integrador, el laboratorio y el operador pueden controlar riesgos diferentes. Esta pluralidad explica por qué la responsabilidad puede ser concurrente y por qué las cláusulas contractuales solo distribuyen internamente costes, pero no eliminan deberes imperativos frente al consumidor o la autoridad.

Mapa preliminar de sujetos responsables

Sujeto	Fuente principal de responsabilidad	Circunstancias especialmente relevantes
Fabricante o desarrollador de IA	AI Act, producto defectuoso, contrato, responsabilidad extracontractual	Defectos de diseño, datos inadecuados, documentación insuficiente, falta de actualizaciones, ciberseguridad deficiente
Proveedor tecnológico o distribuidor	Contrato, AI Act, información precontractual, integración	Recomendaciones incorrectas, ocultación de limitaciones, configuración defectuosa, asistencia inadecuada
Integrador o consultor	Contrato profesional, negligencia técnica, posible consideración como proveedor	Selección del modelo, conexión con procesos industriales, modificación sustancial, validación incorrecta
Laboratorio	Contrato, diligencia profesional, acreditación y regulación sectorial	Muestreo, método, incertidumbre, interpretación, validación del software, falsos negativos o positivos

Sujeto	Fuente principal de responsabilidad	Circunstancias especialmente relevantes
Operador alimentario	Reglamento 178/2002, higiene, APPCC, trazabilidad, retirada, régimen sancionador	Comercialización, control del proceso, validación, seguimiento y respuesta ante desviaciones
Director Técnico o responsable de calidad	Responsabilidad laboral, civil, administrativa o penal según funciones reales	Firma, aprobación, conocimiento del riesgo, capacidad de paralización y omisión de medidas
Órgano de administración	Deberes societarios, compliance, supervisión y control	Falta de recursos, ausencia de gobierno de IA, aceptación consciente de riesgos estructurales
Persona jurídica	Responsabilidad administrativa, civil y, cuando el tipo penal lo permita, penal	Defectos organizativos, falta de controles, cultura de incumplimiento
Administración pública	Responsabilidad patrimonial, invalidez del acto, Derecho administrativo	Decisiones automatizadas, fallos de inspección, sistemas de alertas, autorizaciones o controles oficiales

Tabla 1. Sujetos potencialmente responsables y fuentes de imputación.

El operador alimentario: responsable primario, aunque no necesariamente único

El operador de empresa alimentaria ocupa la posición central porque es la persona física o jurídica responsable de que se cumplan los requisitos de la legislación alimentaria dentro de la empresa bajo su control. Esa definición y el artículo 17 del Reglamento n.º 178/2002 sitúan al operador en la mejor posición para organizar un sistema seguro y verificar su funcionamiento.

La utilización de una herramienta externa no convierte al proveedor tecnológico en operador alimentario. Salvo que el proveedor ejerza realmente funciones propias de la empresa alimentaria, el control del producto, del proceso y de la decisión de comercialización seguirá correspondiendo al operador.

Obligaciones indelegables en su dimensión externa

El operador puede externalizar actividades materiales:

- análisis microbiológicos;
- desarrollo de modelos;
- mantenimiento de sensores;
- elaboración de informes;
- asesoramiento regulatorio;
- predicción de vida útil;
- clasificación de imágenes;
- vigilancia de temperaturas.

Pero no puede externalizar por completo su obligación de asegurarse de que esas actividades son adecuadas.

Por tanto, deberá poder demostrar:

- por qué eligió el sistema;
- qué función concreta le asignó;
- con qué datos fue validado;
- para qué matrices y procesos resulta aplicable;
- qué limitaciones presenta;
- qué persona revisa sus resultados;
- qué umbrales activan una intervención;
- qué registros se conservan;
- cómo se detecta la deriva;
- cuándo debe suspenderse su uso.

Un proveedor prestigioso no sustituye la diligencia del operador

La reputación comercial, una certificación genérica o el uso del sistema por otras empresas no acreditan necesariamente su idoneidad para una matriz, formulación, línea, población microbiana o condición industrial determinada.

De ese modo, hay que adopter el criterio de que la validación debe ser contextual.

Un modelo entrenado con carne cocida no puede trasladarse automáticamente a ovoproductos. Un sistema de visión validado para envases opacos puede no ser fiable con materiales reflectantes. Una predicción de vida útil obtenida con una cadena de frío estable puede fallar cuando existen fluctuaciones logísticas.

Cuando el operador ignora estas diferencias, el error deja de ser exclusivamente «del algoritmo» y se convierte también en un defecto de integración y control empresarial.

Fabricante, proveedor tecnológico e integrador

El AI Act distingue entre proveedor, responsable del despliegue, importador y distribuidor. Estas categorías no dependen solamente de la denominación utilizada en el contrato, sino de las funciones efectivamente realizadas.

El artículo 25 contiene una regla especialmente importante, cuando dice que un distribuidor, importador, responsable del despliegue u otro tercero puede pasar a ser considerado proveedor de un sistema de alto riesgo cuando coloca su nombre o marca, efectúa una modificación sustancial o altera la finalidad prevista de manera que el sistema pasa a ser de alto riesgo.

Por tanto, una empresa alimentaria puede dejar de ser una simple usuaria y asumir obligaciones de proveedor cuando:

- reentrena significativamente el modelo;
- modifica los umbrales de decisión;
- cambia su finalidad;
- lo incorpora a una solución comercial propia;
- lo comercializa con su marca;
- lo transforma en un componente de seguridad;
- integra varios modelos de forma que crea un nuevo sistema.

Posibles defectos imputables al proveedor

El proveedor puede responder por:

- selección inadecuada de la arquitectura;
- datos de entrenamiento insuficientes o sesgados;
- ausencia de validación representativa;
- métricas engañosas;
- ocultación de falsos negativos;
- documentación técnica incompleta;
- instrucciones ambiguas;
- falta de advertencia sobre usos no validados;
- vulnerabilidades de ciberseguridad;
- actualizaciones que deterioran el rendimiento;
- ausencia de vigilancia poscomercialización;
- incumplimiento de obligaciones de notificación.

Para los sistemas de alto riesgo, el Reglamento de Inteligencia Artificial exige, entre otras medidas, gestión de riesgos durante el ciclo de vida, documentación técnica, registros, sistema de gestión de calidad, evaluación de conformidad y vigilancia posterior.

La integración puede ser la verdadera causa del daño

En numerosos incidents que ocurren en la industria alimentaria, el modelo aislado puede funcionar correctamente, mientras que el fallo surge al integrarlo con:

- sensores mal calibrados;
- bases de datos incompletas;
- unidades de medida incompatibles;
- sistemas ERP;
- equipos de dosificación;
- límites críticos incorrectos;

- protocolos de comunicación;
- interfaces deficientes;
- procesos humanos mal diseñados.

En estos casos, la imputación puede recaer principalmente sobre el integrador o sobre la propia empresa que efectuó la integración.

El laboratorio: responsabilidad analítica y responsabilidad algorítmica

El laboratorio no responde automáticamente de todo daño derivado del producto analizado. Su responsabilidad se limita, en principio, al ámbito de las prestaciones asumidas y al nivel de diligencia técnica exigible.

Puede responder cuando exista:

- muestreo incorrecto;
- pérdida de trazabilidad;
- método no adecuado;
- equipo sin calibración;
- incumplimiento del alcance de acreditación;
- utilización incorrecta de límites de cuantificación;
- interpretación errónea;
- emisión negligente del informe;
- falta de comunicación de una incertidumbre relevante;
- validación insuficiente del software o modelo utilizado;
- omisión de resultados discordantes.

Los laboratorios oficiales designados conforme al Reglamento (UE) 2017/625 deben operar, con las excepciones previstas, de acuerdo con la norma EN ISO/IEC 17025 y estar acreditados conforme a ella.

Sin embargo, un informe analítico conforme no exime al operador cuando:

- la muestra no es representativa;
- el plan de muestreo es insuficiente;
- el peligro no analizado era previsible;
- el resultado contradice otros indicadores;
- la IA interpreta incorrectamente el resultado;
- se utiliza un ensayo fuera de su campo de aplicación;
- se ignora la incertidumbre de medida.

El laboratorio responde por la calidad de su actividad analítica. El operador continúa respondiendo por el sistema global de seguridad alimentaria.

El Director Técnico: ni responsable automático ni figura decorativa

Debe rechazarse una simplificación frecuente que se traduce en que el Director Técnico no responde siempre de todo lo que ocurre en la empresa por el mero hecho de ostentar ese título.

En la industria alimentaria general no existe un estatuto único y universal del Director Técnico aplicable a todas las actividades. Su responsabilidad dependerá de:

- la regulación específica del subsector;
- las funciones contractuales;
- los poderes delegados;
- la capacidad real de decisión;
- la intervención en el expediente;
- los documentos firmados;
- el conocimiento del riesgo;
- los medios disponibles;
- la posibilidad de detener el proceso;
- la conducta posterior a la detección del problema.

La responsabilidad personal se refuerza cuando el Director Técnico:

- aprueba expresamente el sistema;
- firma su validación;
- conoce tasas de error relevantes;
- autoriza su utilización fuera del ámbito validado;
- elimina controles humanos;
- ignora alertas reiteradas;
- ordena liberar lotes;
- oculta desviaciones;
- impide una retirada;
- carece deliberadamente de documentación;
- mantiene el sistema pese a una deriva conocida.

Por el contrario, la atribución personal se debilita cuando el profesional:

- carecía de poder decisorio;
- formuló advertencias documentadas;
- solicitó medidas correctoras;
- propuso la paralización;
- fue desautorizado por la dirección;
- no tuvo acceso a la información relevante;
- el fallo era técnicamente imprevisible;
- actuó conforme al estado de la ciencia y de la técnica.

La responsabilidad penal por omisión exige, en España, que la persona incumpla un especial deber jurídico de evitar el resultado y que la no evitación pueda equipararse jurídicamente a su causación. Así lo establece el artículo 11 del Código Penal.

Por tanto, el análisis no debe centrarse exclusivamente en el organigrama formal. Debe reconstruir quién tenía capacidad real de control, qué sabía, cuándo lo supo y qué hizo después.

Órgano de administración y responsabilidad de la persona jurídica

La implantación de IA en procesos críticos no es exclusivamente una decisión informática. Puede constituir una cuestión de gobierno corporativo.

En ese caso, los administradores deben actuar con la diligencia de un ordenado empresario, adoptar las medidas necesarias para la buena dirección y control de la sociedad y recabar la información adecuada para cumplir sus obligaciones.

La dirección no tiene que conocer el código fuente de cada modelo, pero sí debe asegurarse de que existen:

- responsables definidos;
- procedimientos de aprobación;
- inventario de sistemas;
- clasificación por criticidad;
- validación independiente;
- recursos humanos suficientes;
- mecanismos de escalado;
- auditorías;
- seguros adecuados;
- planes de contingencia;
- evidencias documentales.

Cuando un delito se comete en beneficio de la empresa y existe un incumplimiento grave de los deberes de supervisión, vigilancia y control, puede plantearse la responsabilidad penal de la persona jurídica en los supuestos expresamente previstos por el Código Penal. La adopción y ejecución eficaz de modelos de organización y gestión adecuados puede tener efectos exoneradores o atenuantes.

Un programa de compliance que no contemple los riesgos algorítmicos puede resultar insuficiente cuando la IA interviene materialmente en decisiones que afectan a la salud pública.

Responsabilidad de la Administración pública y actuación automatizada

Las Administraciones utilizan progresivamente sistemas automatizados para:

- priorizar inspecciones;
- seleccionar operadores de riesgo;
- detectar incumplimientos;
- gestionar alertas;
- analizar resultados oficiales;
- proponer sanciones;
- controlar importaciones;
- evaluar expedientes;
- ordenar actuaciones.

La Ley 40/2015 define la actuación administrativa automatizada como aquella realizada íntegramente por medios electrónicos sin intervención directa de un empleado público y exige identificar los órganos responsables de la definición, programación, mantenimiento, supervisión, control de calidad y, en su caso, auditoría del sistema, así como el órgano responsable de la impugnación.

La Administración no puede alegar que «el sistema lo decidió». El acto sigue siendo administrativo, debe respetar la legalidad, estar suficientemente motivado cuando proceda y poder someterse a control judicial.

Cuando un sistema automatizado cause un daño antijurídico derivado del funcionamiento normal o anormal de los servicios públicos, podrá plantearse la responsabilidad patrimonial conforme a los artículos 32 y siguientes de la Ley 40/2015.

Ahora bien, una autorización, una inspección favorable o la ausencia de actuación administrativa no exonera automáticamente al operador. La responsabilidad primaria de la empresa sobre los alimentos bajo su control sigue existiendo.

CAPÍTULO 4. REGÍMENES DE RESPONSABILIDAD APLICABLES

Los mismos hechos pueden generar consecuencias contractuales, civiles, administrativas y penales. Conviene separar cada régimen, porque sus presupuestos, sujetos, estándares de prueba y finalidades son distintos. La existencia de un error no basta. Antes al contrario, debe existir un incumplimiento, un defecto o una omisión jurídicamente relevante.

La responsabilidad algorítmica como sistema de responsabilidades concurrentes

Cuando una decisión algorítmica produce un resultado incorrecto deben distinguirse, al menos, cuatro planos jurídicos:

1. Incumplimiento regulatorio, aunque todavía no se haya producido un daño efectivo.
2. Responsabilidad contractual, derivada del incumplimiento entre proveedor, integrador, laboratorio y operador.
3. Responsabilidad civil extracontractual o por producto defectuoso, frente a consumidores y terceros perjudicados.
4. Responsabilidad administrativa o penal, cuando la conducta encaje en una infracción o delito.

Estos planos pueden coexistir.

Un modelo de inteligencia artificial puede haber sido suministrado incumpliendo las prestaciones contratadas; puede, además, constituir un producto defectuoso; su utilización puede haber determinado una infracción de la legislación alimentaria y, si se comercializan alimentos nocivos para la salud, la conducta puede alcanzar relevancia penal.

La investigación jurídica no debe buscar prematuramente un único culpable. Debe reconstruir la contribución causal y el deber jurídico de cada participante.

El error algorítmico no implica automáticamente responsabilidad

No todo resultado incorrecto constituye una infracción jurídica.

Un sistema predictivo puede fallar aun habiendo sido:

- correctamente diseñado;
- validado con datos representativos;
- utilizado dentro de su finalidad prevista;
- supervisado por personal competente;
- mantenido conforme al estado de la técnica;
- sometido a controles de contingencia razonables.

La responsabilidad surge cuando el error puede conectarse con un defecto, incumplimiento u omisión jurídicamente relevante.

Por tanto, deben separarse tres conceptos:

1. **Error técnicamente inevitable**

Resultado incorrecto comprendido dentro de la incertidumbre conocida y aceptable del sistema.

2. **Error negligente**

Resultado que podría haberse evitado aplicando la diligencia técnica, profesional u organizativa exigible.

3. **Error doloso o conscientemente tolerado**

Resultado derivado de la utilización del sistema pese a conocerse su inadecuación, sus limitaciones o el riesgo grave que generaba.

Esta distinción es esencial, puesto que el Derecho no exige infalibilidad absoluta, pero sí una gestión razonable, documentada y proporcional del riesgo.

Responsabilidad contractual entre los participantes

La primera controversia suele aparecer entre empresas:

- operador alimentario y proveedor tecnológico;
- fabricante y desarrollador del modelo;
- operador y laboratorio;
- proveedor de IA e integrador;
- fabricante y empresa de mantenimiento;
- distribuidor y fabricante del alimento.

El Código Civil somete a indemnización a quienes incumplen sus obligaciones por dolo, negligencia, morosidad o contravención del contenido contractual. La diligencia exigible se determina atendiendo a la naturaleza de la obligación y a las circunstancias de las personas, el tiempo y el lugar.

En materia algorítmica, el contrato debe permitir determinar con precisión:

- qué producto o servicio se suministra;
- cuál es su finalidad prevista;
- qué matrices, productos y procesos cubre;
- qué prestaciones han sido garantizadas;
- qué tasa de falsos positivos y falsos negativos resulta admisible;
- qué datos debe aportar cada parte;
- quién realiza la validación;
- quién controla las actualizaciones;
- quién conserva los registros;
- quién supervisa el funcionamiento;
- qué ocurre cuando se detecta deriva;
- quién debe comunicar un incidente;
- qué garantías y seguros existen.

Un contrato que se limite a señalar que el proveedor suministra una «solución de inteligencia artificial para mejorar la seguridad alimentaria» es jurídicamente insuficiente.

Obligación de medios y obligación de resultado

No todas las prestaciones tecnológicas tienen la misma naturaleza, y en consecuencia, puede existir una obligación de medios cuando el proveedor se compromete a aplicar conocimientos técnicos diligentes sin garantizar un resultado absoluto, por ejemplo:

- asesorar sobre posibles arquitecturas;
- realizar una prueba de concepto;
- prestar asistencia técnica;
- analizar preliminarmente datos históricos.

Y puede aproximarse a una obligación de resultado cuando se garantiza contractualmente:

- una sensibilidad mínima;
- una tasa máxima de falsos negativos;
- un tiempo de disponibilidad;
- la detección de determinados defectos;
- la generación correcta de una etiqueta;
- la interoperabilidad con una línea específica;
- el cumplimiento de una especificación verificable.

La denominación utilizada por las partes no es definitiva. Lo relevante será el contenido real de la prestación, la publicidad técnica, las métricas prometidas, la documentación entregada y la finalidad conocida por el proveedor.

Incumplimientos típicos del proveedor tecnológico

Podrá existir responsabilidad contractual del proveedor cuando:

- el sistema no alcance las métricas garantizadas;
- se hayan utilizado datos de validación no representativos;
- las prestaciones comunicadas sean engañosas;
- no se hayan revelado limitaciones conocidas;
- el modelo funcione únicamente en condiciones de laboratorio no reproducibles industrialmente;
- una actualización modifique materialmente el rendimiento;
- no se comuniquen vulnerabilidades conocidas;
- no exista el soporte contratado;
- los registros sean insuficientes para reconstruir un incidente;
- el sistema no permita implementar la supervisión humana prometida.

En sistemas de alto riesgo, cuando resulten aplicables las correspondientes obligaciones del Reglamento de Inteligencia Artificial (AI Act), la normativa exige medidas de gestión del riesgo, gobernanza de datos, documentación, conservación de registros, supervisión humana y seguimiento del funcionamiento. El responsable del despliegue debe asignar la supervisión a personas con competencia, formación, autoridad y apoyo suficientes y, cuando controle los datos de entrada, garantizar su pertinencia y representatividad.

Incumplimientos del operador frente al proveedor

La responsabilidad contractual también puede recaer sobre el cliente cuando:

- proporciona datos erróneos o incompletos;
- oculta cambios en la formulación;
- utiliza el sistema fuera del ámbito acordado;
- modifica los umbrales sin autorización;
- conecta sensores no compatibles;
- ignora los requisitos de calibración;
- permite el uso por personal no formado;
- desactiva controles;
- no instala actualizaciones críticas;
- no comunica incidentes o resultados anómalos.

La expresión «el sistema no funcionó» no determina quién incumplió. Puede haber fallado el modelo, pero también los datos de entrada, la integración, el sensor, el procedimiento humano o la configuración realizada por el operador.

Límites de responsabilidad y cláusulas de exoneración

En contratos B2B es habitual limitar la responsabilidad del proveedor a:

- el importe anual del contrato;
- una cantidad máxima;
- los daños directos;
- la reposición del servicio;
- la repetición del análisis;
- la exclusión del lucro cesante.

Estas cláusulas deben revisarse con especial cautela cuando el sistema interviene en seguridad alimentaria.

Una limitación contractual puede regular la relación económica interna entre las partes, pero no elimina:

- las potestades sancionadoras de la Administración;
- los derechos del consumidor;
- la responsabilidad frente a terceros;
- la responsabilidad penal;
- las obligaciones imperativas del operador alimentario.

Además, excluir contractualmente toda responsabilidad por un sistema destinado precisamente a controlar peligros alimentarios puede vaciar de contenido la prestación contratada.

Daños reclamables entre empresas

El daño contractual puede comprender tanto la pérdida efectivamente sufrida como la ganancia dejada de obtener, siempre que exista relación causal y se cumplan los requisitos de previsibilidad y acreditación.

En un incidente algorítmico pueden reclamarse:

- destrucción de producto;
- retirada y recuperación de lotes;
- transporte y logística inversa;
- análisis extraordinarios;
- paralización de líneas;
- sustitución de envases;
- indemnizaciones a clientes;
- penalizaciones de distribuidores;
- campañas de comunicación;
- pérdida de ventas;
- pérdida de contratos;
- costes regulatorios y jurídicos;
- restauración de sistemas;
- auditorías forenses;
- deterioro reputacional, cuando sea jurídicamente acreditable.

La mera estimación interna de una pérdida reputacional no basta. Debe demostrarse el daño, su cuantía y su vinculación causal con el incumplimiento.

Responsabilidad civil extracontractual

Cuando el perjudicado no mantiene una relación contractual con el responsable tecnológico, puede entrar en juego la responsabilidad extracontractual.

El artículo 1902 del Código Civil obliga a reparar el daño causado por acción u omisión cuando intervenga culpa o negligencia. La empresa puede responder asimismo, en determinados supuestos, por los daños ocasionados por sus dependientes en el ejercicio de sus funciones.

Para que exista responsabilidad deberán acreditarse generalmente:

3.una acción u omisión;
4.un daño real;
5.culpa o negligencia, salvo regímenes objetivos especiales;
6.relación de causalidad;
7.imputación jurídica del resultado.

En los sistemas algorítmicos, la principal dificultad suele residir en la causalidad.

El daño puede ser resultado de una cadena compleja:

datos insuficientes → predicción errónea → revisión humana superficial → liberación del lote → ruptura de la cadena de frío → consumo → lesión.

No todos los participantes en esa secuencia responderán necesariamente en la misma medida.

Responsabilidad por productos defectuosos

El alimento defectuoso y el sistema algorítmico defectuoso

Deben diferenciarse dos productos potencialmente defectuosos:

- el alimento finalmente comercializado;
- el software o sistema de inteligencia artificial que intervino en su producción o control.

El régimen español vigente de responsabilidad por productos defectuosos atribuye responsabilidad al productor por los daños causados por un producto que no ofrezca la seguridad legítimamente esperable. En el caso de alimentos destinados al consumo humano, el productor no puede invocar la denominada excepción de riesgos de desarrollo para afirmar que el estado de los conocimientos científicos y técnicos no permitía descubrir el defecto.

Esta previsión resulta especialmente exigente para la industria alimentaria. Así, si el alimento es inseguro, el productor no puede neutralizar la reclamación del consumidor sosteniendo simplemente que el algoritmo utilizado era innovador o que el defecto era difícil de detectar.

La Directiva (UE) 2024/2853

La Directiva (UE) 2024/2853 amplía expresamente el concepto de producto para incluir el software, incluidos los sistemas de inteligencia artificial. También contempla actualizaciones, servicios digitales relacionados, ciberseguridad y modificaciones sustanciales. Los Estados deben transponerla antes del 9 de diciembre de 2026 y su nuevo régimen se aplicará a productos introducidos en el mercado o puestos en servicio desde esa fecha.

Esto permitirá articular de forma más directa reclamaciones contra productores de software defectuoso.

No obstante, deberán diferenciarse cuidadosamente:

- el proveedor del modelo general;
- el fabricante de la aplicación alimentaria;
- el integrador;
- quien realiza una modificación sustancial;
- quien comercializa el sistema bajo su propio nombre;
- el fabricante del alimento.

En un sistema compuesto, pueden existir varios productores jurídicamente relevantes.

¿Cuándo puede considerarse defectuoso un sistema de IA?

Un sistema no es defectuoso por el mero hecho de cometer un error. Sin embargo, puede considerarse defectuoso cuando no ofrece la seguridad que razonablemente cabe esperar atendiendo, entre otros factores, a:

- la finalidad prevista;
- los usuarios previsibles;
- las instrucciones;
- la presentación comercial;
- el nivel de automatización;
- la posibilidad de supervisión;

- el aprendizaje posterior;
- las actualizaciones;
- la ciberseguridad;
- el estado de la técnica;
- la interacción con otros productos;
- el uso razonablemente previsible.

Podrá existir defecto cuando:

- la tasa real de falsos negativos sea materialmente superior a la declarada;
- el sistema no advierta que opera fuera de distribución;
- no detecte datos de entrada físicamente imposibles;
- una actualización elimine controles esenciales;
- no exista mecanismo de parada;
- la interfaz induzca a confiar indebidamente en el resultado;
- los registros sean insuficientes para investigar un incidente;
- la documentación o las advertencias sean inadecuadas;
- el sistema pueda ser manipulado mediante vulnerabilidades previsibles.

Responsabilidad administrativa alimentaria

La responsabilidad administrativa constituye probablemente el riesgo jurídico más inmediato para el operador, pues puede existir infracción aunque no se haya producido una intoxicación efectiva. Basta, según el tipo aplicable, con:

- introducir un alimento inseguro en el mercado;
- incumplir obligaciones de higiene;
- no aplicar correctamente el APPCC;
- omitir información obligatoria;
- no declarar un alérgeno;
- incumplir la trazabilidad;
- no comunicar un riesgo;
- retrasar una retirada;
- obstaculizar el control oficial;
- incumplir medidas ordenadas por la autoridad.

La Ley 17/2011 clasifica las infracciones en leves, graves y muy graves atendiendo, entre otros factores, al riesgo para la salud, la alteración sanitaria, la intencionalidad, la posición del infractor en el mercado, el beneficio obtenido, la generalización y la reincidencia. También permite adoptar medidas como la suspensión, el cierre o la retirada precautoria o definitiva, algunas de las cuales tienen naturaleza de medidas de protección y no de sanción.

No existe una responsabilidad sancionadora puramente objetiva

En el Derecho administrativo sancionador español no debe imponerse una sanción sin dolo, culpa o negligencia por ser esta imposición presunta *in natura contra legem*. El artículo 28 de la Ley 40/2015 exige responsabilidad culpable y la doctrina constitucional rechaza la responsabilidad objetiva en este ámbito.

Sin embargo, la diligencia exigible a un operador profesional es elevada, de tal suerte que la empresa no podrá alegar fácilmente ausencia de culpa cuando:

- no validó el sistema;
- desconocía quién lo supervisaba;
- no conservaba registros;
- no había fijado límites de uso;
- no verificó los datos;
- carecía de procedimiento de contingencia;
- ignoró alertas;
- no evaluó la deriva;
- no incorporó el sistema al APPCC;
- dejó que el algoritmo sustituyera controles obligatorios.

La sanción recaerá normalmente sobre el operador

La autoridad alimentaria dirigirá habitualmente su actuación contra quien:

- fabrica;
- importa;
- distribuye;
- almacena;
- etiqueta;
- comercializa;
- controla el establecimiento;
- introduce el producto en el mercado.

El proveedor tecnológico puede responder conforme al Reglamento de Inteligencia Artificial, a la normativa de mercado o a otras normas, pero esto no desplaza la posición del operador ante la legislación alimentaria.

Después de la sanción, el operador podrá ejercitar acciones de repetición contra el proveedor, laboratorio o integrador cuando el incumplimiento de estos haya contribuido al resultado.

El uso de IA puede agravar la negligencia organizativa

No porque la tecnología sea jurídicamente sospechosa, sino porque su implantación exige controles específicos.

Una empresa que automatiza la liberación de lotes y, simultáneamente:

- reduce personal;
- elimina la doble revisión;
- no audita el modelo;
- no registra las decisiones;
- no comprueba falsos negativos;
- no establece una alternativa manual,

está incrementando voluntariamente su dependencia de una herramienta que no controla suficientemente.

La automatización no rebaja el estándar de diligencia. En decisiones críticas, normalmente lo eleva.

Responsabilidad penal

La responsabilidad penal debe reservarse para conductas que reúnan todos los elementos del delito. No toda infracción alimentaria, fallo técnico o negligencia empresarial es delito. Sin embargo, la utilización de inteligencia artificial no impide que determinados hechos puedan encajar en delitos contra la salud pública.

El Código Penal sanciona, entre otras conductas, la fabricación o venta de bebidas o alimentos nocivos para la salud, el tráfico con productos corrompidos, la elaboración o comercialización de productos no autorizados y perjudiciales, la adulteración con aditivos o agentes no autorizados susceptibles de causar daños y el envenenamiento o adulteración grave de aguas o alimentos destinados al uso público o colectivo. Los hechos cometidos por imprudencia grave reciben también respuesta penal conforme al artículo 367.

La IA como instrumento, no como autor

El sistema algorítmico no puede ser autor penal. En estos casos, la responsabilidad recaerá sobre la persona física que:

- decidió;
- ordenó;
- ejecutó;
- autorizó;
- toleró;
- omitió actuar pese a estar obligada.

El algoritmo será un elemento del hecho, de forma análoga a:

- una máquina mal configurada;
- un instrumento de laboratorio;
- una hoja de cálculo defectuosa;

- un sensor averiado;
- un procedimiento técnico incorrecto.

Comisión por omisión

En los delitos de resultado puede responder quien, teniendo un deber jurídico especial de impedirlo, no evita el resultado cuando su omisión equivale jurídicamente a causarlo.

El artículo 11 del Código Penal exige una obligación legal o contractual específica de actuar o que el propio omitente haya creado previamente la situación de riesgo.

Esta figura puede afectar a:

- responsables de producción;
- responsables de calidad;
- directores técnicos;
- administradores;
- jefes de laboratorio;
- responsables de seguridad alimentaria.

Pero no basta el cargo formal.

Será necesario demostrar:

- la posición de garante;
- el conocimiento o cognoscibilidad del riesgo;
- la capacidad de intervención;
- la omisión de la actuación debida;
- la relación con el resultado.

Imprudencia grave

La frontera entre negligencia administrativa e imprudencia penal grave dependerá de la intensidad del incumplimiento. Podrían aproximarse a la imprudencia grave conductas como:

- liberar repetidamente lotes pese a falsos negativos conocidos;
- ignorar deliberadamente una alerta microbiológica;
- utilizar un modelo de vida útil en matrices totalmente diferentes;
- eliminar la revisión humana para reducir costes;
- mantener un sistema descalibrado;
- destruir registros después del incidente;
- no retirar un alimento pese a indicios sólidos de riesgo grave;
- utilizar una IA generativa no validada como única fuente de formulación o etiquetado.

En cambio, un fallo imprevisible de un sistema correctamente validado no debería convertirse por sí solo en responsabilidad penal.

Responsabilidad penal de la persona jurídica

El Código Penal permite atribuir responsabilidad a la persona jurídica por determinados delitos contra la salud pública. El artículo 366 prevé multas y permite imponer otras consecuencias cuando concurran los requisitos del artículo 31 bis.

La responsabilidad corporativa puede surgir por:

- delitos cometidos por representantes o directivos en nombre o beneficio de la empresa;
- delitos cometidos por subordinados cuando se haya incumplido gravemente el deber de supervisión, vigilancia y control.

Un modelo de organización y gestión eficaz puede producir efectos exoneradores o atenuantes cuando identifica los riesgos, establece protocolos, asigna recursos, dispone de canales de información, aplica controles y se revisa periódicamente.

Por ello, el compliance alimentario debe integrar expresamente la IA.

No basta un código ético genérico. Deben existir controles sobre:

- aprobación de sistemas;
- cambios de finalidad;
- calidad de datos;
- validación;
- competencias humanas;
- trazabilidad;
- actualización;
- incidentes;
- retirada;
- comunicación con autoridades;
- conservación de evidencias.

CAPÍTULO 5. CAUSALIDAD Y ESCENARIOS DE FALLO EN LA PRÁCTICA ALIMENTARIA

En los litigios algorítmicos, la causalidad suele ser más compleja que el error. Un modelo puede fallar sin causar el daño, y un resultado correcto puede convertirse en perjudicial por una decisión humana posterior. Los casos de vida útil, alérgenos, microbiología, liberación de lotes y retiradas muestran que el incidente suele ser multicausal.

Causalidad: el problema central

En un litigio algorítmico no basta demostrar que el modelo se equivocó. Debe demostrarse que el error fue causa jurídicamente relevante del daño.

Causalidad material

Debe preguntarse qué habría ocurrido si el sistema hubiese funcionado correctamente.

Ejemplo:

- El modelo clasificó el lote como conforme.
- Una revisión humana obligatoria tampoco se realizó.
- El lote contenía Listeria monocytogenes.
- El alimento llegó al mercado.

Si una revisión humana correctamente ejecutada habría detectado la contaminación, el daño puede imputarse tanto al fallo tecnológico como al fallo de supervisión.

Si la contaminación se produjo después de la clasificación algorítmica, el error del modelo puede no haber causado el daño.

Causalidad jurídica

Aunque una conducta sea condición material del daño, el resultado debe encontrarse dentro del riesgo que la norma incumplida pretendía evitar.

Si el sistema fue contratado para detectar cuerpos extraños y el daño procede de una formulación incorrecta no relacionada con esa función, no puede atribuirse automáticamente al proveedor. La finalidad prevista y el alcance funcional del sistema serán pruebas centrales.

Interrupción de la cadena causal

La intervención posterior de otra persona puede:

- no alterar la responsabilidad anterior;
- compartirla;
- reducirla;
- romper completamente la causalidad.

No rompe necesariamente la cadena causal:

- una revisión humana superficial y previsible;
- el uso conforme a las instrucciones;
- un error inducido por una interfaz confusa;
- una reacción tardía previsible.

Puede romperla:

- una modificación no autorizada del sistema;
- la utilización consciente fuera de su finalidad;
- la manipulación de registros;
- la desactivación intencionada de una alerta;
- la introducción de datos manifiestamente falsos;
- una contaminación posterior independiente.

Supuestos prácticos

Falso negativo microbiológico

Un modelo predice que un lote refrigerado presenta bajo riesgo microbiológico y recomienda su liberación. Posteriormente se detecta un patógeno.

Operador alimentario

Responderá si comercializó el producto sin controles adecuados, especialmente cuando la predicción sustituyó indebidamente análisis, muestreos o verificaciones exigibles. El Reglamento n.º 178/2002 prohíbe introducir alimentos inseguros en el mercado y obliga al operador a garantizar el cumplimiento y actuar cuando considere que un alimento no cumple los requisitos de seguridad.

Proveedor tecnológico

Podrá responder si:

- prometió capacidad diagnóstica no acreditada;
- ocultó una baja sensibilidad;
- entrenó con datos inadecuados;
- no advirtió que la herramienta no sustituía el análisis;
- modificó el sistema sin revalidación.

Laboratorio

Responderá si el falso negativo deriva de:

- muestreo incorrecto;
- método inadecuado;
- contaminación o pérdida de muestra;
- error de interpretación;
- utilización no validada de IA en el análisis.

Director Técnico

Su responsabilidad dependerá de si aprobó el uso, conocía sus limitaciones, podía impedir la liberación y omitió actuar.

Conclusión

La frase «el algoritmo dio negativo» no exonera a nadie. Debe reconstruirse qué significaba exactamente ese resultado y qué decisiones dependían de él.

Predicción incorrecta de vida útil

Un sistema establece una vida útil de 45 días, pero el producto deja de ser seguro a los 25 días.

Deben examinarse:

- matrices utilizadas para entrenar el modelo;
- variabilidad entre lotes;

- pH;
- actividad de agua;
- atmósfera de envasado;
- carga inicial;
- tratamientos térmicos;
- distribución;
- temperatura real;
- abuso térmico previsible;
- microorganismo objetivo;
- validación mediante challenge test;
- márgenes de seguridad.

La responsabilidad del proveedor aumentará si presentó la predicción como una validación científica completa.

La responsabilidad del operador aumentará si adoptó la vida útil sin estudios propios, sin margen de seguridad o ignorando condiciones distintas de las utilizadas para desarrollar el modelo.

Omisión algorítmica de un alérgeno

Una herramienta genera automáticamente la lista de ingredientes, pero omite un alérgeno.

El operador bajo cuyo nombre se comercializa el alimento es responsable de la información alimentaria y debe garantizar su presencia y exactitud conforme al Reglamento (UE) n.º 1169/2011.

El proveedor puede responder contractualmente si:

- el sistema estaba diseñado para identificar alérgenos;
- la base de datos era incorrecta;
- no actualizó las reglas;
- la herramienta suprimió información existente;
- garantizó conformidad regulatoria.

El operador seguirá siendo responsable si:

- no revisó la etiqueta;
- introdujo mal la formulación;
- no actualizó las materias primas;
- ignoró advertencias;
- utilizó un modelo generativo generalista sin validación.

En este supuesto, la revisión humana no debe ser ornamental. Debe ser una verificación efectiva realizada por una persona competente.

Liberación automática de lotes

Un sistema recibe datos de proceso, análisis e inspección visual y libera automáticamente el lote.

Esta configuración concentra un riesgo elevado porque transforma una recomendación en una decisión ejecutiva.

El operador debería poder demostrar:

- validación integral;
- criterios de aceptación;
- calidad de los datos;
- control de sensores;
- bloqueo ante datos incompletos;
- doble confirmación en peligros críticos;
- registro de versiones;
- supervisión humana;
- procedimiento manual alternativo;
- autoridad para detener el sistema.

Cuanto mayor sea la autonomía, menor puede ser la tolerancia jurídica a controles ambiguos.

Retirada tardía

La IA detecta una señal anómala, pero la empresa la considera un falso positivo y retrasa la retirada. En este supuesto, la cuestión no será únicamente si el algoritmo acertó, sino si la empresa actuó razonablemente ante la incertidumbre.

Deben analizarse:

- gravedad potencial;
- probabilidad;
- población expuesta;
- evidencia disponible;
- antecedentes;
- velocidad de distribución;
- capacidad de localización;
- posibilidad de adoptar una retirada precautoria;
- tiempo transcurrido;
- personas que intervinieron.

El artículo 19 del Reglamento n.º 178/2002 obliga al operador que considere o tenga motivos para pensar que un alimento no cumple los requisitos de seguridad, a iniciar su retirada e informar a la autoridad. Además, si el producto puediera haber llegado al consumidor, puede ser necesario informar eficazmente y recuperar los productos.

No es jurídicamente prudente esperar certeza absoluta cuando existe una sospecha fundada de riesgo grave.

Matriz de atribución orientativa

Esta tabla es únicamente orientativa. La responsabilidad efectiva dependerá de los hechos, los contratos, la regulación sectorial, la causalidad y las pruebas disponibles.

Fallo	Operador alimentario	Proveedor de IA	Laboratorio	Director Técnico	Administración
Datos de producción incorrectos	Alta	Baja o media	Baja	Según intervención	Baja
Modelo mal diseñado	Media	Alta	Baja	Según conocimiento	Baja
Uso fuera de finalidad	Alta	Baja si advirtió	Media si participó	Alta si lo autorizó	Baja
Muestreo defectuoso	Media	Baja	Alta	Según supervisión	Media si control oficial
Omisión de alérgeno	Alta	Media o alta	Baja	Media o alta	Baja
Liberación sin revisión	Alta	Media	Media	Alta si era competente	Baja
Actualización defectuosa	Media	Alta	Baja	Baja o media	Baja
Falta de retirada	Muy alta	Media si ocultó datos	Media si no informó	Alta si podía ordenarla	Media según actuación
Sistema oficial defectuoso	Baja o media	Media	Según caso	No aplicable	Alta potencial

Tabla 3. Matriz orientativa de atribución por tipo de fallo.

Síntesis: automatizar la decisión no automatiza la responsabilidad

La implantación de inteligencia artificial no sustituye los deberes legales existentes. En último caso, los redistribuye, intensifica y los torna más difíciles de probar.

El operador alimentario conserva la responsabilidad primaria sobre los alimentos que produce, transforma o comercializa. El proveedor tecnológico responde por los defectos e incumplimientos que le sean imputables. El laboratorio responde por su actividad analítica. El Director Técnico responde solo cuando sus funciones, conocimiento, capacidad de actuación y conducta permiten una imputación personal. La persona jurídica puede responder por defectos graves de organización y control. La Administración responde por sus propios actos y sistemas, sin que ello elimine automáticamente las obligaciones del operador.

La cuestión correcta no es:

> ***«¿Quién pulsó el botón?»***

La cuestión correcta es:

¿Quién creó el riesgo, quién lo controlaba, quién conocía sus límites, quién podía evitar el resultado y qué hizo cuando aparecieron las primeras señales de fallo?

La responsabilidad jurídica por decisiones algorítmicas es, en última instancia, responsabilidad por el gobierno de la tecnología.

CAPÍTULO 6. PRUEBA, EXPLICABILIDAD Y TRAZABILIDAD ALGORÍTMICA

La mayor parte de las controversias se decide en el terreno probatorio. No basta conservar millones de datos, sino que es necesario poder identificar la versión del sistema, las entradas, la salida, la intervención humana y la decisión ejecutada. La trazabilidad algorítmica forma parte de la diligencia, no es un trámite posterior al incidente.

La prueba del fallo algorítmico: donde se decide realmente la responsabilidad

Determinar quién debía controlar el riesgo es solo la primera parte del problema. La segunda, normalmente más difícil, consiste en probar qué ocurrió dentro del sistema, con qué datos operó, qué resultado produjo, quién lo recibió y cómo se transformó ese resultado en una decisión empresarial.

En los procedimientos relacionados con inteligencia artificial rara vez existe una prueba única y concluyente. La responsabilidad suele reconstruirse mediante la combinación de:

- registros automáticos;
- versiones del modelo;
- datos de entrada;
- resultados producidos;
- correos electrónicos;
- actas de validación;
- procedimientos internos;
- informes de laboratorio;
- historiales de mantenimiento;
- declaraciones de empleados;
- decisiones humanas posteriores;
- documentación contractual;
- informes periciales.

La dificultad no es meramente tecnológica. Es también organizativa y jurídica.

Una empresa puede disponer de millones de registros informáticos y, aun así, ser incapaz de demostrar:

- qué versión exacta del modelo intervino;
- qué parámetros estaban activos;
- si el sensor estaba calibrado;
- qué datos fueron descartados;
- quién revisó la alerta;

- por qué se liberó el lote;
- cuándo comenzó a conocerse el problema;
- por qué no se adoptaron medidas antes.

En materia de responsabilidad algorítmica, tener datos no equivale a tener prueba. La prueba requiere integridad, contextualización, trazabilidad, autenticidad y capacidad de interpretación.

Qué debe probar cada parte

El perjudicado

El consumidor, cliente, distribuidor u operador perjudicado deberá normalmente acreditar:

1. la existencia de un daño.
2. la intervención del producto o sistema.
3. el defecto, incumplimiento o conducta negligente.
4. la relación causal entre el fallo y el daño.
5. la identificación del sujeto responsable.

En sistemas opacos o distribuidos, esta carga puede resultar extraordinariamente difícil porque la mayor parte de la información está bajo control del fabricante del software, del proveedor tecnológico o del operador alimentario.

El operador alimentario

La empresa deberá poder demostrar:

- que seleccionó una tecnología adecuada;
- que evaluó sus riesgos;
- que validó el sistema en condiciones representativas;
- que delimitó su finalidad;
- que formó a los usuarios;
- que estableció supervisión humana;
- que conservó los registros relevantes;
- que vigiló su funcionamiento;
- que reaccionó ante las desviaciones;
- que no sustituyó indebidamente controles obligatorios.

El proveedor tecnológico

El proveedor deberá poder acreditar:

- las prestaciones reales del sistema;
- el origen y calidad de los datos;
- la metodología de entrenamiento;
- la validación;
- las limitaciones comunicadas;
- las versiones suministradas;
- las actualizaciones realizadas;
- la documentación entregada;
- los incidentes conocidos;
- las medidas de seguridad y vigilancia.

El Director Técnico o responsable de calidad

El profesional deberá poder demostrar:

- cuál era su ámbito real de funciones;
- qué información recibió;
- qué decisiones tomó;
- qué advertencias formuló;
- qué recursos solicitó;
- si tenía capacidad para paralizar el proceso;

- si su criterio fue desatendido;
- si actuó con la diligencia profesional exigible.

Esta última cuestión es particularmente importante, dado que en una investigación, la ausencia de constancia documental puede convertir una advertencia real en una advertencia jurídicamente inexistente.

Las seis capas de la evidencia algorítmica

Una investigación solvente debe separar, al menos, seis niveles probatorios.

1. Capa contractual

Permite determinar qué se compró realmente.

Debe incluir:

- contrato principal;
- anexos técnicos;
- niveles de servicio;
- documentación precontractual;
- presentaciones comerciales;
- métricas comprometidas;
- límites de uso;
- garantías;
- responsabilidades;
- obligaciones de actualización;
- derechos de auditoría;
- acceso a registros.

Esta capa es esencial porque el proveedor puede afirmar que el sistema era meramente orientativo, mientras que la documentación comercial lo presentaba como una solución de liberación automática o de garantía de conformidad.

2. Capa de datos

Debe reconstruirse:

- fuente de los datos;
- fecha de obtención;
- método de captura;
- integridad;
- transformaciones;
- exclusiones;
- imputaciones;
- etiquetado;
- representatividad;
- calidad;
- posibles sesgos;
- variables ausentes.

En industria alimentaria deben considerarse, entre otros:

- formulación;
- proveedor de materias primas;
- lote;
- pH;
- actividad de agua;
- humedad;
- temperatura;
- tiempo;
- atmósfera;
- proceso térmico;
- carga microbiana;

- resultados de laboratorio;
- condiciones logísticas.

Un modelo puede ser matemáticamente correcto y producir un resultado incorrecto porque recibió datos falsos, incompletos, desactualizados o pertenecientes a una unidad de medida distinta.

3. Capa del modelo

Debe identificar:

- modelo utilizado;
- arquitectura;
- fecha de entrenamiento;
- conjunto de entrenamiento;
- conjunto de validación;
- versión;
- hiperparámetros;
- umbrales;
- métricas;
- límites conocidos;
- modificaciones;
- actualizaciones;
- componentes de terceros.

No basta con señalar el nombre comercial de la herramienta. Dos ejecuciones realizadas con versiones diferentes pueden producir resultados distintos.

4. Capa operativa

Permite conocer cómo se utilizó el sistema en el caso concreto:

- fecha y hora;
- usuario;
- dispositivo;
- datos de entrada;
- salida;
- nivel de confianza;
- alerta generada;
- estado de sensores;
- incidencias;
- intervención manual;
- conexión con otros sistemas;
- acción ejecutada.

5. Capa humana

Debe reconstruir:

- quién vio el resultado;
- qué formación tenía;
- qué comprendió;
- si podía contradecir al sistema;
- si existía presión productiva;
- si revisó los datos;
- si solicitó una segunda comprobación;
- si documentó la decisión;
- quién autorizó finalmente el lote.

6. Capa de respuesta al incidente

Debe recoger:

- primera señal de anomalía;
- momento de conocimiento;

- personas informadas;
- investigaciones iniciadas;
- lotes afectados;
- medidas cautelares;
- comunicación a clientes;
- información a autoridades;
- retirada;
- recuperación;
- correcciones del sistema.

La cronología suele ser más importante que el discurso defensivo posterior.

Los registros automáticos y el Reglamento de Inteligencia Artificial

El artículo 12 del Reglamento de Inteligencia Artificial exige que los sistemas de alto riesgo permitan técnicamente el registro automático de acontecimientos durante su funcionamiento. Los registros deben facilitar la trazabilidad, la vigilancia del sistema, la detección de situaciones de riesgo y la investigación posterior.

El artículo 26 exige a los responsables del despliegue conservar los registros generados automáticamente que estén bajo su control durante un período adecuado y, como mínimo, durante seis meses, salvo que otra norma europea o nacional disponga algo diferente.

Tras la reforma introducida por el *AI Omnibus*, las obligaciones específicas para los sistemas de alto riesgo del anexo III se aplicarán desde el 2 de diciembre de 2027 y las relativas a sistemas integrados en productos del anexo I desde el 2 de agosto de 2028. El resto del Reglamento de Inteligencia Artificial comenzó a aplicarse, con sus excepciones, el 2 de agosto de 2026.

Sin embargo, sería un error concluir que una empresa alimentaria puede esperar hasta esas fechas para conservar evidencias.

La obligación práctica de documentar el funcionamiento puede derivar ya de:

- la legislación alimentaria;
- el APPCC;
- la trazabilidad;
- las normas de calidad;
- la diligencia profesional;
- el contrato;
- la necesidad de defenderse en un procedimiento;
- las obligaciones generales de seguridad.

Además, los plazos mínimos del Reglamento de Inteligencia Artificial no deben confundirse con el período de conservación jurídicamente recomendable.

Seis meses pueden resultar insuficientes cuando:

- la vida útil del producto es prolongada;
- el daño se manifiesta tardíamente;
- existe un período largo de distribución;
- el contrato tiene varios años de duración;
- la acción de responsabilidad puede ejercitarse posteriormente;
- el registro resulta necesario para acreditar una validación histórica.

La política de conservación debe vincularse al riesgo, a la vida comercial del producto y a los posibles plazos de reclamación, no únicamente al mínimo regulatorio.

Qué debe contener un registro algorítmico útil

Un log que se limita a indicar:

> ***«Resultado: conforme»***

tiene un valor probatorio muy reducido.

Un registro técnicamente defendible debería permitir identificar:

El registro debe permitir diferenciar:

- lo que propuso la IA;
- lo que entendió el usuario;
- lo que decidió la empresa;
- lo que finalmente se ejecutó.

Confundir estas fases puede conducir a atribuir al algoritmo una decisión que, jurídicamente, fue humana.

Elemento	Información mínima
Sistema	Nombre, proveedor y finalidad
Versión	Modelo, software, reglas y configuración
Momento	Fecha, hora y zona horaria
Identificador	Lote, muestra, línea, equipo o expediente
Entrada	Datos utilizados y fuente
Calidad del dato	Valores ausentes, anomalías y advertencias
Salida	Predicción, clasificación o recomendación
Confianza	Probabilidad, intervalo o indicador aplicable
Umbral	Criterio que activa aceptación, rechazo o revisión
Usuario	Persona o sistema que ejecutó la consulta
Supervisión	Persona que revisó el resultado
Decisión final	Aceptación, rechazo, bloqueo, retirada o repetición
Excepción	Razón de cualquier modificación manual
Integridad	Firma, sello de tiempo, hash o mecanismo equivalente
Vinculación	Referencia a informes, análisis y documentos relacionados

Tabla 5. Contenido mínimo de un registro algorítmico útil.

Carga de la prueba y facilidad probatoria

El artículo 217 de la Ley de Enjuiciamiento Civil establece las reglas generales sobre carga de la prueba. El demandante debe acreditar los hechos constitutivos de su pretensión y el demandado los hechos impeditivos, extintivos o excluyentes. No obstante, el tribunal debe tener en cuenta la disponibilidad y facilidad probatoria de cada parte. Este criterio resulta especialmente relevante en litigios algorítmicos.

El consumidor puede saber:

- que enfermó;
- qué producto consumió;
- cuándo lo adquirió;
- cuál fue el diagnóstico.

Pero normalmente no puede saber:

- qué modelo liberó el lote;
- con qué versión;
- qué tasa de error tenía;
- qué alertas se ignoraron;
- qué actualización estaba instalada;
- qué datos utilizó;
- qué comunicaciones existieron entre proveedor y operador.

Esta asimetría no supone una inversión automática y general de la carga de la prueba, pero puede influir de forma decisiva en la valoración judicial.

Una empresa que controla toda la evidencia tecnológica y no la conserva, no la aporta o la presenta de forma incompleta se sitúa en una posición procesal muy débil.

Exhibición de documentos y acceso a la evidencia

La Ley de Enjuiciamiento Civil permite solicitar la exhibición de documentos relevantes que se encuentren bajo el control de la contraparte y, en determinadas condiciones, de terceros. También reconoce como medios de prueba los instrumentos que permiten archivar, conocer o reproducir datos, cifras y operaciones relevantes para el proceso.

En un litigio sobre IA podrían solicitarse:

- logs;
- modelos o versiones;
- expedientes de validación;
- métricas;
- comunicaciones internas;
- informes de incidencias;
- historial de actualizaciones;
- documentación de sensores;
- datos de entrenamiento relevantes;
- instrucciones de uso;
- auditorías;
- alertas;
- decisiones humanas registradas.

La negativa injustificada a exhibir documentos puede producir consecuencias probatorias adversas conforme a la Ley de Enjuiciamiento Civil. Es por ello evidente que la empresa no debe confiar en que la complejidad técnica o el almacenamiento en un proveedor externo impedirán el acceso a la información.

Si los registros son relevantes, la externalización de la infraestructura no elimina el deber de colaboración ni sustituye la necesidad de disponer contractualmente de derechos de acceso.

La nueva Directiva de productos defectuosos y las presunciones probatorias

La Directiva (UE) 2024/2853 incorpora mecanismos destinados a reducir las dificultades probatorias de lEl órgano jurisdiccional podrá ordenar al demandado la exhibición de pruebas pertinentes que estén bajo su control, siempre de forma necesaria y proporcionada. La Directiva también introduce presunciones refutables de defecto o causalidad en determinados supuestos.

Podrá presumirse el carácter defectuoso cuando, entre otras circunstancias:

- el demandado incumpla la obligación de exhibir pruebas;
- el producto no cumpla requisitos obligatorios de seguridad;
- resulte evidente que el daño fue causado por un funcionamiento manifiestamente defectuoso durante un uso razonablemente previsible.

También podrán aplicarse presunciones cuando el perjudicado se enfrente a dificultades excesivas para acreditar el defecto o el nexo causal debido a la complejidad técnica o científica y pueda demostrar que es probable que el producto fuera defectuoso o que el defecto causara el daño. Las presunciones son refutables por el demandado.

La Directiva debe transponerse antes del 9 de diciembre de 2026 y se aplicará a productos introducidos en el mercado o puestos en servicio desde esa fecha. Por tanto, a 6 de agosto de 2026 todavía no constituye el régimen directamente aplicable a productos anteriores, pero debe condicionar desde ahora el diseño documental de los fabricantes y proveedores.

La consecuencia empresarial es evidente, y de acuerdo con esta prevision normativa: ***Quien no pueda explicar y documentar razonablemente su producto tendrá cada vez más dificultades para destruir las presunciones que puedan operar en su contra.***

El secreto empresarial no es un derecho a ocultar la prueba

Los proveedores suelen invocar:

- código fuente;
- arquitectura;
- pesos del modelo;
- datos de entrenamiento;
- parámetros;
- metodologías;
- documentación técnica,

como secretos empresariales.

La protección puede ser legítima. Sin embargo, el secreto empresarial no constituye un derecho absoluto a impedir la investigación de un daño.

La Ley 1/2019 permite que los órganos judiciales adopten medidas específicas para proteger la confidencialidad:

- restringir el acceso a documentos;
- limitar las personas que pueden asistir a determinadas vistas;
- facilitar versiones no confidenciales;
- ocultar pasajes sensibles;
- mantener el deber de confidencialidad incluso después del procedimiento.

Por tanto, el conflicto no debe plantearse como una elección absoluta entre:

- revelar públicamente el modelo; o
- impedir todo acceso.

Existen soluciones intermedias:

- acceso exclusivo de peritos;
- sala de confidencialidad;
- revisión por experto independiente;
- entrega parcial;
- documentación anonimizada;
- extracción de métricas;
- auditoría bajo deber de secreto;
- informe técnico sin difusión del código.

La protección del secreto debe ser compatible con la tutela judicial efectiva y el derecho de defensa.

Explicabilidad no significa entregar el código fuente

En el debate sobre IA se utiliza con frecuencia el término «*explicabilidad*» de forma imprecisa.

Pueden distinguirse varios niveles.

1. Explicación funcional

Responde a:

- para qué sirve;
- qué decisión apoya;
- qué entradas utiliza;
- qué salida produce;
- cuáles son sus límites.

2. Explicación técnica

Analiza:

- arquitectura;
- entrenamiento;
- variables;

- parámetros;
- métricas;
- sensibilidad;
- robustez;
- validación.

3. Explicación individual

Pretende identificar por qué el sistema produjo un resultado concreto para un lote, muestra o expediente.

4. Explicación causal

Busca determinar qué factores fueron determinantes y si el resultado habría cambiado modificando alguna variable.

5. Explicación jurídica

Permite comprender:

- qué norma o criterio se aplicó;
- quién tomó la decisión;
- qué controles existían;
- por qué la actuación fue considerada diligente.

Una descarga de miles de líneas de código no constituye necesariamente una explicación útil. Del mismo modo, una frase comercial como «*el sistema utiliza algoritmos avanzados*» tampoco satisface una exigencia de transparencia.

La explicación debe ser adecuada al destinatario:

- técnico;
- auditor;
- autoridad;
- órgano judicial;
- consumidor;
- perito.

Resolución	Principio útil para el análisis
TJUE, asuntos C-503/13 y C-504/13, Boston Scientific	La seguridad legítimamente esperable y el riesgo anormal de fallo pueden sustentar la apreciación de defecto en productos pertenecientes a una misma serie.
TJUE, asunto C-621/15, W y otros / Sanofi Pasteur	La prueba del defecto y de la causalidad puede apoyarse en indicios sólidos, concretos y concordantes, sin convertirlos en una presunción automática.
TJUE, asunto C-315/05, Lidl Italia	La posición del distribuidor y su capacidad real de verificar o influir en la información son relevantes al delimitar obligaciones.
STC 76/1990, de 26 de abril	El Derecho administrativo sancionador excluye la responsabilidad puramente objetiva y exige culpabilidad, al menos a título de negligencia.

Tabla 4. Anclajes jurisprudenciales de utilidad interpretativa.

La prueba pericial algorítmica

La Ley de Enjuiciamiento Civil permite aportar dictámenes periciales cuando sean necesarios conocimientos científicos, técnicos o prácticos para valorar hechos relevantes. En un incidente alimentario relacionado con IA rara vez será suficiente un único perfil profesional.

La pericial debería integrar, según el caso:

- ciencia y tecnología de los alimentos;
- microbiología;
- química;
- toxicología;
- ingeniería de procesos;
- metrología;

- ciencia de datos;
- informática forense;
- ciberseguridad;
- regulación alimentaria;
- análisis jurídico.

Un **informático** puede determinar cómo funcionó el modelo, pero no necesariamente si la vida útil era microbiológicamente segura.

Un **microbiólogo** puede valorar el riesgo de crecimiento, pero no necesariamente si los registros fueron manipulados.

Un **jurista** puede interpretar las obligaciones, pero no evaluar por sí solo la representatividad del conjunto de validación.

La pericial debe responder preguntas concretas:

1) ¿Qué sistema intervino?
2) ¿Qué versión estaba activa?
3) ¿Qué datos recibió?
4) ¿Eran correctos y representativos?
5) ¿El sistema se utilizó dentro de su finalidad?
6) ¿Qué resultado produjo?
7) ¿Era técnicamente razonable?
8) ¿Qué controles debían aplicarse?
9) ¿Qué intervención humana existió?
10) ¿El fallo causó el daño?
11) ¿Podría haberse evitado?
12) ¿Qué participante controlaba cada riesgo?

Integridad, autenticidad y cadena de custodia digital

Los registros deben preservarse de forma que pueda demostrarse que:

- existían en una fecha determinada;
- no fueron alterados;
- proceden del sistema indicado;
- están completos;
- se corresponden con el lote investigado;
- la copia examinada coincide con el original.

La Ley de Enjuiciamiento Civil regula la fuerza probatoria de los documentos electrónicos y permite discutir su autenticidad, integridad, fecha y hora. Los servicios electrónicos de confianza pueden reforzar la acreditación de estas características.

Entre las medidas técnicas recomendables se encuentran:

- sellos de tiempo;
- firmas electrónicas;
- hashes;
- almacenamiento inmutable;
- control de accesos;
- registros de auditoría;
- copias forenses;
- versionado;
- segregación de funciones;
- documentación de cada extracción.

Una captura de pantalla aislada tiene menor valor que un registro exportado de forma controlada, con metadatos y verificación de integridad.

Protocolo de preservación inmediata ante un incidente

Cuando aparece una sospecha razonable, la empresa debe activar un protocolo de preservación de evidencias.

Fase 1. Bloqueo

- impedir el borrado automático;
- suspender rotaciones de logs;
- congelar la versión del modelo;
- preservar las configuraciones;
- bloquear modificaciones no autorizadas.

Fase 2. Identificación

- determinar sistemas afectados;
- identificar lotes;
- localizar usuarios;
- identificar proveedores;
- acotar el período temporal.

Fase 3. Copia forense

- realizar exportaciones verificadas;
- conservar metadatos;
- calcular hashes;
- documentar quién interviene;
- mantener originales intactos.

Fase 4. Cronología

- primera alerta;
- decisiones;
- comunicaciones;
- análisis;
- medidas;
- retirada;
- modificaciones.

Fase 5. Separación

Deben distinguirse:

- documentación técnica;
- investigación interna;
- comunicaciones jurídicas;
- comunicaciones regulatorias;
- comunicaciones comerciales.

Fase 6. Custodia

- responsable;
- ubicación;
- acceso;
- plazo;
- inventario;
- historial de modificaciones.

Modificar el sistema inmediatamente después del incidente sin conservar la versión anterior puede destruir la posibilidad de conocer qué ocurrió.

Errores probatorios frecuentes

Conservar solo el resultado final

No permite saber por qué se produjo.

No identificar la versión del modelo

Impide reproducir la decisión.

Sobrescribir registros

Destruye la secuencia histórica.

Mezclar pruebas y reconstrucciones posteriores

Un documento elaborado después del incidente no equivale a un registro contemporáneo.

No conservar las advertencias del sistema

Puede ofrecer una imagen falsa de seguridad.

Carecer de registro de intervención humana

Impide determinar si existió supervisión efectiva.

Basarse exclusivamente en capturas de pantalla

Dificulta acreditar autenticidad e integridad.

Alegar secreto empresarial de forma indiscriminada

Puede interpretarse como resistencia a la investigación.

Modificar el modelo antes del análisis forense

Impide reproducir el fallo.

Elaborar una narrativa corporativa antes de fijar los hechos

La investigación debe preceder a la conclusión, no al contrario.

Ejemplo completo: retirada de producto refrigerado

Una empresa utiliza un modelo para estimar el riesgo de crecimiento de *Listeria monocytogenes*. El sistema recomienda 35 días de vida útil. A los 22 días se detectan resultados positivos en unidades comercializadas.

La investigación debe reconstruir:

Datos

- formulación real;
- pH;
- actividad de agua;
- carga inicial;
- tratamiento térmico;
- contaminación posterior;
- temperaturas registradas.

Modelo

- versión;
- población microbiana considerada;
- condiciones de entrenamiento;
- margen de seguridad;
- tasa de error;
- límites declarados.

Validación

- challenge test;
- lotes analizados;
- variabilidad;
- condiciones de abuso;
- fecha de validación;
- cambios posteriores.

Decisión humana

- quién aprobó 35 días;

- qué documentación revisó;
- si existían discrepancias;
- si se aplicó margen adicional;
- si se consultó al laboratorio.

Incidente

- primera señal;
- lotes afectados;
- distribución;
- reacción;
- comunicación;
- retirada;
- modificación del sistema.

La responsabilidad puede recaer de manera concurrente en:

- proveedor, por sobreestimar la capacidad predictiva;
- integrador, por configurar incorrectamente variables;
- laboratorio, por una validación defectuosa;
- operador, por adoptar la vida útil sin verificación suficiente;
- Director Técnico, si conocía las limitaciones y autorizó el uso;
- administradores, si impusieron una automatización sin controles.

El informe pericial no debe limitarse a afirmar que el modelo falló, sino que debe determinar qué fallo fue causal, quién podía detectarlo y qué barrera de seguridad dejó de funcionar.

Expediente probatorio mínimo de una decisión algorítmica alimentaria

Toda decisión crítica debería generar un expediente compuesto, como mínimo, por:

8. identificación del producto y lote;
9. finalidad de la decisión;
10. sistema y versión;
11. datos de entrada;
12. controles de calidad del dato;
13. resultado algorítmico;
14. nivel de confianza;
15. advertencias;
16. revisión humana;
17. decisión definitiva;
18. identidad del responsable;
19. documentos de soporte;
20. fecha y hora;
21. evidencia de integridad;
22. incidencias posteriores.

Este expediente no debe concebirse como una carga burocrática añadida.

Es simultáneamente:

- mecanismo de control;
- herramienta de calidad;
- soporte regulatorio;
- defensa contractual;
- prueba judicial;
- instrumento de aprendizaje.

Síntesis: lo que no puede reconstruirse difícilmente puede defenderse

La opacidad algorítmica no constituye por sí sola una prueba de responsabilidad. Pero la imposibilidad de reconstruir una decisión crítica puede convertirse en un indicio muy perjudicial contra quien tenía el control de la información.

Es claro que una empresa no necesita explicar matemáticamente cada operación interna del modelo. Pero en cambio sí necesita poder demostrar:

- qué sistema utilizó;
- para qué;
- con qué datos;
- con qué límites;
- bajo qué validación;
- con qué supervisión;
- qué decisión adoptó;
- por qué actuó como lo hizo.

En responsabilidad algorítmica, la documentación no es una formalidad posterior. Forma parte de la propia diligencia. Una decisión alimentaria que no deja rastro verificable es una decisión jurídicamente indefendible.

El verdadero objetivo de la trazabilidad algorítmica no es conocer cada cálculo interno, sino evitar que, cuando aparezca el daño, todos los participantes puedan afirmar que la decisión pertenecía a otro.

Figura 3. Capas de reconstrucción de la evidencia algorítmica.

CAPÍTULO 7. GOBIERNO CORPORATIVO, APPCC DIGITAL Y SUPERVISIÓN HUMANA

El gobierno de la inteligencia artificial debe integrarse en el sistema de gestión de la empresa. El inventario, la clasificación de criticidad, la validación contextual, el control de cambios y la supervisión humana son prolongaciones del APPCC y del deber de organización. El Director Técnico desempeña un papel relevante, pero su responsabilidad depende de funciones y autoridad reales.

Gobierno corporativo de la inteligencia artificial en la industria alimentaria

La prevención de la responsabilidad jurídica no comienza cuando se produce una intoxicación, una retirada o una inspección. Comienza en el momento en que la empresa decide incorporar un sistema algorítmico a una actividad relevante.

Una organización diligente debe poder responder, antes de utilizar la herramienta, a cinco preguntas:

1. ¿Qué decisión apoyar o ejecutar?
2. ¿Qué riesgo produciría un resultado incorrecto?
3. ¿Quién conserva la autoridad final?
4. ¿Cómo se comprobará su funcionamiento?
5. ¿Qué ocurrirá cuando el sistema falle?

Cuando ninguna persona puede contestarlas con precisión, la empresa no dispone de un verdadero gobierno de la inteligencia artificial. Dispone únicamente de tecnología instalada.

El gobierno corporativo de la IA puede definirse como el conjunto de competencias, políticas, controles, responsabilidades y evidencias mediante el que una organización dirige y supervisa el ciclo de vida de sus sistemas algorítmicos.

Este gobierno debe abarcar:

- selección;
- adquisición;
- desarrollo;
- validación;
- integración;
- autorización de uso;
- supervisión;
- modificación;
- vigilancia;
- respuesta a incidentes;
- retirada del sistema.

No constituye una responsabilidad exclusiva del departamento informático. En una empresa alimentaria intervienen necesariamente:

- Dirección General;
- Dirección Técnica;
- Calidad y Seguridad Alimentaria;
- Producción;
- Laboratorio;
- Informática;
- Protección de Datos;
- Ciberseguridad;
- Prevención de Riesgos Laborales;
- Asesoría Jurídica;
- Compliance;
- Compras;
- Recursos Humanos.

La dimensión tecnológica debe integrarse en el sistema general de gestión. Mantener un programa de IA separado de APPCC, calidad, compliance y gobierno corporativo crea silos que dificultan la detección de riesgos y favorecen la dispersión de responsabilidades.

El inventario algorítmico: no puede gobernarse lo que la empresa desconoce

La primera obligación organizativa consiste en identificar todos los sistemas algorítmicos utilizados. El inventario no debe limitarse a las herramientas denominadas comercialmente «inteligencia artificial». Debe incluir sistemas que:

- clasifican;
- predicen;
- recomiendan;
- detectan anomalías;
- calculan umbrales;
- generan documentación;
- asignan prioridades;

- automatizan actuaciones;
- modifican parámetros de proceso.

También deben registrarse soluciones incorporadas indirectamente a:

- maquinaria;
- equipos de visión;
- sistemas de laboratorio;
- ERP;
- software de formulación;
- aplicaciones de mantenimiento;
- plataformas de proveedores;
- soluciones de trazabilidad;
- herramientas de etiquetado;
- servicios en la nube.

Ficha mínima del inventario

Deben incluirse las herramientas gratuitas o generalistas utilizadas informalmente por los trabajadores. Una parte significativa del riesgo puede surgir de la denominada IA en la sombra: aplicaciones no autorizadas que reciben formulaciones, resultados analíticos, información de clientes o documentación confidencial sin control empresarial.

Campo	Contenido
Identificación	Nombre comercial e identificador interno
Proveedor	Fabricante, distribuidor e integrador
Titular interno	Departamento responsable
Finalidad	Decisión o proceso en el que interviene
Producto afectado	Matrices, líneas y categorías
Tipo de resultado	Predicción, clasificación, recomendación o actuación
Nivel de automatización	Informativo, asistido, semiautomático o automático
Consecuencia del error	Calidad, legalidad, seguridad, salud o continuidad
Datos utilizados	Fuente, periodicidad y responsable
Validación	Fecha, alcance, responsable y resultado
Supervisión	Persona o función asignada
Versión	Software, modelo y configuración
Proveedor externo	Acceso, soporte, mantenimiento y subcontratistas
Evidencias	Logs, informes, instrucciones y auditorías
Estado	Piloto, validado, activo, suspendido o retirado

Tabla 6. Ficha mínima del inventario algorítmico.

Clasificación interna por criticidad

La clasificación jurídica del Reglamento de Inteligencia Artificial no sustituye la evaluación interna del riesgo alimentario a practicar por el servicio correspondiente o delegado. Un sistema puede no ser jurídicamente de alto riesgo conforme al Reglamento de Inteligencia Artificial y, sin embargo, ser crítico para la seguridad alimentaria de una empresa concreta.

Por ejemplo, una herramienta que determina si un lote debe liberarse puede no encajar automáticamente en las categorías de alto riesgo del anexo III, pero su fallo podría producir un daño grave para la salud.

El AI Act establece requisitos reforzados para los sistemas jurídicamente clasificados como de alto riesgo, incluidos gestión de riesgos, documentación, registros, supervisión humana, exactitud, robustez y ciberseguridad. Tras la reforma vigente desde el 27 de julio de 2026, las obligaciones relativas a los sistemas de alto riesgo del

anexo III comenzarán a aplicarse el 2 de diciembre de 2027, mientras que las correspondientes a determinados sistemas integrados en productos regulados se aplicarán desde el 2 de agosto de 2028.

Y las empresas alimentarias no deben esperar a que una herramienta quede formalmente incluida en esas categorías. Deben establecer su propia clasificación atendiendo a la gravedad y probabilidad del daño.

Propuesta de niveles de criticidad

Nivel I. Auxiliar

El sistema no produce efectos directos sobre la conformidad o seguridad.

Ejemplos:

- resumen de documentación;
- previsión comercial;
- generación de ideas;
- clasificación administrativa;
- traducción preliminar.

Nivel II. Relevante

El resultado influye en una decisión técnica, pero existe comprobación independiente obligatoria.

Ejemplos:

- recomendación de formulación;
- predicción preliminar de vida útil;
- selección de muestras;
- revisión asistida de etiquetas;
- detección de tendencias analíticas.

Nivel III. Crítico

El resultado condiciona directamente:

- liberación de lotes;
- tratamiento térmico;
- dosificación;
- declaración de alérgenos;
- aceptación de materia prima;
- valoración microbiológica;
- retirada;
- evaluación de peligros.

Nivel IV. Crítico automatizado

El sistema ejecuta o desencadena una actuación con impacto directo sobre seguridad o conformidad sin revisión humana previa en cada caso.

Cuanto mayor sea el nivel, más exigentes deben ser:

- validación;
- segregación de funciones;
- supervisión;
- trazabilidad;
- ciberseguridad;
- auditoría;
- aprobación jerárquica;
- contingencia.

Integración de la IA en el sistema APPCC

El artículo 5 del Reglamento (CE) n.º 852/2004 obliga a los operadores a establecer, aplicar y mantener procedimientos permanentes basados en los principios APPCC. Estos procedimientos deben revisarse cuando se introduzca una modificación en el producto, el proceso o cualquiera de sus fases.

La implantación de una herramienta algorítmica puede constituir una modificación relevante cuando:

- sustituye una comprobación;
- modifica la frecuencia de muestreo;
- selecciona unidades para análisis;
- controla un límite crítico;
- activa una acción correctiva;
- recomienda la liberación;
- modifica una formulación;
- determina una vida útil;
- interpreta un resultado.

Por tanto, no basta con instalarla desde el departamento informático. Debe evaluarse dentro del equipo APPCC.

La IA no es un peligro; puede ser fuente, detector o barrera

Conviene evitar una formulación simplista según la cual «la IA es un peligro APPCC».

Dependiendo del caso, el sistema puede actuar como:

Fuente de peligro

Cuando un error algorítmico introduce o incrementa un riesgo.

Ejemplo: dosificación incorrecta de un conservante.

Herramienta de detección

Cuando identifica desviaciones.

Ejemplo: visión artificial para detectar cuerpos extraños.

Medida de control

Cuando interviene activamente para mantener un peligro dentro de límites aceptables.

Ejemplo: ajuste automático de un tratamiento térmico.

Elemento de verificación

Cuando revisa tendencias, registros o resultados.

Ejemplo: detección de desviaciones históricas en temperaturas.

Esta distinción determina la intensidad de la validación requerida.

Análisis de peligros algorítmicos

El equipo APPCC debe valorar, al menos:

¿Puede la IA controlar un punto crítico?

En abstracto, sí, pero no por el mero hecho de que el proveedor lo afirme.

Si un sistema interviene en un punto de control crítico debe demostrarse:

- que el parámetro controlado es adecuado;
- que el método de medición es fiable;
- que el límite crítico está científicamente justificado;
- que el sistema detecta la pérdida de control;
- que la respuesta se produce a tiempo;
- que existe verificación independiente;
- que el fallo conduce a un estado seguro;
- que se conservan registros;
- que existe una alternativa operativa.

Una IA que controla un tratamiento térmico no puede quedar configurada para continuar silenciosamente cuando pierde la conexión con un sensor. El diseño seguro exige que la ausencia o incoherencia de datos provoque bloqueo, alarma o transición a un procedimiento de contingencia.

Riesgo algorítmico	Posible consecuencia alimentaria
Datos incompletos	Liberación de producto no conforme
Sensor descalibrado	Parámetros de proceso incorrectos
Deriva del modelo	Pérdida progresiva de sensibilidad
Cambio de formulación	Predicción fuera del ámbito validado
Error de unidades	Dosificación o cálculo incorrecto
Actualización no controlada	Modificación de umbrales
Ciberataque	Manipulación de parámetros
Sesgo de muestreo	Falsos resultados de conformidad
Alucinación generativa	Declaraciones técnicas inexistentes
Interfaz confusa	Interpretación humana equivocada
Dependencia excesiva	Omisión de controles independientes
Caída del servicio	Pérdida de capacidad de control

Tabla 7. Riesgos algorítmicos y posibles consecuencias alimentarias.

El APPCC digital

La expresión APPCC digital no designa una categoría jurídica autónoma. Puede utilizarse como modelo de gestión para integrar los riesgos derivados de sensores, automatización, software e inteligencia artificial dentro del sistema de seguridad alimentaria.

Su estructura debería comprender:

23. inventario de sistemas;
24. relación entre sistema y peligro alimentario;
25. identificación de datos críticos;
26. validación inicial;
27. límites de funcionamiento;
28. supervisión humana;
29. monitorización de rendimiento;
30. control de cambios;
31. gestión de incidentes;
32. conservación de evidencias.

Diferencia entre validación y verificación

Validación

Demuestra, antes o durante la implantación controlada, que el sistema puede cumplir la finalidad prevista.

Debe responder:

¿Puede este modelo controlar o apoyar eficazmente esta decisión en estas condiciones?

Verificación

Confirma de forma periódica que el sistema continúa funcionando como estaba previsto.

Debe responder:

¿Sigue funcionando correctamente después de entrar en operación?

Confundir ambas actividades es peligroso, puesto que una validación inicial satisfactoria no garantiza el rendimiento indefinido. Cambian:

- materias primas;
- proveedores;
- líneas;
- sensores;

- formulaciones;
- poblaciones microbianas;
- condiciones climáticas;
- logística;
- software;
- comportamiento humano.

Control de cambios y revalidación

Toda modificación relevante debe activar una evaluación formal.

Deben considerarse como cambios:

- nueva versión del modelo;
- reentrenamiento;
- actualización de software;
- modificación de umbrales;
- sustitución de sensores;
- incorporación de nuevos proveedores;
- cambio de formulación;
- modificación del envase;
- cambio de vida útil;
- nuevo mercado;
- nueva población objetivo;
- modificación de instrucciones;
- conexión con un equipo diferente.

Cambios mayores y menores

Cambio menor

No altera la finalidad, la lógica de decisión ni el rendimiento esperado.

Puede requerir:

- revisión documental;
- comprobación funcional;
- aprobación simplificada.

Cambio mayor

Puede afectar a la seguridad, exactitud, finalidad, datos o nivel de autonomía.

Debe exigir:

- análisis de riesgos;
- validación;
- revisión APPCC;
- aprobación técnica;
- actualización de instrucciones;
- formación;
- nueva línea base de rendimiento.

La calificación realizada por el proveedor no debe aceptarse automáticamente. Un cambio considerado «menor» desde el punto de vista informático puede ser crítico para el proceso alimentario.

Supervisión humana efectiva

La supervisión humana no consiste en colocar nominalmente a una persona junto al algoritmo.

Para los sistemas de alto riesgo, el Reglamento de Inteligencia Artificial exige medidas que permitan comprender las capacidades y limitaciones del sistema, detectar anomalías, evitar la dependencia automática de sus resultados, interpretar correctamente las salidas y decidir no utilizar, anular o detener el sistema. El responsable del despliegue debe encomendar la supervisión a personas con competencia, formación, autoridad y

apoyo suficientes. Aunque estas obligaciones específicas tengan un calendario de aplicación escalonado, constituyen una referencia razonable para diseñar desde ahora cualquier sistema crítico en alimentación.

Requisitos de una supervisión real

La persona supervisora debe:

- conocer la finalidad del sistema;
- comprender sus limitaciones;
- identificar datos anómalos;
- entender el significado del resultado;
- conocer los falsos positivos y negativos;
- poder solicitar una segunda comprobación;
- disponer de tiempo suficiente;
- tener acceso a la documentación;
- poder detener el proceso;
- no sufrir represalias por discrepar.

Sin autoridad efectiva, la supervisión es ficticia.

El sesgo de automatización

Existe una tendencia humana a aceptar una recomendación automatizada porque se percibe como más objetiva o sofisticada.

La supervisión fracasa cuando el empleado:

- pulsa «aprobar» de manera rutinaria;
- desconoce cómo cuestionar el resultado;
- carece de información alternativa;
- sabe que contradecir al sistema requiere una autorización compleja;
- trabaja bajo objetivos incompatibles con una revisión cuidadosa;
- considera que la responsabilidad pertenece al algoritmo.

La empresa debe evaluar no solo la interfaz técnica, sino el contexto organizativo en el que se adopta la decisión.

Capacidad de anulación

Todo sistema crítico debería contemplar:

- anulación manual;
- parada de emergencia;
- bloqueo automático;
- modo degradado seguro;
- procedimiento alternativo;
- escalado a un nivel superior;
- registro de la intervención.

La posibilidad técnica de anular el sistema no basta si el trabajador no está autorizado, no ha sido formado o teme consecuencias disciplinarias.

Supervisión humana proporcional al tipo de decisión

No toda salida requiere una firma individual. Pero toda decisión crítica necesita una arquitectura de supervisión coherente con sus consecuencias.

Decisión	Supervisión recomendable
Idea preliminar de producto	Revisión técnica ordinaria
Cálculo de costes	Verificación financiera
Revisión de etiqueta	Validación regulatoria antes de impresión
Predicción de vida útil	Confirmación experimental y aprobación técnica
Evaluación de proveedor crítico	Revisión multidisciplinar

Decisión	Supervisión recomendable
Resultado microbiológico	Interpretación por personal competente
Liberación de lote	Aprobación definida en el sistema de calidad
Modificación de PCC	Validación previa y revisión APPCC
Retirada de producto	Comité de crisis con autoridad ejecutiva
Dosificación automática	Control en tiempo real, alarmas y bloqueo seguro

Tabla 8. Supervisión humana proporcional a la decisión.

El Director Técnico en el sistema de gobierno algorítmico

El Director Técnico no debe convertirse ni en firmante universal ni en responsable residual de todo lo que la empresa no haya asignado correctamente. Su función debe definirse de forma expresa.

Funciones razonables

Según la estructura de la empresa, pueden corresponderle:

- aprobar el uso técnico previsto;
- evaluar la compatibilidad con APPCC;
- exigir validación científica;
- revisar criterios de aceptación;
- definir límites de uso;
- aprobar cambios relevantes;
- participar en incidentes;
- ordenar o proponer la suspensión;
- informar a la dirección sobre riesgos;
- custodiar determinadas evidencias.

Funciones que no deben presumirse

No debe asumirse automáticamente que el Director Técnico:

- desarrolló el algoritmo;
- controla la infraestructura informática;
- conoce el código fuente;
- gestiona la ciberseguridad;
- negocia todos los contratos;
- autoriza todas las actualizaciones;
- dispone de poder para retirar productos;
- puede paralizar unilateralmente la actividad.

Estas funciones deben acreditarse mediante:

- contrato;
- poderes;
- organigrama;
- procedimientos;
- delegaciones;
- práctica real.

Autoridad y responsabilidad deben estar alineadas

No es jurídicamente razonable atribuir al Director Técnico la responsabilidad de garantizar el funcionamiento de la IA si:

- no participa en su selección;
- no conoce las actualizaciones;
- no tiene acceso a los registros;
- no puede ordenar pruebas;
- no dispone de presupuesto;

- no puede suspender el sistema;
- sus advertencias pueden ser ignoradas sin escalado.

La responsabilidad debe acompañarse de:

- información;
- recursos;
- competencia;
- independencia;
- autoridad;
- acceso directo al órgano de administración.

Deber de advertencia

Cuando detecte un riesgo relevante, el Director Técnico debe comunicarlo de forma:

- clara;
- inmediata;
- verificable;
- dirigida al órgano competente;
- acompañada de una recomendación.

Una advertencia vaga como «convendría revisar el sistema» es menos eficaz que una comunicación que indique:

- riesgo identificado;
- lotes o procesos afectados;
- posible consecuencia;
- evidencia disponible;
- medida propuesta;
- plazo;
- necesidad de suspensión.

Cuando exista riesgo grave, la comunicación debe dejar constancia de la urgencia y del desacuerdo técnico, si lo hubiera.

El comité de gobierno algorítmico

Las empresas con varios sistemas relevantes deberían constituir un comité específico o asignar formalmente estas funciones a un órgano ya existente.

No es necesario crear una estructura burocrática desproporcionada. En una PYME, las funciones pueden integrarse en el comité de calidad o seguridad alimentaria. En grupos industriales, puede ser necesario un órgano corporativo con representación de distintas plantas.

Composición mínima

- Dirección;
- Dirección Técnica;
- Calidad y Seguridad Alimentaria;
- Tecnología o Datos;
- Producción;
- Jurídico o Compliance;
- Ciberseguridad;
- Protección de Datos, cuando proceda.

Según el sistema podrán participar:

- laboratorio;
- mantenimiento;
- compras;
- recursos humanos;
- prevención;
- asesor externo;
- proveedor tecnológico.

Competencias

El comité debería:

- aprobar la política;
- revisar el inventario;
- clasificar sistemas;
- autorizar proyectos críticos;
- aprobar validaciones;
- revisar incidentes;
- supervisar proveedores;
- controlar cambios;
- revisar indicadores;
- informar al órgano de administración;
- ordenar la suspensión o escalado.

Materias que deben constar en acta

- sistema analizado;
- finalidad;
- riesgos;
- documentación revisada;
- discrepancias;
- condiciones de aprobación;
- responsables;
- plazos;
- votos o reservas;
- fecha de revisión.

El acta no debe transformarse en una fórmula para trasladar responsabilidad colectivamente. Debe demostrar que existió una deliberación real e informada.

Las tres líneas de defensa

Un modelo eficaz puede estructurarse en tres niveles.

Primera línea: operación

Integrada por quienes utilizan el sistema:

- producción;
- calidad;
- laboratorio;
- mantenimiento;
- logística.

Responsabilidades:

- utilizarlo conforme a instrucciones;
- revisar resultados;
- comunicar anomalías;
- conservar registros;
- activar contingencias.

Segunda línea: control

Integrada por:

- Dirección Técnica;
- Seguridad Alimentaria;
- Compliance;
- Protección de Datos;
- Ciberseguridad;
- Prevención.

Responsabilidades:

- establecer políticas;
- evaluar riesgos;
- definir controles;
- supervisar cumplimiento;
- revisar incidentes;
- asesorar.

Tercera línea: auditoría

Debe evaluar de forma independiente:

- diseño;
- cumplimiento;
- eficacia;
- calidad de evidencias;
- cierre de acciones correctivas.

La auditoría puede ser interna o externa, pero debe disponer de independencia suficiente respecto de quienes desarrollan y operan el sistema.

Gestión de proveedores tecnológicos

La diligencia del operador comienza antes de contratar.

Evaluación previa

Debe solicitarse:

- descripción funcional;
- finalidad prevista;
- arquitectura general;
- métricas;
- metodología de validación;
- matrices evaluadas;
- limitaciones;
- requisitos de datos;
- política de actualizaciones;
- ciberseguridad;
- continuidad de servicio;
- subcontratistas;
- seguros;
- historial de incidentes;
- derechos de auditoría.

Señales de alerta

Deben generar cautela:

- afirmaciones de precisión absoluta;
- ausencia de falsos negativos documentados;
- negativa a revelar metodología;
- validaciones exclusivamente internas;
- demostraciones con datos seleccionados;
- referencias comerciales sin evidencia;
- actualizaciones automáticas no controlables;
- imposibilidad de exportar logs;
- exclusión total de responsabilidad;
- uso secundario indeterminado de datos;
- dependencia técnica irreversible.

Evaluación continua

El proveedor no debe evaluarse solo al inicio. Deben revisarse de modo periódico:

- cambios societarios;
- continuidad financiera;
- incidentes;
- vulnerabilidades;
- soporte;
- cumplimiento de niveles de servicio;
- modificaciones del producto;
- calidad de actualizaciones;
- desempeño real.

Ciberseguridad y continuidad operacional

Un sistema algorítmico puede fallar por error estadístico, pero también por:

- manipulación;
- acceso no autorizado;
- ransomware;
- corrupción de datos;
- indisponibilidad del proveedor;
- sabotaje;
- alteración de sensores;
- dependencia de conectividad.

El AI Act incorpora robustez, exactitud y ciberseguridad entre los requisitos de los sistemas de alto riesgo. En alimentación deben contemplarse, al menos:

- autenticación;
- perfiles de acceso;
- segregación de funciones;
- copias de seguridad;
- restauración;
- cifrado;
- control de proveedores;
- parcheado;
- registro de cambios;
- respuesta a incidentes;
- funcionamiento manual alternativo.

La indisponibilidad del algoritmo no puede conducir automáticamente a trabajar sin control. La empresa debe decidir previamente:

- qué procesos pueden continuar;
- cuáles deben detenerse;
- qué comprobaciones manuales sustituyen temporalmente al sistema;
- quién autoriza el modo degradado;
- cuánto tiempo puede mantenerse.

Dimensión laboral y preventiva

La introducción de IA puede afectar a:

- organización del trabajo;
- cargas mentales;
- autonomía profesional;
- vigilancia;
- evaluación de rendimiento;
- responsabilidades;

- cualificación necesaria.

La Ley de Prevención de Riesgos Laborales exige integrar la prevención en todas las fases de la actividad empresarial y evaluar los riesgos derivados de procesos, equipos y condiciones de trabajo.

La implantación debe evaluar riesgos como:

- sobrecarga de alertas;
- fatiga decisional;
- pérdida de competencia;
- dependencia tecnológica;
- presión para confirmar resultados;
- dificultad para cuestionar al sistema;
- estrés por responsabilidad;
- monitorización excesiva.

La supervisión humana no puede descansar en una persona sin tiempo, formación o condiciones psicológicas adecuadas para ejercerla.

Canales de información y protección del informante

Los fallos algorítmicos suelen ser detectados inicialmente por:

- operarios;
- técnicos;
- analistas;
- personal de laboratorio;
- responsables de calidad.

La empresa debe permitir que comuniquen:

- resultados anómalos;
- falsos negativos;
- manipulación de datos;
- presión para liberar lotes;
- uso fuera de validación;
- eliminación de controles;
- alteración de registros.

La Ley 2/2023 protege, en los supuestos comprendidos en su ámbito, a quienes informen en un contexto laboral o profesional sobre infracciones penales o administrativas graves o muy graves, y exige sistemas internos de información a las entidades obligadas.

En todo caso, el canal no debe utilizarse para sustituir la comunicación técnica ordinaria, pero sí debe ofrecer una vía segura cuando:

- la cadena jerárquica no responde;
- existe conflicto de intereses;
- se temen represalias;
- el incidente se está ocultando;
- la dirección está implicada.

Modelo de compliance algorítmico alimentario

Un programa defendible debería contener diez elementos.

1. Política aprobada por la dirección

Debe establecer:

- principios;
- ámbito;
- roles;
- niveles de riesgo;

- prohibiciones;
- escalado.

2. Inventario

Debe mantenerse actualizado y vinculado a responsables.

3. Evaluación de riesgos

Debe combinar:

- riesgo alimentario;
- tecnológico;
- jurídico;
- laboral;
- reputacional;
- de ciberseguridad.

4. Aprobación previa

Ningún sistema crítico debe pasar a producción sin autorización documentada.

5. Validación y verificación

Deben existir protocolos, criterios de aceptación y revalidación.

6. Supervisión humana

Debe asignarse a personas concretas con autoridad efectiva.

7. Control de proveedores

Debe abarcar selección, contrato, auditoría y seguimiento.

8. Gestión de incidentes

Debe definir:

- detección;
- contención;
- investigación;
- comunicación;
- retirada;
- preservación de pruebas.

9. Formación

Debe adaptarse al rol de cada persona.

10. Auditoría y mejora

El programa debe revisarse periódicamente y tras cualquier incidente relevante.

Los modelos de organización y gestión pueden ser jurídicamente relevantes para valorar la diligencia corporativa y, en los supuestos legalmente previstos, la responsabilidad penal de la persona jurídica. El Código Penal exige que los modelos eficaces identifiquen actividades de riesgo, establezcan protocolos, asignen recursos, impongan obligaciones de información, prevean un sistema disciplinario y se revisen periódicamente.

Matriz RACI para decisiones algorítmicas críticas

Las funciones deben asignarse mediante una matriz clara:

- R — Responsible: ejecuta la actividad.
- A — Accountable: responde por la aprobación final.
- C — Consulted: debe ser consultado.
- I — Informed: debe ser informado.

La matriz debe adaptarse a cada organización. Su valor reside en impedir que, tras un incidente, todos los participantes afirmen que la decisión correspondía a otra persona.

Actividad	Dirección	Director Técnico	Calidad	Tecnología	Jurídico	Proveedor
Selección preliminar	A	C	C	R	C	I
Clasificación de criticidad	I	A	R	C	C	C
Validación técnica	I	A	R	C	I	C
Validación informática	I	C	C	A/R	I	C
Aprobación de uso crítico	A	R	C	C	C	I
Modificación de umbrales	I	A	R	C	I	C
Actualización de modelo	I	C	C	A/R	I	R
Liberación de lote	I	A/C	R	I	I	I
Gestión de incidente	A	R	R	R	C	C
Retirada de producto	A	R	R	I	C	I
Conservación de evidencias	I	C	R	R	C	C
Auditoría	I	C	C	C	A/R	I

Tabla 9. Matriz RACI orientativa para decisiones algorítmicas críticas.

Indicadores de control

El órgano de gobierno no debe limitarse a recibir informes cualitativos.

Debe revisar indicadores como:

- número de sistemas activos;
- porcentaje clasificado;
- porcentaje validado;
- modelos pendientes de revalidación;
- falsos positivos;
- falsos negativos;
- anulaciones humanas;
- alertas ignoradas;
- tiempo de respuesta;
- incidentes;
- cambios no autorizados;
- actualizaciones pendientes;
- disponibilidad;
- usuarios formados;
- auditorías vencidas;
- acciones correctivas abiertas.

La tasa de anulación como indicador

Una tasa de anulación humana muy alta puede indicar:

- mal rendimiento;
- umbrales incorrectos;
- mala integración;
- rechazo de usuarios.

Una tasa de anulación igual a cero tampoco demuestra perfección. Puede revelar:

- automatismo;
- falta de autoridad;
- miedo a cuestionar;
- ausencia de revisión.

Los indicadores deben interpretarse, no simplemente contabilizarse.

Auditoría interna mínima

La auditoría debería preguntar:

33. ¿Existe inventario completo?
34. ¿Se ha clasificado cada sistema?
35. ¿Está definida la finalidad?
36. ¿Se ha evaluado el riesgo alimentario?
37. ¿Existe validación representativa?
38. ¿Se conocen falsos positivos y negativos?
39. ¿Se identifica la versión?
40. ¿Se controlan las actualizaciones?
41. ¿Existe supervisión humana efectiva?
42. ¿Puede detenerse el sistema?
43. ¿Hay procedimiento alternativo?
44. ¿Se conservan registros íntegros?
45. ¿Los datos de entrada están controlados?
46. ¿Se evalúa la deriva?
47. ¿Se han incorporado los riesgos al APPCC?
48. ¿Existe plan de incidentes?
49. ¿Los contratos permiten acceder a evidencias?

50. ¿Se ha formado a los usuarios?
51. ¿Se revisan proveedores?
52. ¿El órgano de administración recibe información?

Una respuesta negativa en un sistema crítico debe generar una acción correctiva con responsable y plazo.

Niveles de madurez organizativa

Nivel 0. Uso no controlado

- no existe inventario;
- cada departamento contrata herramientas;
- no hay validación;
- no se conservan evidencias.

Nivel 1. Control reactivo

- existen normas parciales;
- se actúa después de incidentes;
- las responsabilidades son ambiguas.

Nivel 2. Control documentado

- inventario;
- clasificación;
- procedimientos;
- responsables;
- validación inicial.

Nivel 3. Gestión integrada

- IA integrada en APPCC, calidad y compliance;
- auditorías;
- indicadores;
- control de cambios;
- formación.

Nivel 4. Gobierno avanzado

- vigilancia continua;
- validación externa;
- métricas de deriva;
- simulacros;
- auditoría independiente;
- información periódica al órgano de administración.

El objetivo no debe ser alcanzar el nivel más complejo en todas las aplicaciones. Debe aplicarse proporcionalidad: máxima exigencia para los sistemas que pueden afectar a la salud, y controles simplificados para herramientas auxiliares.

Caso práctico: automatización de la liberación de producto

Una empresa introduce una plataforma que integra:

- resultados microbiológicos;
- temperaturas;
- inspección visual;
- registros de limpieza;
- conformidad documental.

El sistema emite automáticamente una orden de liberación.

Fallos de gobierno

La investigación revela que:

- Compras seleccionó al proveedor por coste.
- Informática realizó la integración.

- Calidad no participó en la configuración.
- El Director Técnico desconocía los umbrales.
- El laboratorio enviaba algunos resultados en formato no compatible.
- El sistema interpretaba campos vacíos como «sin desviación».
- La actualización se instalaba automáticamente.
- Nadie revisaba la tasa de falsos negativos.
- No existía modo manual documentado.

El incidente no debe calificarse simplemente como fallo de software.

Existe un fallo sistémico de gobierno:

- selección inadecuada;
- ausencia de análisis de riesgos;
- validación insuficiente;
- responsabilidades difusas;
- datos deficientes;
- automatización excesiva;
- falta de supervisión;
- ausencia de contingencia.

En estas circunstancias, la empresa tendría dificultades para sostener que actuó diligentemente aunque el defecto inicial procediera del proveedor.

Caso práctico: Director Técnico que advierte y es desautorizado

El Director Técnico detecta que el modelo de vida útil se entrenó con una formulación anterior y recomienda suspender su uso. La dirección comercial rechaza la medida por el coste de reducir la fecha de caducidad.

Para proteger el producto, la empresa y su propia posición jurídica, el Director Técnico debería:

53. identificar el riesgo;
54. documentar la incompatibilidad;
55. proponer medidas concretas;
56. solicitar una decisión formal;
57. escalar al órgano competente;
58. activar los canales internos cuando proceda;
59. abstenerse de firmar una validación que no comparte;
60. valorar la necesidad de adoptar medidas adicionales si existe riesgo para la salud.

Una advertencia correctamente documentada no elimina automáticamente toda posible responsabilidad, pero permite acreditar:

- conocimiento limitado;
- actuación diligente;
- oposición;
- ausencia de control sobre la decisión final.

La dirección que ignora deliberadamente una advertencia técnica sólida puede asumir una exposición jurídica muy superior.

Síntesis: la responsabilidad se previene mediante arquitectura organizativa

El gobierno de la inteligencia artificial no puede reducirse a una política ética ni a una declaración de principios.

Debe poder verse en:

- organigramas;
- contratos;
- validaciones;
- registros;
- actas;
- controles;
- formación;

- decisiones;
- auditorías;
- reacciones ante incidentes.

La supervisión humana solo es efectiva cuando la persona competente comprende el sistema, dispone de información, tiene tiempo, puede discrepar y posee autoridad para detenerlo.

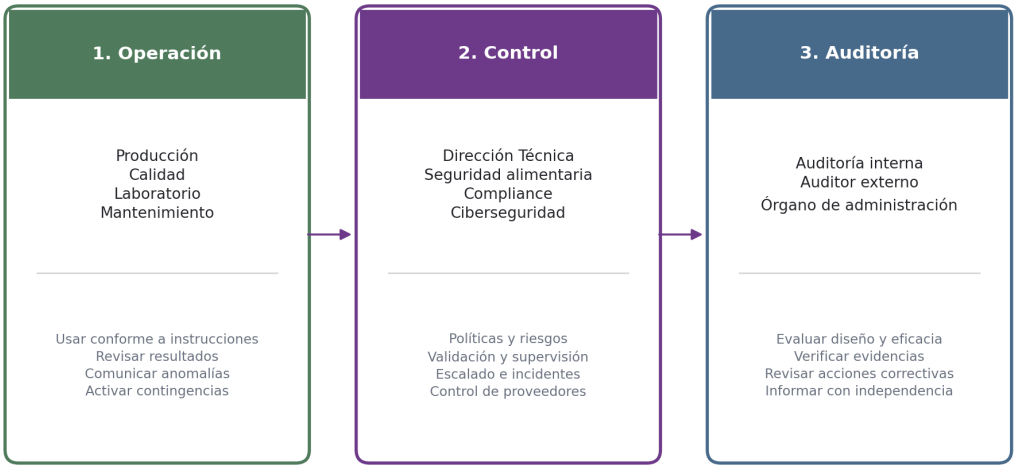
El Director Técnico no debe aceptar una responsabilidad abstracta sobre herramientas que no controla. Pero tampoco puede permanecer pasivo cuando conoce un riesgo situado dentro de su ámbito funcional.

El operador alimentario debe asumir que la IA forma parte de su sistema de producción y control. No es un servicio informático periférico cuando condiciona la seguridad, la conformidad o la comercialización del producto.

Una empresa no gobierna la IA porque haya nombrado a un responsable. La gobierna cuando ninguna decisión crítica puede adoptarse sin que estén definidos el riesgo, la autoridad, la validación, la supervisión y la evidencia.

La diferencia entre una organización diligente y una organización expuesta no reside en que sus algoritmos nunca fallen. Reside en que la primera conoce sus límites, detecta el fallo antes de que cause daño y puede demostrar exactamente cómo actuó.

Arquitectura de gobierno: tres líneas de defensa



La independencia aumenta de izquierda a derecha; la responsabilidad operativa no desaparece por la existencia de control o auditoría.

Figura 4. Arquitectura de gobierno mediante tres líneas de defensa.

CAPÍTULO 8. SANCIONES Y RESPUESTA ANTE INCIDENTES

Cuando aparece una señal de riesgo, la empresa debe separar la protección inmediata de la investigación de responsabilidades. Primero se contiene el peligro y se preserva la evidencia; después se determina quién soporta el coste. El régimen sancionador alimentario y el Reglamento de IA pueden operar de forma paralela cuando protegen intereses y obligaciones distintos.

Sanciones, seguros, contratos y respuesta ante incidentes algorítmicos

La responsabilidad jurídica por el uso de inteligencia artificial en la industria alimentaria no se agota en la indemnización del daño. Un mismo incidente puede activar simultáneamente:

- medidas de inmovilización y retirada;
- sanciones alimentarias;
- sanciones derivadas del Reglamento de Inteligencia Artificial;

- reclamaciones civiles;
- penalizaciones contractuales;
- responsabilidad penal;
- pérdida o discusión de coberturas aseguradoras;
- medidas correctivas exigidas por autoridades de vigilancia del mercado.

Esta superposición exige separar tres conceptos que con frecuencia se confunden:

Medida de protección

Busca evitar o reducir el riesgo.

Ejemplos:

- inmovilización;
- suspensión del sistema;
- retirada;
- recuperación;
- cierre cautelar;
- bloqueo de lotes.

Sanción

Castiga una infracción administrativa acreditada mediante el correspondiente procedimiento.

Responsabilidad indemnizatoria

Pretende reparar los daños sufridos por consumidores, clientes, distribuidores u otros perjudicados.

La retirada de un alimento no es necesariamente una sanción. Puede adoptarse como medida preventiva aunque todavía no se haya determinado quién es responsable. La Ley 17/2011 precisa que la retirada precautoria o definitiva de bienes por razones de salud y seguridad, así como determinados cierres o suspensiones dirigidos a corregir riesgos, no tienen naturaleza sancionadora.

Acumulación de responsabilidades y principio non bis in idem

La Ley 17/2011 establece que las infracciones alimentarias pueden sancionarse sin perjuicio de las responsabilidades civiles, penales o de otro orden que concurran. También impide imponer una doble sanción por los mismos hechos y en función de los mismos intereses públicos protegidos.

Esto no significa que un incidente solo pueda generar una consecuencia jurídica.

Puede concurrir, por ejemplo:

- una infracción alimentaria por comercialización de un producto inseguro;
- una infracción del Reglamento de Inteligencia Artificial por incumplir obligaciones del proveedor o responsable del despliegue;
- una infracción de protección de datos;
- una reclamación civil por lesiones;
- una acción contractual del operador frente al proveedor;
- una investigación penal por imprudencia grave.

El principio non bis in idem impide duplicar sanciones cuando coinciden sustancialmente:

61. el sujeto;
62. los hechos;
63. el fundamento o interés jurídico protegido.

No impide necesariamente que autoridades diferentes reaccionen frente a aspectos distintos del mismo incidente.

Ejemplo

Una herramienta automatizada omite un alérgeno en el etiquetado.

Pueden existir:

- responsabilidad alimentaria por etiquetado defectuoso y riesgo para la salud;
- responsabilidad contractual del proveedor de software;
- responsabilidad civil frente al consumidor afectado;

- posible infracción del Reglamento de Inteligencia Artificial, si el sistema y la obligación incumplida se encuentran dentro de su ámbito aplicable;
- responsabilidad penal, si concurren los elementos exigidos por el Código Penal.

No se está sancionando necesariamente dos veces la misma ilicitud. Cada régimen puede proteger un interés diferente y exigir presupuestos distintos.

Régimen sancionador alimentario

La Ley 17/2011 considera infracciones, entre otras conductas:

- la falta o deficiente aplicación de sistemas de autocontrol;
- las deficiencias documentales y de trazabilidad;
- el etiquetado insuficiente o defectuoso;
- la omisión de pruebas exigibles;
- la comercialización en condiciones no permitidas;
- la falta de comunicación de riesgos a la autoridad;
- la aportación de registros falsos o inexactos;
- el incumplimiento de medidas cautelares.

La utilización de inteligencia artificial no constituye por sí misma una infracción. El problema aparece cuando su uso provoca o facilita alguno de estos incumplimientos.

Graduación

Las infracciones se clasifican como leves, graves o muy graves atendiendo a factores como:

- riesgo para la salud;
- posición del infractor en el mercado;
- beneficio obtenido;
- intencionalidad;
- gravedad de la alteración sanitaria;
- generalización;
- reincidencia.

La ausencia de registros esenciales, la falta de autocontroles, la omisión de análisis que comporte riesgo para la salud o la falta de comunicación de un riesgo pueden calificarse como infracciones graves. La falta consciente de controles o precauciones cuando comporte un riesgo grave para la salud puede alcanzar la categoría de muy grave.

Cuantías estatales básicas

La Ley 17/2011 establece:

En las infracciones muy graves puede acordarse el cierre temporal del establecimiento por un máximo de cinco años. También pueden imponerse decomiso, costes de transporte y destrucción y, en determinados supuestos, publicidad de la sanción firme.

Estas cuantías no describen por sí solas toda la exposición jurídica. Deben añadirse:

- regímenes autonómicos;
- normas sectoriales;
- defensa de consumidores;
- calidad alimentaria;
- protección de datos;
- costes de retirada;
- pérdida de producto;
- reclamaciones de clientes;
- daño reputacional;
- posibles responsabilidades penales.

En numerosos incidentes, la multa administrativa puede ser inferior al coste económico de la retirada, la destrucción de mercancía o la pérdida de contratos.

Categoría	Multa
Leve	Hasta 5.000 euros
Grave	De 5.001 a 20.000 euros
Muy grave	De 20.001 a 600.000 euros

Tabla 10. Cuantías estatales básicas de la Ley 17/2011.

Sanciones del Reglamento Europeo de Inteligencia Artificial

El Reglamento de Inteligencia Artificial es aplicable con carácter general desde el 2 de agosto de 2026, aunque determinadas obligaciones relativas a sistemas de alto riesgo cuentan con plazos ampliados. Tras el AI Omnibus, las reglas específicas de los sistemas del anexo III se aplicarán desde el 2 de diciembre de 2027 y las de determinados sistemas integrados en productos del anexo I desde el 2 de agosto de 2028.

Por ello, debe evitarse una conclusión equivocada:

Que las obligaciones específicas de ciertos sistemas de alto riesgo se hayan aplazado no significa que el Reglamento de Inteligencia Artificial entero esté suspendido.

Las prácticas prohibidas, las obligaciones ya aplicables y las normas de transparencia o de modelos de propósito general deben analizarse conforme a su propio calendario.

Límites máximos

El artículo 99 establece, con carácter general:

Para las empresas se aplica, con carácter general, la cifra fija o el porcentaje, según cuál resulte superior. Para las pymes, incluidas las empresas emergentes, el límite se determina aplicando la cifra o el porcentaje que resulte inferior.

La graduación debe considerar, entre otros elementos:

- naturaleza, gravedad y duración;
- número de personas afectadas;
- daños;
- tamaño y cuota de mercado;
- beneficio obtenido;
- cooperación;
- medidas técnicas y organizativas;
- notificación voluntaria;
- intencionalidad o negligencia;
- acciones de mitigación.

Aplicación práctica en alimentación

Muchas aplicaciones alimentarias ordinarias no serán sistemas de alto riesgo conforme al Reglamento de Inteligencia Artificial. Por tanto, no es correcto presentar las multas de 35 millones de euros como consecuencia automática de cualquier error de una herramienta alimentaria.

Para aplicar el régimen deberá determinarse:

64. si existe jurídicamente un sistema de IA;
65. cuál es su clasificación;
66. qué función desempeña;
67. qué sujeto es proveedor, importador, distribuidor o responsable del despliegue;
68. qué obligación estaba vigente;
69. qué conducta concreta se incumplió;
70. si la autoridad competente puede atribuir la infracción al operador investigado.

La sanción alimentaria y la del Reglamento de Inteligencia Artificial protegen ámbitos parcialmente diferentes. La primera se centra en seguridad y cumplimiento alimentario; la segunda, en la conformidad y utilización de los sistemas de IA.

Incumplimiento	Límite máximo
Prácticas de IA prohibidas	35 millones de euros o 7 % del volumen mundial anual
Determinadas obligaciones de operadores y organismos notificados	15 millones de euros o 3 % del volumen mundial anual
Información incorrecta, incompleta o engañosa a autoridades u organismos notificados	7,5 millones de euros o 1 % del volumen mundial anual

Tabla 11. Límites máximos de multas del Reglamento de Inteligencia Artificial.

Incidentes graves conforme al AI Act

Para los sistemas de alto riesgo sometidos a las correspondientes obligaciones, el proveedor debe establecer vigilancia poscomercialización y recopilar y analizar información sobre el rendimiento del sistema a lo largo de su vida útil. El responsable del despliegue que tenga razones para considerar que el sistema presenta un riesgo debe informar sin demora al proveedor o distribuidor y a la autoridad de vigilancia del mercado y suspender su utilización. Cuando detecte un incidente grave debe informar al proveedor y a los restantes sujetos y autoridades previstos.

La notificación de incidentes graves se realiza, como regla general, inmediatamente después de establecerse el vínculo causal o su probabilidad razonable y, en todo caso, dentro de los quince días siguientes al conocimiento. Existen plazos más breves para determinados incidentes, incluida la notificación en dos días en ciertas infracciones generalizadas y un plazo máximo de diez días en caso de fallecimiento.

Estos plazos no sustituyen las obligaciones alimentarias de reacción inmediata. Si existe una sospecha fundada de que un alimento no cumple los requisitos de seguridad, el operador debe proceder inmediatamente a su retirada, informar a las autoridades y, cuando el producto pueda haber llegado al consumidor, comunicar eficazmente las razones y recuperar el producto cuando sea necesario.

Dos canales regulatorios

Un mismo hecho puede exigir:

Canal alimentario

- bloqueo;
- trazabilidad;
- comunicación a la autoridad sanitaria;
- retirada;
- información al consumidor;
- recuperación.

Canal algorítmico

- suspensión del sistema;
- comunicación al proveedor;
- conservación de logs;
- investigación causal;
- notificación a vigilancia del mercado;
- corrección o retirada del sistema.

Esperar a completar la investigación informática antes de adoptar medidas de seguridad alimentaria puede ser jurídicamente inaceptable.

La primacía de la protección de la salud

En un incidente deben separarse dos decisiones:

71. qué medida protege inmediatamente al consumidor;
72. quién soportará posteriormente el coste.

La empresa no debe retrasar una retirada necesaria mientras discute si el responsable es:

- el proveedor de IA;
- el laboratorio;

- el fabricante del sensor;
- el integrador;
- un empleado;
- el operador logístico.

La atribución definitiva puede investigarse después. La protección inmediata no.

Principio operativo

Primero se contiene el riesgo; después se distribuye la responsabilidad.

Esto no implica retirar indiscriminadamente todos los productos ante cualquier alerta. Exige una evaluación rápida, proporcional y documentada de:

- gravedad;
- probabilidad;
- extensión;
- exposición;
- vulnerabilidad de los consumidores;
- reversibilidad;
- fiabilidad de la alerta;
- capacidad de acotar lotes.

Cuando existe incertidumbre científica pero el daño potencial es grave, la prudencia debe prevalecer sobre el ahorro económico inmediato.

Protocolo de respuesta ante un incidente algorítmico

Fase 1. Contención inmediata

Debe ejecutarse sin esperar a determinar la responsabilidad definitiva.

- suspender temporalmente el sistema afectado;
- bloquear los lotes relacionados;
- evitar nuevas liberaciones automáticas;
- pasar a procedimiento manual seguro;
- preservar la versión del modelo;
- impedir la sobrescritura de registros;
- identificar productos distribuidos;
- informar al responsable de crisis.

Fase 2. Evaluación alimentaria

- identificar el peligro;
- evaluar gravedad y probabilidad;
- verificar resultados mediante métodos independientes;
- revisar APPCC;
- determinar lotes y mercados;
- valorar retirada o recuperación;
- contactar con la autoridad cuando proceda.

Fase 3. Evaluación tecnológica

- identificar versión;
- revisar datos de entrada;
- comprobar sensores;
- analizar umbrales;
- revisar actualizaciones;
- examinar intervenciones humanas;
- comparar con la validación;
- determinar si existe deriva o uso fuera de finalidad.

Fase 4. Preservación jurídica

- activar retención documental;
- realizar copias forenses;

- conservar correos y mensajes;
- preservar contratos;
- impedir modificaciones retrospectivas;
- documentar la cronología;
- identificar testigos.

Fase 5. Notificaciones

Debe elaborarse una matriz que contemple:

- autoridad alimentaria;
- vigilancia del mercado de IA;
- proveedor;
- clientes;
- distribuidores;
- aseguradoras;
- consumidores;
- autoridad de protección de datos, si procede;
- órgano de administración.

Fase 6. Corrección y revalidación

- análisis de causa raíz;
- acciones correctivas y preventivas;
- modificación técnica;
- revisión contractual;
- formación;
- revalidación;
- auditoría de eficacia;
- autorización formal antes de reiniciar.

Cronología orientativa de actuación

Esta cronología es organizativa, no sustituye ningún plazo legal específico. Cuando una norma exige actuación inmediata, debe actuarse inmediatamente.

Momento	Prioridad
Primeras horas	Seguridad, bloqueo, preservación y escalado
Primer día	Evaluación de riesgo, trazabilidad, contraste analítico y notificaciones urgentes
Primeras 72 horas	Investigación causal, perímetro de lotes y estrategia de retirada
Primera semana	Informe preliminar, relación con proveedores y aseguradoras
Fase posterior	CAPA, revalidación, reclamaciones y mejora del sistema

Tabla 12. Cronología organizativa de respuesta a incidentes.

Figura 5. Secuencia de respuesta ante un incidente algorítmico.

CAPÍTULO 9. SEGURO, CONTRATACIÓN Y DISTRIBUCIÓN ECONÓMICA DEL RIESGO

La contratación y el seguro deben diseñarse antes de la puesta en servicio. Una licencia tecnológica estándar resulta insuficiente cuando el sistema condiciona la seguridad del producto. La empresa necesita métricas verificables, control de cambios, acceso a logs, cooperación en incidentes, seguros adecuados y una contraparte patrimonialmente solvente.

El seguro no sustituye al cumplimiento

El seguro de responsabilidad civil cubre, dentro de los límites legales y contractuales, el riesgo de que nazca para el asegurado la obligación de indemnizar a un tercero por daños de los que resulte civilmente responsable.

Esto significa que la existencia de una póliza no:

- legaliza la conducta;
- evita la sanción;
- sustituye la retirada;
- elimina el deber de prevención;
- garantiza la cobertura de todos los costes.

La cobertura depende de:

- riesgo definido;
- actividad declarada;
- exclusiones;
- suma asegurada;
- franquicia;
- ámbito territorial;
- período temporal;
- fecha del hecho;
- fecha de reclamación;
- cumplimiento de deberes de comunicación.

Pólizas potencialmente relevantes

Una empresa que utiliza IA en procesos alimentarios debería revisar, al menos:

Responsabilidad civil de explotación

Daños derivados de la actividad general.

Responsabilidad civil de producto

Daños causados por productos puestos en circulación.

Retirada de productos

Gastos de localización, retirada, transporte, destrucción, sustitución y comunicación, cuando estén expresamente cubiertos.

Responsabilidad profesional

Errores en asesoramiento, diseño, laboratorio, software o servicios técnicos.

Seguro cibernético

Incidentes de seguridad, corrupción de datos, interrupción y determinados gastos de respuesta.

D&O

Responsabilidad de administradores y directivos, dentro de los límites y exclusiones pactados.

Defensa jurídica

Costes de asistencia y defensa en procedimientos cubiertos.

Estas coberturas no deben darse por supuestas. Una póliza de responsabilidad civil de producto puede cubrir daños corporales a terceros y excluir los costes de retirada del producto propio.

Riesgos de falta de cobertura

Un incidente algorítmico puede quedar total o parcialmente fuera de cobertura por:

- actividad tecnológica no declarada;
- uso del sistema distinto del comunicado;
- conocimiento previo del defecto;
- incumplimiento deliberado;
- ausencia de mantenimiento;
- exclusiones de retirada;
- exclusiones de daños propios;
- exclusiones cibernéticas;
- límites territoriales;
- siniestros anteriores a la fecha retroactiva;
- notificación tardía;
- ausencia de cobertura para filiales o técnicos concretos.

Las multas administrativas suelen estar excluidas o sometidas a restricciones legales y contractuales. No debe diseñarse el programa de cumplimiento partiendo de la hipótesis de que la aseguradora pagará una sanción.

Comunicación de agravación del riesgo

Durante la vigencia del contrato, el asegurado debe comunicar las alteraciones de los factores declarados que agraven el riesgo de manera relevante.

La introducción de automatización crítica puede ser materialmente relevante cuando modifica:

- proceso productivo;
- controles;
- autonomía;
- exposición cibernética;
- volumen;
- mercados;
- capacidad de retirada.

No toda implantación de IA constituye automáticamente una agravación asegurable. Debe analizarse el cuestionario, la póliza y la naturaleza del cambio.

Comunicación del siniestro

La Ley de Contrato de Seguro establece, con carácter general, la comunicación del siniestro dentro de los siete días siguientes a su conocimiento, salvo que la póliza contemple un plazo más amplio. Por ello, el protocolo de incidentes debe incluir una revisión temprana de las pólizas. Esperar a recibir una demanda formal puede ser demasiado tarde.

Auditoría aseguradora de la IA

Antes de implantar sistemas críticos, la empresa debería remitir a su corredor o aseguradora información suficiente sobre:

- función;
- nivel de autonomía;
- productos afectados;
- validación;
- supervisión humana;
- ciberseguridad;
- proveedores;
- mercados;
- volúmenes;

- procedimiento de retirada.

La revisión debe confirmar por escrito:

73. qué póliza responde;
74. qué daños están cubiertos;
75. si se cubren costes de retirada;
76. si existen exclusiones de software;
77. si el proveedor está asegurado;
78. qué límite se aplica;
79. qué franquicia existe;
80. qué territorios están incluidos;
81. qué plazo de notificación rige;
82. quién dirige la defensa.

Contratación tecnológica orientada a la responsabilidad

La contratación de una solución algorítmica no puede tratarse como una simple licencia informática cuando el sistema interviene en seguridad alimentaria.

El contrato debe funcionar como instrumento de control técnico y de distribución interna de riesgos.

Identificación exacta de las partes

Debe aclararse quién actúa como:

- fabricante;
- proveedor;
- distribuidor;
- importador;
- integrador;
- mantenedor;
- responsable del despliegue;
- propietario de los datos;
- subcontratista.

La denominación comercial no prevalece sobre la función real.

Finalidad prevista

Debe describirse qué puede y qué no puede hacer el sistema.

No es suficiente:

“Sistema para mejorar el control de calidad.”

Debe precisarse, por ejemplo:

“Sistema destinado a identificar visualmente envases con defectos de sellado en la línea X, para temperaturas y formatos definidos, como herramienta de apoyo y sin sustituir la verificación de integridad prevista en el procedimiento Q-17.”

Datos

Debe regularse:

- origen;
- calidad;
- propiedad;
- acceso;
- reutilización;
- conservación;
- anonimización;
- transferencia;
- devolución;
- borrado;
- responsabilidad por datos erróneos.

Prestaciones verificables

- sensibilidad;
- especificidad;
- falsos negativos;
- falsos positivos;
- disponibilidad;
- latencia;
- robustez;
- condiciones de funcionamiento;
- precisión por subgrupos;
- tolerancias.

Las métricas deben vincularse a un protocolo de medición. Una precisión global del 98 % puede ocultar una sensibilidad insuficiente frente al defecto más peligroso.

Validación

Debe establecerse:

- quién diseña el protocolo;
- quién aporta muestras;
- quién asume el coste;
- criterios de aceptación;
- validación externa;
- revalidación;
- consecuencias del fracaso.

Control de cambios

El proveedor no debería modificar unilateralmente elementos críticos sin:

- aviso previo;
- documentación;
- evaluación de impacto;
- posibilidad de prueba;
- aprobación del operador;
- reversibilidad.

Registros

El contrato debe garantizar:

- generación;
- acceso;
- exportación;
- conservación;
- integridad;
- entrega tras terminación;
- disponibilidad ante autoridades y litigios.

Incidentes

Debe fijar:

- definición;
- canal;
- plazo;
- información mínima;
- cooperación;
- investigación;
- preservación;
- comunicación a autoridades;
- acciones correctivas.

Auditoría

El operador debería disponer de derechos proporcionados para:

- revisar documentación;
- comprobar controles;
- solicitar evidencias;
- auditar subcontratistas críticos;
- utilizar peritos independientes;
- verificar acciones correctivas.

Responsabilidad e indemnidad

Deben regularse:

- límites;
- exclusiones;
- daños directos;
- retirada;
- reclamaciones de terceros;
- infracción regulatoria;
- propiedad intelectual;
- protección de datos;
- ciberseguridad;
- acciones de repetición.

Una limitación equivalente al importe mensual de la licencia puede ser económicamente inadecuada cuando el sistema controla lotes de gran valor o riesgos para la salud.

Cláusulas contractuales especialmente peligrosas

“El sistema se proporciona tal cual”

Puede ser incompatible con las prestaciones concretamente prometidas y con el uso profesional conocido por el proveedor.

“El proveedor no responde de ningún resultado”

Vacía de contenido la obligación cuando el resultado constituye precisamente el objeto del contrato.

“Las actualizaciones se instalarán sin aviso”

Es inaceptable para elementos que afecten a parámetros críticos.

“Los registros son propiedad exclusiva del proveedor”

Puede impedir al operador cumplir sus deberes regulatorios y probatorios.

“El cliente garantiza todos los datos”

Debe diferenciarse la calidad del dato aportado por el cliente de los controles que razonablemente debe realizar el sistema.

“El sistema garantiza cumplimiento normativo”

Ningún proveedor debería convertir esta afirmación en sustituto de la revisión regulatoria y técnica del operador.

“La responsabilidad se limita a repetir el servicio”

Puede ser insuficiente cuando el error causa retirada, lesiones o destrucción de producto.

Due diligence del proveedor

Antes de contratar debe comprobarse:

- existencia jurídica;
- solvencia;
- experiencia sectorial;
- referencias verificables;
- metodología;

- personal cualificado;
- seguros;
- subcontratación;
- localización de datos;
- seguridad;
- continuidad;
- historial de incidentes;
- capacidad de soporte;
- derechos sobre el modelo;
- dependencia de componentes externos.

Preguntas esenciales

83. ¿Con qué matrices se entrenó?
84. ¿Qué muestras se utilizaron?
85. ¿Cuántas procedían de entornos industriales?
86. ¿Cuál es la sensibilidad frente al peligro crítico?
87. ¿Qué falsos negativos se observaron?
88. ¿Cómo detecta datos fuera de distribución?
89. ¿Qué ocurre cuando faltan datos?
90. ¿Cómo se controlan las actualizaciones?
91. ¿Se puede reproducir una decisión histórica?
92. ¿Qué seguro cubre el producto?

Una empresa que se niega a facilitar información mínima sobre limitaciones, validación y registros no debería ser seleccionada para una función crítica.

Distribución interna de costes

El operador puede reclamar al proveedor los costes derivados de su incumplimiento cuando concurran los presupuestos jurídicos y contractuales correspondientes. Pero debe diferenciar:

Responsabilidad frente al exterior

Quién responde ante:

- consumidor;
- autoridad;
- cliente;
- distribuidor.

Repetición interna

Quién soporta finalmente el coste entre las empresas participantes.

Ejemplo:

93. El operador retira el producto y compensa a su cliente.
94. La autoridad sanciona al operador por incumplimiento alimentario.
95. El operador reclama al proveedor tecnológico por defecto del sistema.
96. El proveedor reclama al integrador si la causa fue una configuración incorrecta.
97. Las aseguradoras discuten la distribución de cobertura.

Esta sucesión no altera la necesidad de que el operador adopte inmediatamente las medidas alimentarias pertinentes.

Simulacros de incidente algorítmico

La empresa debería realizar ejercicios periódicos que combinen:

- fallo tecnológico;
- peligro alimentario;
- indisponibilidad del proveedor;
- presión comercial;
- necesidad de retirada;

- comunicación pública.

Escenario

El sistema de visión detecta una disminución anormal de defectos. Producción interpreta el resultado como mejora del proceso. Tres días después se descubre que una actualización desactivó una clase de detección. El simulacro debe comprobar:

- quién detecta la anomalía;
- quién puede suspender el sistema;
- cómo se identifican lotes;
- cuánto se tarda en recuperar registros;
- cómo se contacta con el proveedor;
- quién informa a la autoridad;
- quién decide la retirada;
- qué póliza se notifica;
- qué procedimiento manual se activa.

El simulacro debe concluir con acciones correctivas, no con una mera acta de celebración.

Cuadro de mando del riesgo jurídico algorítmico

Indicador	Riesgo que permite detectar
Sistemas sin clasificación	Falta de gobierno
Modelos sin validación vigente	Uso no demostrado
Actualizaciones no revisadas	Cambio incontrolado
Falsos negativos	Riesgo de seguridad
Alertas ignoradas	Supervisión ineficaz
Anulaciones humanas	Posible desajuste operativo
Incidentes no comunicados	Riesgo sancionador
Logs incompletos	Debilidad probatoria
Proveedores sin seguro	Riesgo de recuperación
Pólizas sin revisión	Falta de cobertura
Contratos sin auditoría	Dependencia informativa
Sistemas sin contingencia	Riesgo de paralización
Hallazgos APPCC abiertos	Riesgo alimentario persistente

Tabla 13. Indicadores de riesgo jurídico y organizativo.

Test de asegurabilidad y contratación antes de la puesta en servicio

Ningún sistema crítico debería entrar en producción sin responder afirmativamente a las siguientes preguntas:

Jurídicas

- ¿Está definida la función de cada parte?
- ¿Se conoce la clasificación conforme al Reglamento de Inteligencia Artificial?
- ¿Está delimitada la finalidad?
- ¿El contrato permite acceder a registros?
- ¿Existen obligaciones claras de notificación?
- ¿La responsabilidad está razonablemente distribuida?

Técnicas

- ¿Se ha validado?
- ¿Se conocen sus errores?
- ¿Se controla la versión?

- ¿Existe supervisión humana?
- ¿Puede detenerse?
- ¿Existe modo alternativo?

Alimentarias

- ¿Está integrado en APPCC?
- ¿Se han revisado peligros?
- ¿Se han definido límites?
- ¿Se mantiene verificación independiente?
- ¿Está documentada la liberación de lotes?

Aseguradoras

- ¿La actividad está declarada?
- ¿Existe cobertura de producto?
- ¿Existe cobertura de retirada?
- ¿Se cubren errores tecnológicos?
- ¿Se ha comunicado la modificación del riesgo?
- ¿Se conocen los plazos de notificación?

Una respuesta negativa no siempre obliga a cancelar el proyecto. Sí obliga a corregir el déficit o a justificar expresamente su aceptación.

Caso integrado: algoritmo de alérgenos, retirada y conflicto entre proveedores

Una empresa alimentaria utiliza una plataforma que combina:

- formulaciones;
- fichas de materias primas;
- base de datos de alérgenos;
- generación automática de etiquetas.

Tras un cambio de proveedor, el sistema no identifica la presencia de proteína láctea. Se distribuyen 80.000 unidades.

Cadena causal

La investigación revela:

98. El proveedor de materia prima remitió una nueva ficha.
99. Compras la almacenó en una carpeta no conectada.
100. El ERP mantuvo la versión anterior.
101. El sistema de IA generó la etiqueta con datos desactualizados.
102. Regulación revisó solo el formato.
103. Calidad aprobó la impresión.
104. El producto llegó a consumidores alérgicos.

Responsabilidad del operador

Es elevada porque:

- comercializó el producto;
- no garantizó la actualización de especificaciones;
- no verificó el alérgeno;
- la revisión humana fue formal;
- falló el control de cambios.

Proveedor del sistema

Podrá responder si:

- conocía el riesgo de utilizar versiones obsoletas;
- no implantó controles prometidos;
- no avisó de datos no sincronizados;
- presentó el sistema como verificador integral.

Proveedor de materia prima

Su responsabilidad dependerá de:

- calidad y claridad de la información;
- momento de envío;
- canal acordado;
- posible inconsistencia documental.

Director Técnico

Solo responderá personalmente si:

- tenía funciones y autoridad sobre el proceso;
- conoció o debió conocer el fallo;
- aprobó o toleró el sistema deficiente;
- omitió actuar pudiendo hacerlo.

Medidas inmediatas

- bloqueo;
- retirada;
- información a autoridades;
- comunicación al consumidor;
- recuperación;
- preservación de evidencias;
- notificación a aseguradoras;
- suspensión del sistema;
- revisión de todas las etiquetas generadas.

Enseñanza

El algoritmo no fue la única causa. El daño surgió de una combinación de:

- información;
- integración;
- procedimiento;
- revisión;
- gobierno.

La empresa no puede reducir el incidente a un «fallo de IA». Tampoco debe asumir que toda la responsabilidad pertenece al operador tecnológico.

Síntesis: la responsabilidad debe financiarse, contratarse y ensayarse antes del fallo

La prevención jurídica no consiste únicamente en redactar políticas. Debe reflejarse en:

- contratos ejecutables;
- coberturas aseguradoras coherentes;
- facultades de auditoría;
- obligaciones de notificación;
- sistemas de retirada;
- simulacros;
- preservación de pruebas;
- protocolos de actuación inmediata.

El seguro no transforma un sistema inseguro en aceptable. El contrato no desplaza la responsabilidad regulatoria del operador. La cláusula de indemnidad no protege al consumidor. Y la discusión entre proveedores no justifica retrasar una retirada.

La empresa jurídicamente madura es aquella que, antes de automatizar una decisión crítica, ya ha establecido:

- quién actúa;
- quién paga;
- quién informa;

- quién conserva las pruebas;
- quién puede detener el sistema;
- cómo se protege al consumidor.

La responsabilidad algorítmica no se gestiona únicamente atribuyendo culpa después del incidente. Se gestiona diseñando de antemano quién controla el riesgo, qué recursos existen para repararlo y qué decisiones deben adoptarse cuando la tecnología deja de ser fiable.

CAPÍTULO 10. DIMENSIÓN TRANSFRONTERIZA, JURISDICCIÓN Y LEY APLICABLE

Los sistemas algorítmicos se prestan desde infraestructuras y sociedades dispersas en distintas jurisdicciones. La nube no elimina la responsabilidad, pero puede dificultar el acceso a la prueba y la ejecución de reclamaciones. La ley aplicable, el foro, la posición del importador y la localización de los datos deben resolverse antes del incidente.

La dimensión transfronteriza: cuando el algoritmo, el alimento y el daño se encuentran en países diferentes

La arquitectura habitual de una solución algorítmica alimentaria puede distribuirse entre varias jurisdicciones:

- el desarrollador del modelo está en Estados Unidos;
- el proveedor contractual tiene domicilio en Irlanda;
- la infraestructura se aloja en Alemania;
- el integrador trabaja desde España;
- el alimento se fabrica en Valencia;
- el distribuidor opera desde Francia;
- el consumidor perjudicado reside en Bélgica.

En este contexto, identificar a los posibles responsables no basta. También debe determinarse:

105. qué autoridades pueden actuar;
106. ante qué tribunales puede presentarse una reclamación;
107. qué Derecho nacional resulta aplicable;
108. dónde se encuentran las pruebas;
109. contra qué entidad puede ejecutarse una resolución;
110. qué operador establecido en la Unión asume las obligaciones regulatorias.

La contratación de una solución tecnológica extranjera no desplaza el proceso industrial fuera del ordenamiento europeo. Cuando el sistema se utiliza para fabricar, controlar o comercializar alimentos en la Unión, continúa siendo aplicable la legislación alimentaria europea y, cuando concurran sus presupuestos, el Reglamento de Inteligencia Artificial.

Alcance territorial del Reglamento de Inteligencia Artificial

El AI Act no se aplica únicamente a las empresas establecidas físicamente en la Unión Europea. Su ámbito territorial comprende, entre otros:

- proveedores que introducen sistemas de IA o modelos de propósito general en el mercado de la Unión;
- responsables del despliegue establecidos o situados en la Unión;
- proveedores y responsables del despliegue situados en terceros países cuando las salidas producidas por el sistema se utilizan en la Unión.

Esta extensión pretende evitar que una empresa eluda las obligaciones europeas alojando el modelo o formalizando el contrato fuera del territorio de la Unión.

Ejemplo alimentario

Una empresa estadounidense ofrece desde sus servidores un modelo que decide si una planta española debe liberar determinados lotes.

Aunque:

- el código esté alojado fuera de Europa;
- el proveedor no tenga oficina en España;
- el contrato se facture desde Estados Unidos,

resulta evidente que la salida del sistema se utiliza en la Unión y puede entrar en el ámbito territorial del Reglamento de Inteligencia Artificial.

Esto no significa que toda obligación del Reglamento resulte automáticamente aplicable. Será necesario determinar:

- si la herramienta encaja en la definición legal de sistema de IA;
- qué clasificación le corresponde;
- qué función desempeña;
- cuál es la fecha de aplicación de la obligación concreta;
- qué sujeto ocupa cada posición regulatoria.

El proveedor extranjero y la necesidad de una presencia responsable en la Unión

Cuando un proveedor de un sistema de alto riesgo está establecido fuera de la Unión, el Reglamento de Inteligencia Artificial puede exigir la designación de un representante autorizado establecido en la Unión antes de introducir el sistema en el mercado europeo. Además, la cadena de comercialización puede incluir:

- proveedor;
- representante autorizado;
- importador;
- distribuidor;
- responsable del despliegue.

Cada figura tiene obligaciones distintas. El importador y el distribuidor no son simples intermediarios comerciales cuando introducen o facilitan el acceso a un sistema regulado.

Antes de comercializar determinados sistemas de alto riesgo, el distribuidor debe comprobar, entre otros extremos, la existencia del marcado CE, la declaración de conformidad, las instrucciones y el cumplimiento de obligaciones correspondientes al proveedor y, en su caso, al importador.

El contrato no determina por sí solo el rol regulatorio

Una entidad puede denominarse contractualmente «revendedor» y actuar materialmente como:

- importador;
- integrador;
- proveedor;
- distribuidor;
- fabricante de producto.

La calificación depende de la actividad realmente desarrollada. Especialmente relevante es el supuesto en el que una empresa:

- comercializa el sistema bajo su propia marca;
- cambia su finalidad;
- lo modifica sustancialmente;
- lo integra en un producto propio;
- reentrena de forma determinante el modelo.

En estas situaciones puede asumir obligaciones superiores a las correspondientes a un mero usuario.

El importador de alimentos no puede invocar la distancia tecnológica

El artículo 11 del Reglamento (CE) n.º 178/2002 exige que los alimentos y piensos importados para su comercialización en la Unión cumplan los requisitos pertinentes de la legislación alimentaria europea o condiciones reconocidas como equivalentes.

Por ello, un importador europeo no puede justificar un alimento inseguro alegando que:

- la fábrica extranjera utilizó un algoritmo defectuoso;
- el modelo fue desarrollado en otro país;
- el laboratorio se encontraba fuera de la Unión;
- el certificado de conformidad fue generado automáticamente;
- el proveedor extranjero no facilita los registros.

La externalización geográfica puede dificultar la investigación, pero no elimina las obligaciones del operador que importa y comercializa el alimento.

Diligencia reforzada del importador

Cuando el fabricante extranjero utiliza IA para funciones críticas, el importador debería verificar:

- finalidad del sistema;
- validación;
- equivalencia de los controles;
- disponibilidad de registros;
- acceso a los datos de los lotes;
- procedimientos de retirada;
- conservación documental;
- cooperación en inspecciones;
- identidad de proveedores tecnológicos;
- capacidad de reproducir decisiones.

Una certificación genérica de la planta no sustituye esta evaluación cuando el sistema algorítmico determina:

- esterilidad;
- tratamiento térmico;
- vida útil;
- declaración de alérgenos;
- liberación;
- detección de contaminantes.

La futura responsabilidad europea cuando el fabricante está fuera de la Unión

La Directiva (UE) 2024/2853 busca asegurar que exista un sujeto establecido en la Unión frente al que el perjudicado pueda dirigir una reclamación cuando el fabricante del producto defectuoso se encuentre en un tercer país. Sin perjuicio de la posible responsabilidad del fabricante extranjero, la Directiva contempla, según la estructura de la cadena:

- al importador;
- al representante autorizado;
- cuando no exista ninguno de los anteriores, al prestador de servicios logísticos;
- en determinadas circunstancias, al distribuidor que no identifique oportunamente a un operador económico responsable.

La Directiva incluye dentro del concepto de producto al software y reconoce como operadores económicos al fabricante, proveedor de un servicio relacionado, representante autorizado, importador, prestador de servicios logísticos y distribuidor.

Este régimen deberá aplicarse a los productos introducidos en el mercado o puestos en servicio a partir del 9 de diciembre de 2026, una vez incorporado al Derecho nacional. Hasta ese momento, deben aplicarse el régimen vigente y las restantes normas civiles, contractuales y sectoriales pertinentes.

Consecuencia estratégica

Una empresa europea que importe o distribuya software alimentario no debe asumir que toda responsabilidad podrá trasladarse al desarrollador extranjero. Puede convertirse en el sujeto económicamente accesible frente a:

- consumidores;
- clientes;
- autoridades;
- aseguradoras;
- otros operadores de la cadena.

Por ello debe disponer de:

- acción contractual de repetición;
- garantías;
- seguro del proveedor;
- documentación técnica;
- derecho de auditoría;
- cooperación procesal;
- jurisdicción ejecutable.

Una indemnidad firmada por una empresa sin activos o sin presencia ejecutable tiene un valor práctico muy limitado.

Jurisdicción: ante qué tribunales puede plantearse el litigio

En litigios civiles y mercantiles dentro de la Unión, el Reglamento (UE) n.º 1215/2012 —Bruselas I bis— establece como regla general que las personas domiciliadas en un Estado miembro sean demandadas ante los tribunales de ese Estado. El Reglamento también reconoce foros especiales en materia contractual y extracontractual.

Acciones contractuales

En una reclamación del operador español contra el proveedor tecnológico europeo podrá ser competente, según el contrato y las circunstancias:

- el tribunal expresamente elegido;
- el tribunal del domicilio del demandado;
- el tribunal del lugar de cumplimiento de la obligación contractual relevante.

La identificación del lugar de cumplimiento puede ser compleja en servicios digitales porque:

- el proveedor trabaja desde un país;
- el servidor está en otro;
- la planta se encuentra en España;
- el resultado se entrega remotamente;
- la obligación combina licencia, soporte, integración y mantenimiento.

Por ello, la cláusula de jurisdicción debe redactarse expresamente.

Acciones extracontractuales

En materia delictual o cuasidelictual, el Reglamento permite acudir a los tribunales del lugar donde se produjo o puede producirse el hecho dañoso.

En una cadena alimentaria pueden existir varios lugares relevantes:

- lugar donde se diseñó o actualizó defectuosamente el sistema;
- lugar donde se adoptó la decisión;
- lugar donde se fabricó el alimento;
- lugar donde se consumió;
- lugar donde se manifestó el daño.

La elección del foro debe analizarse caso por caso. No debe asumirse automáticamente que el litigio deberá plantearse en el país del desarrollador.

Acuerdo de elección de foro

El artículo 25 de Bruselas I bis reconoce, con las condiciones previstas en la norma, los acuerdos por los que las partes atribuyen competencia a los tribunales de un Estado miembro para resolver disputas derivadas de una relación jurídica determinada.

Una cláusula adecuada debería precisar:

- tribunal o Estado elegido;
- carácter exclusivo o no exclusivo;
- contratos y anexos cubiertos;
- acciones contractuales relacionadas;
- medidas cautelares;
- pluralidad de demandados;
- vigencia después de la terminación.

El error de confundir jurisdicción con ley aplicable

Dos cuestiones distintas pueden resolverse mediante cláusulas diferentes:

Jurisdicción

Determina qué tribunal conoce del litigio.

Ley aplicable

Determina qué Derecho sustantivo utiliza ese tribunal.

Un contrato puede atribuir competencia a tribunales españoles y someter el fondo del contrato a Derecho irlandés. Pero también puede ocurrir lo contrario:

- tribunal extranjero;
- Derecho español aplicable.

La redacción «este contrato se regirá por los tribunales de Madrid» es técnicamente deficiente porque mezcla ambos conceptos.

Ley aplicable al contrato: Reglamento Roma I

El Reglamento (CE) n.º 593/2008, (Roma I), permite que las partes elijan la ley aplicable a su contrato. La elección debe constar expresamente o resultar claramente de los términos del contrato o de las circunstancias. Para el caso de que no exista elección válida, el Reglamento establece reglas de conexión según la naturaleza contractual. En los contratos de prestación de servicios, la regla general conduce al Derecho del país donde el prestador tiene su residencia habitual, salvo que de las circunstancias resulte una conexión manifiestamente más estrecha con otro país.

Riesgo para el operador alimentario

Una empresa española puede contratar en línea una solución extranjera y aceptar, sin advertirlo:

- Derecho de otro Estado;
- jurisdicción remota;
- arbitraje extranjero;
- limitaciones de responsabilidad;
- exclusión de retirada;
- plazos breves de reclamación;
- obligación de pagar costas;
- prohibición de auditoría.

Estas condiciones pueden encontrarse incorporadas mediante:

- hipervínculo;
- clickwrap;
- orden de compra;
- renovación automática;

- condiciones de la nube;
- anexos del distribuidor.

La *due diligence* contractual debe examinar la cadena documental completa, no únicamente la propuesta comercial principal.

Las normas imperativas no desaparecen

La elección de una ley extranjera no permite eludir las normas imperativas aplicables a:

- seguridad alimentaria;
- control oficial;
- retirada;
- etiquetado;
- protección de consumidores;
- vigilancia del mercado;
- protección de datos;
- responsabilidad penal.

El contrato regula principalmente la relación interna. No privatiza la potestad regulatoria de las autoridades europeas o españolas.

Ley aplicable a la responsabilidad extracontractual y al producto defectuoso

El Reglamento Roma II establece, como regla general, la aplicación de la ley del país donde se produce el daño directo, con independencia del país donde ocurrió el hecho que lo originó o donde se manifiesten consecuencias indirectas. Para la responsabilidad por productos existe una regla específica en cascada.

Sin perjuicio de determinados supuestos, se atiende sucesivamente:

111. al país de residencia habitual del perjudicado, si el producto se comercializó allí;
112. en su defecto, al país donde se adquirió el producto, si se comercializó allí;
113. en su defecto, al país donde se produjo el daño, si el producto se comercializó allí.

Si el presunto responsable no podía prever razonablemente la comercialización del producto o de otro del mismo tipo en ese país, puede resultar aplicable la ley de su residencia habitual.

Relevancia para sistemas algorítmicos

En un daño causado por un alimento cuya inseguridad deriva de un sistema de IA, pueden coexistir:

- acción por producto alimentario defectuoso;
- acción contra el fabricante del software;
- acción por negligencia del integrador;
- acción contractual entre empresas;
- reclamación frente al laboratorio.

No todas estas acciones tienen necesariamente:

- el mismo foro;
- la misma ley aplicable;
- los mismos plazos;
- la misma carga de la prueba.

La estrategia procesal debe construir un mapa separado para cada demandado y cada título de responsabilidad.

Cláusulas de ley y jurisdicción: utilidad y límites

Una cláusula bien redactada aporta previsibilidad entre las partes empresariales, pero no resuelve toda la responsabilidad.

No vinculará necesariamente a:

- consumidores perjudicados que no fueron parte;
- autoridades administrativas;
- Ministerio Fiscal;

- terceros distribuidores;
- trabajadores;
- aseguradoras ajenas al contrato.

Tampoco puede eliminar normas indisponibles.

Redacción insuficiente

“Cualquier controversia se resolverá conforme a la legislación del proveedor.”

Problemas:

- no identifica el país;
- puede variar si el proveedor cambia de sede;
- no determina tribunal;
- no regula medidas cautelares;
- no cubre filiales o subcontratistas;
- puede generar incertidumbre sobre el Derecho aplicable.

Redacción operativa

La cláusula debe definir separadamente:

- Derecho aplicable;
- tribunales competentes;
- exclusividad;
- medidas cautelares;
- idioma;
- notificaciones;
- ejecución;
- acumulación de acciones;
- cooperación probatoria.

Arbitraje en contratos tecnológicos alimentarios

El arbitraje puede ofrecer:

- especialización;
- confidencialidad;
- flexibilidad;
- ejecución internacional;
- elección de idioma.

Pero presenta riesgos:

- coste elevado;
- dificultad para incorporar a terceros;
- ausencia de acumulación automática;
- medidas probatorias limitadas según el sistema;
- necesidad de acudir a tribunales para ciertas cautelares;
- complejidad cuando hay consumidores o autoridades.

En una cadena con proveedor, integrador, laboratorio, operador y aseguradoras, cláusulas arbitrales incompatibles pueden fragmentar el conflicto en varios procedimientos.

Antes de aceptar arbitraje debe comprobarse:

- institución;
- sede;
- idioma;
- número de árbitros;
- reglas probatorias;
- medidas de urgencia;
- posibilidad de acumulación;
- ley aplicable;

- costes;
- relación con las pólizas.

Grupos societarios: la marca común no identifica necesariamente al responsable

En los grupos empresariales pueden intervenir:

- matriz tecnológica;
- filial comercial europea;
- empresa que factura;
- entidad propietaria del modelo;
- sociedad que presta soporte;
- distribuidor local.

El uso de una marca común no permite conocer automáticamente:

- qué entidad contrató;
- cuál desarrolló el modelo;
- quién decide las actualizaciones;
- quién posee los datos;
- quién está asegurado;
- quién tiene activos.

Identificación contractual obligatoria

El contrato debe recoger:

- denominación social completa;
- domicilio;
- número registral o fiscal;
- función;
- obligaciones;
- garantías;
- entidad asegurada;
- responsabilidad por filiales;
- autorización para subcontratar.

La filial sin capacidad técnica

Una estructura de riesgo aparece cuando:

- la filial europea firma el contrato;
- toda la tecnología está en la matriz extranjera;
- la filial carece de acceso a logs;
- no puede corregir el modelo;
- su capital es reducido;
- la matriz no presta garantía.

En tal situación, el operador puede disponer formalmente de un proveedor europeo, pero carecer de un responsable con capacidad técnica y patrimonial suficiente.

Debe exigirse, cuando proceda:

- garantía de la matriz;
- responsabilidad solidaria contractual;
- acceso directo a documentación;
- seguro suficiente;
- continuidad del servicio;
- depósito o escrow de componentes esenciales.

Subcontratistas y proveedores en cadena

El proveedor principal puede depender de:

- modelos de propósito general;
- servicios cloud;
- bases de datos;
- sensores;
- herramientas de etiquetado;
- empresas de anotación;
- desarrolladores externos.

El operador alimentario no necesita contratar directamente con todos ellos, pero sí debe conocer las dependencias críticas.

Riesgo de la cláusula abierta

Una autorización genérica para subcontratar «cualquier servicio necesario» puede permitir cambios materiales sin control.

En funciones críticas debería regularse:

- lista o categoría de subcontratistas;
- aviso de cambios;
- derecho de oposición justificada;
- responsabilidad del proveedor principal;
- localización de datos;
- continuidad;
- cooperación probatoria;
- devolución de información.

El proveedor principal no debe poder eludir su responsabilidad alegando que el defecto procedía de una API, un modelo base o una plataforma cloud que él mismo seleccionó.

Datos y pruebas alojados en terceros países

Un sistema puede almacenar fuera de España:

- logs;
- históricos;
- imágenes;
- datos de producción;
- resultados de laboratorio;
- identificadores de empleados;
- comunicaciones;
- versiones del modelo.

Esta configuración plantea simultáneamente riesgos de:

- disponibilidad;
- jurisdicción;
- secreto empresarial;
- protección de datos;
- conservación;
- ejecución judicial.

Acceso contractual

El operador debería asegurarse de que puede:

- exportar los registros;
- conservarlos localmente;
- obtenerlos en formato legible;
- vincularlos a lotes;
- preservar versiones;
- entregarlos a autoridades;
- utilizarlos en un litigio;

- mantener acceso después de terminar el contrato.

Una plataforma que permite visualizar datos, pero no descargarlos con metadatos e integridad, puede resultar insuficiente para una investigación.

Transferencias internacionales de datos personales

Cuando los registros contienen datos personales, por ejemplo identificadores de empleados, firmas, imágenes o perfiles de usuario, las transferencias a terceros países deben cumplir el capítulo V del Reglamento General de Protección de Datos. El artículo 44 exige que responsables y encargados respeten las condiciones previstas para la transferencia y las transferencias ulteriores.

La necesidad de conservar evidencia no autoriza por sí sola cualquier circulación internacional de datos.

Deben analizarse:

- base jurídica;
- minimización;
- contrato de encargado;
- país de destino;
- decisión de adecuación;
- garantías apropiadas;
- acceso de autoridades extranjeras;
- medidas complementarias;
- plazo de conservación.

Preservación ante litigio

El contrato debe obligar al proveedor extranjero a:

- suspender borrados automáticos;
- preservar versiones;
- conservar logs;
- colaborar con peritos;
- autenticar documentos;
- responder a requerimientos;
- evitar modificaciones durante la investigación.

Sin esta obligación, la evidencia puede desaparecer antes de que el operador consiga una orden judicial efectiva.

Medidas judiciales para obtener o preservar pruebas

La Ley de Enjuiciamiento Civil permite, bajo los presupuestos correspondientes:

- diligencias preliminares;
- exhibición de documentos;
- aportación de soportes electrónicos;
- prueba pericial;
- medidas cautelares.

Los documentos requeridos pueden presentarse electrónicamente y los tribunales pueden ordenar la exhibición de documentos relevantes bajo control de la contraparte o, en determinados supuestos, de terceros.

Los instrumentos que permiten archivar, conocer o reproducir datos, cifras y operaciones son medios de prueba admisibles cuando resultan relevantes para el proceso.

El problema práctico

Una orden española puede no bastar por sí sola cuando:

- el proveedor está fuera de la Unión;
- los datos están controlados por otra sociedad;
- existen leyes extranjeras incompatibles;
- el contrato atribuye jurisdicción a otro país;
- la información se ha borrado;

- el modelo pertenece a un tercero.

La contratación debe anticipar estas dificultades.

La mejor prueba no es la que un tribunal consigue recuperar después de años. Es la que la empresa conservó legítimamente desde el inicio.

Conflictos entre autoridades

Un incidente transfronterizo puede afectar a:

- autoridad sanitaria española;
- autoridad del Estado de destino;
- autoridad de vigilancia del mercado de IA;
- autoridad de protección de datos;
- autoridades aduaneras;
- Comisión Europea;
- autoridades de terceros países.

La investigación puede avanzar con ritmos y objetivos diferentes.

Coherencia de comunicaciones

La empresa debe evitar que distintos departamentos comuniquen versiones contradictorias.

Debe existir una fuente de hechos verificados que diferencie:

- información confirmada;
- hipótesis;
- acciones adoptadas;
- datos pendientes;
- análisis jurídicos;
- comunicaciones públicas.

No debe enviarse a una autoridad alimentaria una explicación que atribuya el incidente al algoritmo mientras se sostiene ante la autoridad de IA que el sistema funcionó correctamente.

La coordinación no significa ocultación. Significa rigor factual y coherencia.

Caso transfronterizo integrado

Una empresa española produce una bebida funcional refrigerada. Utiliza un modelo desarrollado por una compañía estadounidense y contratado a través de su distribuidor irlandés. El modelo estima la vida útil microbiológica.

El producto se vende en España, Francia y Bélgica. Varios consumidores belgas resultan afectados por contaminación microbiológica.

Sujetos potenciales

- fabricante español del alimento;
- Director Técnico;
- distribuidor irlandés del sistema;
- desarrollador estadounidense;
- integrador español;
- laboratorio externo;
- distribuidores alimentarios;
- aseguradoras.

Responsabilidad alimentaria

El fabricante español mantiene la responsabilidad primaria sobre el producto que fabrica y comercializa. No puede desplazarla automáticamente al proveedor del modelo.

Responsabilidad tecnológica

Debe determinarse:

- quién validó el modelo;
- quién definió la vida útil;
- si el sistema se utilizó dentro de finalidad;
- qué información proporcionó el desarrollador;
- qué modificaciones realizó el integrador;
- qué entidad controlaba la actualización.

Jurisdicción

Pueden existir distintos foros según:

- domicilio del demandado;
- lugar de cumplimiento contractual;
- lugar del daño;
- cláusula de jurisdicción;
- posición del consumidor;
- pluralidad de demandados.

Ley aplicable

- El contrato entre operador y distribuidor podrá quedar sometido a la ley elegida conforme a Roma I.
- La reclamación del consumidor por producto defectuoso se analizará conforme a las reglas de Roma II.
- La sanción alimentaria se regirá por el Derecho administrativo de la autoridad competente.
- Las posibles responsabilidades penales se determinarán conforme a sus reglas propias.

Prueba

Será necesario obtener:

- logs de servidores extranjeros;
- versión del modelo;
- datos de formulación;
- challenge tests;
- registros térmicos;
- informes del laboratorio;
- comunicaciones del distribuidor;
- documentación comercial del desarrollador.

Conclusión

No existe un único «litigio de IA».

Existe un conjunto coordinado de:

- procedimientos regulatorios;
- reclamaciones contractuales;
- acciones de producto;
- investigaciones técnicas;
- comunicaciones transfronterizas.

La estrategia debe diseñarse globalmente desde las primeras horas del incidente.

Lista de control para contratar un proveedor extranjero

Identidad y solvencia

- ¿Qué entidad firma?
- ¿Dónde está domiciliada?
- ¿Tiene activos?
- ¿Quién controla la tecnología?
- ¿Existe garantía de la matriz?

- ¿Dispone de seguro?

Regulación

- ¿Está sujeto al AI Act?
- ¿Tiene representante autorizado?
- ¿Quién es importador?
- ¿Quién es distribuidor?
- ¿Qué obligaciones resultan aplicables?

Contrato

- ¿Qué ley se aplica?
- ¿Qué tribunales son competentes?
- ¿Existe arbitraje?
- ¿Puede acumularse la reclamación?
- ¿Hay limitación de responsabilidad?
- ¿Se cubre la retirada?

Datos y evidencias

- ¿Dónde se almacenan?
- ¿Puede exportarlos el operador?
- ¿Durante cuánto tiempo?
- ¿Se conserva cada versión?
- ¿Puede una autoridad acceder?
- ¿Se cumplen las reglas de protección de datos?

Continuidad

- ¿Qué ocurre si el proveedor desaparece?
- ¿Puede mantenerse el sistema?
- ¿Existe modo manual?
- ¿Puede recuperarse la información?
- ¿Hay depósito de código o documentación crítica?

Incidentes

- ¿Qué plazo de comunicación existe?
- ¿Quién investiga?
- ¿Quién paga?
- ¿Quién notifica?
- ¿Quién preserva la prueba?
- ¿Quién ejecuta la corrección?

Recomendación contractual para operadores alimentarios europeos

Cuando el sistema afecta a seguridad, legalidad o liberación de producto, el operador debería evitar contratar si no dispone, como mínimo, de:

114. entidad contractual claramente identificada;
115. ley y jurisdicción definidas;
116. documentación de finalidad y límites;
117. métricas verificables;
118. derecho de acceso a logs;
119. obligación de preservación;
120. control de actualizaciones;
121. cooperación con autoridades;
122. responsabilidad por subcontratistas;
123. seguro suficiente;
124. indemnidad económicamente ejecutable;
125. procedimiento de continuidad y salida.

La ausencia de una de estas garantías no convierte automáticamente el contrato en ilícito. Pero debe considerarse una exposición que requiere mitigación y aprobación expresa.

Síntesis: la nube no disuelve la responsabilidad

La distribución internacional de un sistema puede hacer invisible la cadena tecnológica para el usuario final, pero no elimina los deberes jurídicos.

El operador europeo debe saber:

- quién fabrica el sistema;
- quién lo introduce en el mercado;
- quién lo integra;
- quién controla los datos;
- quién puede corregirlo;
- quién conserva la evidencia;
- contra quién puede reclamar.

El AI Act puede alcanzar a proveedores situados fuera de la Unión cuando los resultados de sus sistemas se utilizan en territorio europeo. La legislación alimentaria continúa vinculando al operador y al importador. Las reglas europeas de jurisdicción y ley aplicable permiten distribuir los litigios, pero no garantizan que el responsable extranjero sea patrimonialmente accesible.

La verdadera soberanía tecnológica de una empresa alimentaria no consiste en desarrollar internamente todos sus algoritmos. Consiste en no depender de ningún sistema cuya actuación no pueda conocer, detener, documentar y someter a responsabilidad efectiva.

Cuando una empresa contrata una IA extranjera sin acceso a versiones, registros, validación o responsables solventes, no está transfiriendo el riesgo. Está perdiendo el control sobre él.

CAPÍTULO 11. MODELO OPERATIVO DE ATRIBUCIÓN Y PROGRAMA DE IMPLANTACIÓN

El cierre operativo transforma el análisis jurídico en herramientas de decisión: árbol de imputación, matrices por actores y casos de uso, criterios de exoneración o reducción, decálogo del Director Técnico y programa de implantación. Su finalidad es que la empresa pueda convertir principios jurídicos en controles verificables.

Árbol jurídico de atribución de responsabilidades

La atribución de responsabilidad no debe comenzar preguntando quién fabricó el algoritmo. Debe seguir una secuencia ordenada que permita diferenciar incumplimiento, daño, causalidad, culpabilidad y posición de control.

Paso 1. ¿Qué ocurrió realmente?

Debe identificarse el resultado jurídicamente relevante:

- alimento inseguro;
- etiquetado incorrecto;
- omisión de un alérgeno;
- incumplimiento de un límite legal;
- falso resultado analítico;
- vida útil excesiva;
- liberación indebida de un lote;
- retirada tardía;
- tratamiento térmico insuficiente;
- dosificación incorrecta;
- daño corporal;
- daño patrimonial;
- infracción documental;
- actuación administrativa inválida.

No todo error algorítmico causa un daño. Puede existir:

- incumplimiento regulatorio sin lesión;
- daño sin infracción del Reglamento de Inteligencia Artificial;
- infracción del Reglamento de Inteligencia Artificial sin daño alimentario;
- daño derivado de una causa completamente ajena al sistema.

Paso 2. ¿Qué función desempeñó la IA?

Debe distinguirse si el sistema:

126. generó información;
127. recomendó una actuación;
128. clasificó una muestra o lote;
129. sustituyó una comprobación humana;
130. ejecutó automáticamente una decisión;
131. controló directamente un equipo o proceso;
132. ocultó o no detectó una desviación;
133. produjo documentación regulatoria;
134. priorizó una inspección o actuación administrativa.

La relevancia causal aumenta cuando el sistema deja de ser una herramienta informativa y se convierte en una barrera de seguridad o en el ejecutor de una decisión irreversible.

Paso 3. ¿La salida fue realmente errónea?

Debe comprobarse si existió:

- error del modelo;
- error en los datos de entrada;
- error del sensor;
- error de integración;
- error de interpretación humana;
- uso fuera de finalidad;
- cambio de formulación no comunicado;
- descalibración;
- actualización defectuosa;
- resultado correcto seguido de una decisión humana incorrecta.

Es posible que el algoritmo haya producido una advertencia adecuada y que la empresa la haya ignorado. También puede ocurrir que la salida fuera incorrecta porque el operador introdujo datos falsos o incompletos.

Paso 4. ¿Qué sujetos intervinieron?

Debe identificarse a todas las personas físicas y jurídicas:

- proveedor del modelo;
- fabricante de la aplicación;
- desarrollador;
- distribuidor;
- importador;
- representante autorizado;
- integrador;
- fabricante del sensor;
- proveedor cloud;
- laboratorio;
- operador alimentario;
- responsable de calidad;
- Director Técnico;
- responsables de producción;
- órgano de administración;
- Administración pública.

No debe aceptarse la denominación contractual sin analizar la función real. Una entidad presentada como integrador puede haber efectuado una modificación sustancial y asumir materialmente funciones de proveedor.

Paso 5. ¿Qué deber correspondía a cada sujeto?

La responsabilidad exige asociar cada participante con una obligación concreta:

- diseñar;
- validar;
- advertir;
- documentar;
- suministrar información;
- mantener;
- actualizar;
- supervisar;
- verificar;
- impedir la liberación;
- retirar;
- comunicar;
- preservar registros;
- asignar recursos;
- detener el proceso.

La imputación no puede construirse únicamente desde el organigrama o el título profesional.

Paso 6. ¿Quién controlaba el riesgo?

Debe determinarse quién tenía capacidad para:

- seleccionar el sistema;
- modificar parámetros;
- conocer sus límites;
- detenerlo;
- ordenar una verificación;
- bloquear el lote;
- paralizar la línea;
- comunicar a la autoridad;
- ordenar una retirada.

La responsabilidad tiende a concentrarse en quien reúne simultáneamente:

135. conocimiento;
136. competencia;
137. autoridad;
138. capacidad material de intervención.

Paso 7. ¿Era previsible el fallo?

Debe analizarse si existían:

- advertencias del proveedor;
- desviaciones previas;
- falsos negativos conocidos;
- resultados discordantes;
- cambios de matriz;
- sensores inestables;
- alertas de ciberseguridad;
- incidencias de versiones anteriores;
- observaciones del laboratorio;
- comunicaciones del Director Técnico.

Un fallo que inicialmente pudiera calificarse como imprevisible puede convertirse en negligente cuando la empresa continúa utilizando el sistema después de detectar señales consistentes.

Paso 8. ¿Qué barreras debían impedir el daño?

La investigación debe reconstruir las barreras previstas:

- validación;

- revisión humana;
- análisis de confirmación;
- doble firma;
- bloqueo automático;
- límites de proceso;
- APPCC;
- auditoría;
- mantenimiento;
- procedimiento de retirada.

Si varias barreras fallaron, puede existir una responsabilidad concurrente de distintos sujetos.

Paso 9. ¿Existe relación causal?

Debe determinarse si el daño se habría producido igualmente sin el fallo.

La relación causal puede:

- atribuirse principalmente a un sujeto;
- distribuirse entre varios;
- quedar interrumpida por una actuación posterior;
- no poder demostrarse con certeza suficiente.

La mera intervención de un algoritmo en el proceso no demuestra que haya causado el resultado.

Paso 10. ¿Qué régimen jurídico resulta aplicable?

Puede concurrir:

- responsabilidad contractual;
- responsabilidad civil extracontractual;
- responsabilidad objetiva por producto defectuoso;
- responsabilidad administrativa alimentaria;
- responsabilidad conforme al Reglamento de Inteligencia Artificial;
- responsabilidad societaria;
- responsabilidad penal;
- responsabilidad penal de la persona jurídica;
- responsabilidad patrimonial de la Administración.

Paso 11. ¿Qué grado de culpabilidad existe?

Debe distinguirse:

- ausencia de culpa;
- negligencia ordinaria;
- negligencia profesional;
- imprudencia grave;
- dolo eventual;
- conducta intencional.

La sanción administrativa española exige culpabilidad. La responsabilidad penal requiere los elementos específicos del tipo penal. La responsabilidad por productos defectuosos responde, en cambio, a un régimen objetivo en el que no es necesario demostrar culpa del productor, aunque sí defecto, daño y causalidad en los términos legalmente aplicables.

Paso 12. ¿Qué medidas deben adoptarse inmediatamente?

La determinación definitiva de la responsabilidad puede llevar meses o años. La protección del consumidor no puede esperar.

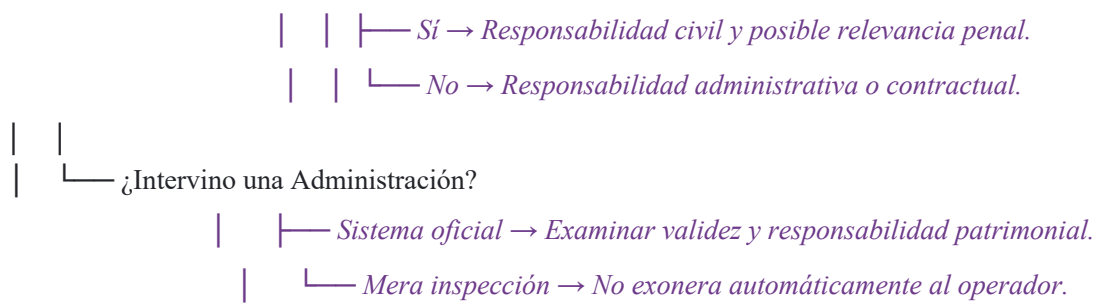
Debe decidirse de inmediato:

- bloqueo;
- inmovilización;
- retirada;
- recuperación;

- información al consumidor;
- notificación a la autoridad;
- suspensión del sistema;
- preservación de evidencias;
- activación de aseguradoras.

Árbol abreviado de decisión

¿Existe daño o incumplimiento?
│
├── *No → Registrar, investigar y corregir.*
│
└── **Sí**
│
├── ¿La IA intervino materialmente?
│ ├── *No → Aplicar responsabilidad alimentaria ordinaria.*
│ └── **Sí**
│ │
│ ├── ¿Falló el modelo?
│ │ ├── *Sí → Analizar proveedor, fabricante e integrador.*
│ │ └── **No**
│ │ │
│ ├── ¿Fallaron los datos o sensores?
│ │ ├── *Sí → Analizar operador, integrador y mantenedor.*
│ │ └── **No**
│ │ │
│ ├── ¿Se usó fuera de finalidad?
│ │ ├── *Sí → Analizar operador y quien autorizó el cambio.*
│ │ └── **No**
│ │ │
│ ├── ¿Existía revisión humana?
│ │ ├── *No → Analizar diseño organizativo y nivel de autonomía.*
│ │ └── **Sí**
│ │ ├── ¿Era real y competente?
│ │ ├── ¿Tenía autoridad?
│ │ └── ¿Ignoró advertencias?
│ │
│ ├── ¿El producto llegó al mercado?
│ │ ├── *Sí → Responsabilidad primaria del operador alimentario.*
│ │ └── *No → Incumplimiento interno o regulatorio sin daño externo.*
│ │
│ ├── ¿Hubo daño corporal o patrimonial?



Matriz consolidada de responsabilidades por actores

Actor	Deber jurídico o técnico principal	Supuestos de responsabilidad	Régimen posible	Elementos de defensa
Proveedor o fabricante del sistema	Diseñar un sistema seguro, documentado y adecuado a su finalidad	Diseño defectuoso, datos no representativos, métricas engañosas, falta de advertencias, actualización defectuosa	AI Act, contractual, producto defectuoso, extracontractual	Uso fuera de finalidad, modificación por tercero, datos falsos del cliente
Desarrollador de modelo base	Cumplir las obligaciones que correspondan a su posición real	Defecto del componente, información insuficiente, vulnerabilidades conocidas	Contractual, producto defectuoso, AI Act según clasificación	Falta de causalidad, integración defectuosa ajena
Integrador	Conectar correctamente modelo, sensores, procesos y sistemas	Errores de configuración, unidades incompatibles, umbrales incorrectos, modificación sustancial	Contractual, profesional, producto defectuoso, AI Act	Especificaciones erróneas del operador o proveedor
Importador o distribuidor tecnológico	Verificar los elementos regulatorios que correspondan y no comercializar sistemas no conformes	Falta de comprobación, ocultación de riesgo, distribución tras conocer el defecto	AI Act, contractual, producto defectuoso	Documentación razonablemente fiable del proveedor, ausencia de conocimiento
Proveedor de sensores o maquinaria	Garantizar funcionamiento, calibración e integración segura	Datos incorrectos, ausencia de alarmas, fallo inseguro	Producto defectuoso, contractual	Mantenimiento omitido o manipulación del operador
Laboratorio	Aplicar métodos adecuados y emitir resultados técnicamente defendibles	Muestreo deficiente, método inapropiado, IA analítica no validada, interpretación errónea	Contractual, profesional, administrativa, civil	Muestra no representativa remitida por el operador, uso incorrecto del informe
Operador alimentario	Garantizar el cumplimiento y seguridad de los alimentos bajo su control	Comercialización insegura, APPCC deficiente, falta de validación, retirada tardía, etiquetado incorrecto	Alimentaria administrativa, civil, contractual, penal	Fallo imprevisible pese a controles adecuados; reacción inmediata; ruptura causal
Responsable de calidad	Aplicar controles, verificar resultados y bloquear desviaciones	Revisión puramente formal, liberación incorrecta, ignorar alertas	Laboral, disciplinaria, civil o penal según funciones	Falta de autoridad, advertencias documentadas, información inaccesible
Director Técnico	Ejercer las funciones técnicas realmente atribuidas con diligencia profesional	Validación indebida, omisión consciente, autorización fuera de alcance, ocultación	Civil, laboral, administrativa o penal según el caso	Falta de competencia real, oposición documentada, imposibilidad de evitar el resultado
Dirección General	Proporcionar recursos y adoptar decisiones organizativas diligentes	Automatización sin controles, presión para liberar, rechazo de advertencias	Societaria, civil, administrativa, penal	Delegación razonable con supervisión efectiva
Administradores	Dirección y control diligente de la sociedad	Defecto estructural de gobierno, ausencia de compliance, tolerancia consciente del riesgo	Societaria, civil y penal en supuestos legalmente previstos	Modelo de organización eficaz, información adecuada y respuesta diligente
Persona jurídica	Mantener una organización capaz de prevenir infracciones	Falta grave de supervisión y control, cultura de incumplimiento	Administrativa, civil, penal en delitos previstos	Programa eficaz, controles reales, reacción y cooperación
Administración pública	Actuar conforme a legalidad, motivación, control y supervisión	Sistema oficial defectuoso, decisión automatizada ilegal, daño antijurídico	Invalidez del acto, responsabilidad patrimonial	Fuerza mayor, inexistencia de daño antijurídico o causalidad
Trabajador usuario	Seguir instrucciones, revisar y comunicar anomalías	Manipulación, desactivación, ocultación o uso abiertamente indebido	Laboral, disciplinaria, civil o penal	Formación insuficiente, interfaz engañosa, presión jerárquica, ausencia de autoridad

Tabla 14. Matriz consolidada de responsabilidades por actores.

Respuesta directa: quién responde cuando falla la IA

La respuesta jurídicamente correcta no consiste en elegir un único sujeto. El operador alimentario ocupa la posición primaria respecto del producto que introduce en el mercado; el proveedor responde por defectos o incumplimientos situados en su esfera; el laboratorio por la calidad de su actividad analítica; el Director Técnico cuando sus funciones, conocimiento y capacidad de intervención permiten una imputación personal; la dirección y los administradores cuando el incidente revela un defecto estructural de organización; y la Administración por sus propias decisiones automatizadas. La distribución final dependerá del deber incumplido, la causalidad y la prueba.

Circunstancias que no exoneran por sí solas

«Lo decidió el algoritmo»

La IA no es sujeto jurídico responsable y su intervención no rompe la cadena de imputación.

«El sistema estaba certificado»

Una certificación acredita un alcance determinado y no demuestra necesariamente:

- idoneidad para la matriz concreta;
- correcta integración;
- funcionamiento posterior;
- ausencia de deriva;
- uso conforme.

«El proveedor es líder del mercado»

La reputación no sustituye la evaluación de idoneidad.

«Había una persona supervisando»

Debe demostrarse que la supervisión era:

- competente;
- informada;
- independiente;
- dotada de tiempo;
- provista de autoridad.

«El sistema acertaba en el 99 % de los casos»

La exactitud global puede ocultar falsos negativos críticos.

Un sistema puede alcanzar una precisión elevada y resultar inaceptable si falla precisamente en la detección del peligro que debe controlar.

«Se contrató a un laboratorio acreditado»

La acreditación no convierte una muestra no representativa en representativa ni justifica utilizar un ensayo fuera de su alcance.

«La actualización era automática»

La automatización del cambio no elimina el deber de control de versiones.

«Fue un ciberataque»

Debe examinarse si:

- la vulnerabilidad era conocida;
- existían medidas razonables;
- se aplicaron actualizaciones;
- había segmentación;
- el sistema fallaba de modo seguro;
- se detectó y comunicó a tiempo.

«El error fue de un trabajador»

La empresa puede continuar respondiendo cuando el error fue favorecido por:

- falta de formación;
- carga de trabajo;
- interfaz deficiente;
- procedimientos ambiguos;
- presión productiva;
- ausencia de doble control.

«La autoridad no había formulado objeciones»

La ausencia de objeciones administrativas no equivale a una garantía de seguridad.

Circunstancias que pueden excluir, reducir o redistribuir la responsabilidad

Fallo científicamente imprevisible

Puede ser relevante cuando el sistema:

- estaba adecuadamente validado;
- se utilizó dentro de su alcance;
- se vigilaba correctamente;
- no existían señales previas;
- se aplicó el estado de la técnica.

En materia alimentaria, esta defensa debe manejarse con especial cautela, especialmente en la responsabilidad por el alimento defectuoso.

Uso fuera de finalidad por el cliente

Puede liberar total o parcialmente al proveedor cuando:

- la limitación estaba claramente documentada;
- el uso no era razonablemente previsible;
- el proveedor no participó en el cambio;
- el daño deriva precisamente del uso indebido.

Modificación sustancial por un tercero

Puede desplazar la responsabilidad hacia quien:

- reentrenó;
- cambió parámetros;
- alteró la finalidad;
- comercializó bajo su marca;
- integró el sistema en una nueva solución.

Ruptura de la cadena causal

Ejemplos:

- contaminación posterior independiente;
- manipulación intencional;
- desactivación consciente de una alarma;
- introducción fraudulenta de datos;
- almacenamiento contrario a instrucciones claras.

Advertencia técnica documentada

Puede reducir la imputación personal del profesional cuando:

- identificó el riesgo;
- lo comunicó al órgano competente;
- propuso una solución;
- solicitó paralización;
- carecía de autoridad final.

Gobierno y compliance efectivos

Un sistema real de prevención puede:

- demostrar diligencia;
- reducir la probabilidad del daño;
- facilitar una defensa;
- permitir atenuación;
- delimitar responsabilidades individuales.

No basta la existencia formal de un manual.

Reacción inmediata

La retirada rápida, la cooperación, la preservación de evidencias y la corrección pueden reducir el daño y ser valoradas en la graduación de consecuencias, aunque no borren el incumplimiento inicial.

Matriz por casos de uso

Aplicación de IA	Responsable primario de la decisión final	Sujetos adicionales potenciales	Control mínimo exigible
Predicción de vida útil	Operador alimentario	Proveedor, laboratorio, Director Técnico	Validación experimental, margen de seguridad y revisión periódica
Liberación de lotes	Operador	Proveedor, integrador, calidad	Datos completos, bloqueo seguro y aprobación competente
Detección de alérgenos	Operador bajo cuyo nombre se comercializa	Proveedor, materias primas, integrador	Verificación regulatoria y control de cambios
Interpretación microbiológica	Laboratorio y operador en sus respectivos ámbitos	Proveedor analítico	Método validado, incertidumbre y confirmación
Dosificación automática	Operador industrial	Fabricante de maquinaria, integrador	Calibración, límites, alarmas y parada segura
Tratamiento térmico	Operador	Fabricante del equipo, integrador	Validación térmica, sensores redundantes y registros
Visión artificial	Operador	Proveedor e integrador	Sensibilidad por defecto crítico y verificación
Etiquetado generativo	Operador responsable de la información	Proveedor, asesor regulatorio	Revisión humana obligatoria y base normativa controlada
Retirada predictiva	Operador y comité de crisis	Proveedor del sistema	No esperar certeza absoluta ante riesgo grave
Inspección administrativa automatizada	Administración	Proveedor público, órgano supervisor	Legalidad, motivación, auditoría e impugnación
Evaluación de proveedores	Operador	Proveedor de datos	Calidad del dato, ausencia de sesgos y revisión humana
Diseño de formulaciones	Operador que fabrica	Proveedor de IA, Director Técnico	Validación legal, tecnológica, toxicológica y sensorial

Tabla 15. Responsabilidad y controles mínimos por caso de uso.

Decálogo específico para el Director Técnico

1. No firmar lo que no pueda verificar

La firma de una validación, liberación o informe crea una evidencia directa de intervención.

2. Exigir delimitación de funciones

Deben constar por escrito:

- competencias;
- autoridad;
- acceso a información;
- capacidad de bloqueo;
- deberes de escalado.

3. No aceptar responsabilidad sin recursos

La responsabilidad técnica debe acompañarse de:

- presupuesto;
- personal;
- datos;
- acceso a proveedores;
- autoridad para detener.

4. Documentar las discrepancias

Cuando exista desacuerdo técnico relevante, debe dejarse constancia clara y contemporánea.

5. Exigir validación contextual

No aceptar métricas obtenidas únicamente con:

- otras matrices;
- datos de laboratorio;
- condiciones ideales;
- muestras no representativas.

6. Integrar la IA en APPCC

Debe revisarse la modificación del análisis de peligros y de las medidas de control.

7. Controlar versiones

No debe permitirse que una actualización crítica entre en producción sin evaluación.

8. Revisar falsos negativos

En seguridad alimentaria, la métrica decisiva puede no ser la exactitud general, sino la probabilidad de no detectar un peligro.

9. Preservar evidencias

Deben conservarse:

- validaciones;
- comunicaciones;
- decisiones;
- advertencias;
- registros;
- versiones.

10. Escalar el riesgo grave

Cuando la salud pueda estar comprometida, el conflicto comercial o jerárquico no elimina el deber profesional de actuar dentro de las facultades disponibles.

Programa ejecutivo de implantación

Primeros 30 días

Gobierno

- designar responsable de coordinación;
- aprobar una instrucción provisional;
- identificar sistemas críticos;
- prohibir usos no autorizados.

Inventario

- localizar aplicaciones;
- identificar proveedores;
- clasificar finalidad;
- detectar IA en la sombra.

Riesgo inmediato

- revisar liberación de lotes;
- revisar etiquetado;
- revisar vida útil;
- revisar controles de alérgenos.

Evidencia

- impedir borrado de logs;
- identificar versiones;
- asegurar exportación de registros.

Entre 30 y 90 días

Evaluación

- clasificar por criticidad;
- revisar APPCC;
- analizar datos y validación;
- comprobar supervisión humana.

Contratos

- revisar derechos de auditoría;
- exigir notificación de cambios;
- verificar seguros;
- revisar limitaciones de responsabilidad.

Procedimientos

- control de cambios;
- gestión de incidentes;
- preservación forense;
- suspensión y contingencia.

Formación

- Dirección;
- Director Técnico;
- calidad;
- laboratorio;
- producción;
- informática.

Entre 90 y 180 días

Validación

- revalidar sistemas críticos;
- establecer líneas base;
- medir falsos negativos;

- analizar deriva.

Auditoría

- revisar cumplimiento;
- probar recuperación de registros;
- realizar simulacro;
- cerrar acciones correctivas.

Gobierno corporativo

- informar al órgano de administración;
- aprobar indicadores;
- integrar IA en compliance;
- establecer revisión anual.

Estándares técnicos complementarios

El cumplimiento legal no se sustituye mediante normas voluntarias, pero estas pueden proporcionar una estructura útil para demostrar organización y diligencia.

ISO/IEC 42001:2023 establece requisitos para implantar, mantener y mejorar un sistema de gestión de inteligencia artificial. ISO/IEC 23894:2023 proporciona orientación específica sobre gestión del riesgo de IA.

En materia alimentaria, ISO 22000:2018 integra los principios APPCC y los programas de prerrequisitos dentro de un sistema de gestión de la inocuidad. El Codex Alimentarius mantiene los Principios generales de higiene de los alimentos, CXC 1-1969, cuya revisión vigente incorpora el APPCC en el cuerpo central del documento.

La arquitectura más sólida consiste en integrar:

- sistema de gestión de IA;
- sistema de seguridad alimentaria;
- compliance penal;
- ciberseguridad;
- protección de datos;
- gobierno corporativo.

No deben funcionar como compartimentos independientes.

CAPÍTULO 12. CONCLUSIONES

Las conclusiones condensan la regla práctica esencial: la organización no tiene que garantizar que ningún algoritmo falle, pero sí que los fallos previsibles sean detectados, contenidos y documentados antes de causar daño.

Conclusiones generales

1. La IA no es sujeto responsable

La responsabilidad recae sobre personas físicas y jurídicas.

2. El operador alimentario conserva la posición central

La automatización no elimina su deber de garantizar y verificar la seguridad del alimento.

3. La responsabilidad puede ser concurrente

Proveedor, integrador, laboratorio, operador y directivos pueden responder por deberes diferentes.

4. No toda IA alimentaria es de alto riesgo conforme al Reglamento de Inteligencia Artificial

La clasificación requiere aplicar los artículos, anexos y fechas pertinentes.

5. No ser de alto riesgo no significa carecer de relevancia jurídica

Continúan vigentes el Derecho alimentario, civil, contractual, administrativo y penal.

6. La finalidad prevista delimita la responsabilidad

El uso fuera de alcance puede desplazar o redistribuir la imputación.

7. Los datos forman parte del sistema de seguridad

Un modelo correcto con datos incorrectos puede producir una decisión peligrosa.

8. La integración es una fuente autónoma de responsabilidad

Sensores, unidades, ERP e interfaces pueden ser la causa real del fallo.

9. La supervisión humana debe ser efectiva

Una persona sin formación, tiempo o autoridad no constituye una barrera real.

10. El Director Técnico no responde por el mero título

Su responsabilidad depende de funciones, conocimiento, capacidad de intervención y conducta.

11. La firma crea evidencia

La aprobación documental debe reflejar una revisión verdadera.

12. El laboratorio no sustituye el autocontrol del operador

Responde por su prestación; el operador, por el sistema global.

13. La certificación no prueba la seguridad del caso concreto

Debe analizarse su alcance y la correcta integración.

14. El contrato distribuye costes, no obligaciones públicas

No puede eliminar sanciones, derechos de consumidores ni responsabilidad penal.

15. El seguro no sustituye la prevención

Puede cubrir determinados daños, pero no transforma una conducta negligente en diligente.

16. La trazabilidad algorítmica es una obligación estratégica

Lo que no puede reconstruirse difícilmente puede defenderse.

17. La conservación de versiones es esencial

Sin versión, parámetros y datos de entrada no puede reproducirse la decisión.

18. Ante riesgo grave, primero se protege al consumidor

La discusión sobre quién pagará no debe retrasar el bloqueo o la retirada.

19. El fallo algorítmico suele ser organizativo

La mayoría de los incidentes relevantes combinan tecnología, datos, proceso y conducta humana.

20. La mejor defensa jurídica es un sistema que detecta el error antes del daño

La responsabilidad no se gestiona únicamente litigando. Se gestiona mediante diseño, validación, autoridad, supervisión y evidencia.

Conclusión final

La inteligencia artificial no altera el fundamento esencial de la responsabilidad en la industria alimentaria: quien controla una fuente de riesgo debe gestionarla con la diligencia correspondiente a la gravedad de sus consecuencias.

El algoritmo introduce nuevas capas de complejidad, pero no crea un vacío jurídico. Detrás de cada decisión automatizada existen personas y organizaciones que:

- seleccionaron el sistema;

- definieron su finalidad;
- aportaron los datos;
- configuraron los límites;
- aceptaron las métricas;
- autorizaron su utilización;
- revisaron o dejaron de revisar sus resultados;
- decidieron mantenerlo en funcionamiento.

Cuando la IA falla, la atribución correcta no debe buscar al sujeto más visible ni al último que intervino. Debe identificar quién tenía el deber y la posibilidad real de evitar el resultado. El fabricante del sistema responderá por los defectos que se encuentren bajo su control. El integrador, por los errores de conexión o configuración. El laboratorio, por la calidad de su actividad analítica. El Director Técnico, cuando sus funciones, conocimiento y capacidad de intervención permitan una imputación personal. El órgano de administración, cuando el fallo revele una deficiencia estructural de gobierno. La Administración, por sus propios actos automatizados cuando concurran los presupuestos legales.

Pero el operador alimentario seguirá ocupando la posición central frente al producto que introduce en el mercado. No porque deba soportar siempre y en exclusiva todo el daño, sino porque es quien organiza el proceso, controla la comercialización y se encuentra en la posición más inmediata para impedir que un alimento inseguro llegue al consumidor.

La formulación jurídica definitiva puede expresarse así:

La decisión puede estar automatizada; la responsabilidad, no.

Y su consecuencia empresarial es igualmente clara:

Ninguna empresa debería permitir que un algoritmo controle una decisión alimentaria crítica si no puede determinar previamente quién lo valida, quién lo supervisa, quién puede detenerlo y quién deberá explicar su actuación cuando falle.

ANEXOS OPERATIVOS

Los anexos convierten las conclusiones del estudio en documentos de trabajo. Deben adaptarse al tamaño de la empresa, al tipo de producto, al sistema de calidad existente y a la clasificación jurídica y técnica de cada herramienta.

Anexo A. Ficha de inventario algorítmico

Campo	Contenido
Identificación	Nombre comercial e identificador interno
Proveedor	Fabricante, distribuidor e integrador
Titular interno	Departamento responsable
Finalidad	Decisión o proceso en el que interviene
Producto afectado	Matrices, líneas y categorías
Tipo de resultado	Predicción, clasificación, recomendación o actuación
Nivel de automatización	Informativo, asistido, semiautomático o automático
Consecuencia del error	Calidad, legalidad, seguridad, salud o continuidad
Datos utilizados	Fuente, periodicidad y responsable
Validación	Fecha, alcance, responsable y resultado
Supervisión	Persona o función asignada

Campo	Contenido
Versión	Software, modelo y configuración
Proveedor externo	Acceso, soporte, mantenimiento y subcontratistas
Evidencias	Logs, informes, instrucciones y auditorías
Estado	Piloto, validado, activo, suspendido o retirado

Anexo A.1. Campos mínimos del inventario algorítmico.

Anexo B. Lista de comprobación previa a la puesta en servicio

- ☐ Finalidad prevista definida y documentada.
- ☐ Clasificación jurídica conforme al Reglamento de IA y clasificación interna de criticidad.
- ☐ Validación con datos y condiciones representativas del producto, proceso y población objetivo.
- ☐ Tasas de falsos positivos y falsos negativos conocidas para el peligro crítico.
- ☐ Supervisión humana asignada a personas con competencia, tiempo y autoridad.
- ☐ Control de versiones, cambios y actualizaciones.
- ☐ Registros exportables, íntegros y vinculables a lote o expediente.
- ☐ Integración en APPCC y revisión de medidas de control.
- ☐ Procedimiento manual alternativo y modo de fallo seguro.
- ☐ Contrato con derechos de auditoría, notificación y preservación de evidencias.
- ☐ Coberturas de seguro revisadas y actividad declarada.
- ☐ Protocolo de incidentes, retirada y comunicación ensayado.

Anexo C. Contenido mínimo del expediente de una decisión crítica

139. Identificación del producto, lote, muestra, línea o expediente.
140. Finalidad de la decisión.
141. Sistema, proveedor, versión y configuración.
142. Datos de entrada y controles de calidad del dato.
143. Resultado, nivel de confianza, umbral y advertencias.
144. Revisión humana y persona competente.
145. Decisión final y justificación de cualquier anulación.
146. Documentos de soporte, análisis y calibraciones.
147. Fecha, hora, integridad y cadena de custodia.
148. Incidencias posteriores, acciones correctivas y comunicaciones.

Anexo D. Glosario técnico-jurídico

Término	Definición
Alucinación	Generación de contenido no sustentado por los datos, las fuentes o la realidad verificable.
Automatización	Ejecución de una tarea o decisión con intervención humana reducida o inexistente.
Deriva del modelo	Cambio del rendimiento por alteraciones en los datos, el entorno o la relación entre variables y resultado.
Explicabilidad	Capacidad de ofrecer información comprensible sobre finalidad, funcionamiento, límites o resultado del sistema.
Falso negativo	Caso peligroso o no conforme que el sistema clasifica erróneamente como seguro o conforme.
Falso positivo	Caso seguro o conforme que el sistema clasifica erróneamente como peligroso o no conforme.
Finalidad prevista	Uso para el que el proveedor diseñó el sistema y respecto del cual comunica capacidades y límites.
Integrador	Entidad que conecta el modelo con datos, sensores, procesos, interfaces o maquinaria.

Término	Definición
Log	Registro automático que documenta eventos, datos, usuarios, versiones y acciones.
Modificación sustancial	Cambio que puede afectar a la conformidad, la finalidad o el rendimiento de un sistema.
Responsable del despliegue	Persona física o jurídica que utiliza un sistema de IA bajo su autoridad, salvo uso personal no profesional.
Supervisión humana	Conjunto de medios y competencias que permiten comprender, cuestionar, anular o detener el sistema.
Trazabilidad algorítmica	Capacidad de reconstruir de forma verificable cómo se produjo y ejecutó una decisión.
Validación	Demostración de que el sistema puede cumplir la finalidad prevista en condiciones definidas.
Verificación	Comprobación periódica de que el sistema continúa funcionando como estaba previsto.

Anexo D.1. Glosario esencial.

BIBLIOGRAFÍA Y FUENTES

Las referencias se presentan en formato editorial próximo a APA 7. En las normas jurídicas se mantiene la denominación oficial y el identificador institucional.

Normativa de la Unión Europea

Parlamento Europeo y Consejo de la Unión Europea. (2002). Reglamento (CE) n.º 178/2002, de 28 de enero de 2002, por el que se establecen los principios y requisitos generales de la legislación alimentaria, se crea la Autoridad Europea de Seguridad Alimentaria y se fijan procedimientos relativos a la seguridad alimentaria. Fuente oficial / DOI

Parlamento Europeo y Consejo de la Unión Europea. (2004). Reglamento (CE) n.º 852/2004, de 29 de abril de 2004, relativo a la higiene de los productos alimenticios. Fuente oficial / DOI

Parlamento Europeo y Consejo de la Unión Europea. (2011). Reglamento (UE) n.º 1169/2011, de 25 de octubre de 2011, sobre la información alimentaria facilitada al consumidor. Fuente oficial / DOI

Parlamento Europeo y Consejo de la Unión Europea. (2016). Reglamento (UE) 2016/679, de 27 de abril de 2016, Reglamento General de Protección de Datos. Fuente oficial / DOI

Parlamento Europeo y Consejo de la Unión Europea. (2017). Reglamento (UE) 2017/625, de 15 de marzo de 2017, relativo a los controles oficiales. Fuente oficial / DOI

Parlamento Europeo y Consejo de la Unión Europea. (2024). Reglamento (UE) 2024/1689, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial. Fuente oficial / DOI

Parlamento Europeo y Consejo de la Unión Europea. (2026). Reglamento (UE) 2026/1744, de 8 de julio de 2026, que modifica el Reglamento (UE) 2024/1689 en relación con la simplificación de su aplicación. Fuente oficial / DOI

Parlamento Europeo y Consejo de la Unión Europea. (2024). Directiva (UE) 2024/2853, de 23 de octubre de 2024, sobre responsabilidad por los daños causados por productos defectuosos. Fuente oficial / DOI

Unión Europea. (2026). Corrección de errores de la Directiva (UE) 2024/2853. Diario Oficial de la Unión Europea, 7 de mayo de 2026. Fuente oficial / DOI

Parlamento Europeo y Consejo de la Unión Europea. (2008). Reglamento (CE) n.º 593/2008 sobre la ley aplicable a las obligaciones contractuales (Roma I). Fuente oficial / DOI

Parlamento Europeo y Consejo de la Unión Europea. (2007). Reglamento (CE) n.º 864/2007 sobre la ley aplicable a las obligaciones extracontractuales (Roma II). Fuente oficial / DOI

Parlamento Europeo y Consejo de la Unión Europea. (2012). Reglamento (UE) n.º 1215/2012 relativo a la competencia judicial, reconocimiento y ejecución de resoluciones (Bruselas I bis). Fuente oficial / DOI

Normativa española

España. (1889). Código Civil. Fuente oficial / DOI

España. (1980). Ley 50/1980, de 8 de octubre, de Contrato de Seguro. Fuente oficial / DOI

España. (1995). Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. Fuente oficial / DOI

España. (1995). Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales. Fuente oficial / DOI

España. (2000). Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil. Fuente oficial / DOI

España. (2007). Real Decreto Legislativo 1/2007, de 16 de noviembre, texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios. Fuente oficial / DOI

España. (2010). Real Decreto Legislativo 1/2010, de 2 de julio, texto refundido de la Ley de Sociedades de Capital. Fuente oficial / DOI

España. (2011). Ley 17/2011, de 5 de julio, de seguridad alimentaria y nutrición. Fuente oficial / DOI

España. (2015). Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. Fuente oficial / DOI

España. (2015). Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público. Fuente oficial / DOI

España. (2019). Ley 1/2019, de 20 de febrero, de Secretos Empresariales. Fuente oficial / DOI

España. (2023). Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas. Fuente oficial / DOI

Jurisprudencia

Tribunal de Justicia de la Unión Europea. (2006). Sentencia de 23 de noviembre de 2006, Lidl Italia, C-315/05, ECLI:EU:C:2006:736. Fuente oficial / DOI

Tribunal de Justicia de la Unión Europea. (2015). Sentencia de 5 de marzo de 2015, Boston Scientific Medizintechnik, asuntos acumulados C-503/13 y C-504/13, ECLI:EU:C:2015:148. Fuente oficial / DOI

Tribunal de Justicia de la Unión Europea. (2017). Sentencia de 21 de junio de 2017, W y otros, C-621/15, ECLI:EU:C:2017:484. Fuente oficial / DOI

Tribunal Constitucional. (1990). Sentencia 76/1990, de 26 de abril. Fuente oficial / DOI

Normas, guías y literatura técnica

Codex Alimentarius Commission. (2022). General principles of food hygiene: CXC 1-1969. FAO/WHO. Fuente oficial / DOI

International Organization for Standardization. (2017). ISO/IEC 17025:2017. General requirements for the competence of testing and calibration laboratories. Fuente oficial / DOI

International Organization for Standardization. (2018). ISO 22000:2018. Food safety management systems. Fuente oficial / DOI

International Organization for Standardization. (2019). ISO 20976-1:2019. Microbiology of the food chain — Requirements and guidelines for conducting challenge tests. Fuente oficial / DOI

International Organization for Standardization. (2023). ISO/IEC 23894:2023. Artificial intelligence — Guidance on risk management. Fuente oficial / DOI

International Organization for Standardization. (2023). ISO/IEC 42001:2023. Artificial intelligence — Management system. Fuente oficial / DOI

National Institute of Standards and Technology. (2023). Artificial Intelligence Risk Management Framework (AI RMF 1.0). Fuente oficial / DOI

Amershi, S., Begel, A., Bird, C., et al. (2019). Software engineering for machine learning: A case study. Proceedings of the 41st International Conference on Software Engineering: Software Engineering in Practice, 291-300. Fuente oficial / DOI

Gebru, T., Morgenstern, J., Vecchione, B., et al. (2021). Datasheets for datasets. Communications of the ACM, 64(12), 86-92. Fuente oficial / DOI

Mitchell, M., Wu, S., Zaldivar, A., et al. (2019). Model cards for model reporting. Proceedings of the Conference on Fairness, Accountability, and Transparency, 220-229. Fuente oficial / DOI

Parasuraman, R., & Riley, V. (1997). Humans and automation: Use, misuse, disuse, abuse. Human Factors, 39(2), 230-253. Fuente oficial / DOI

Ribeiro, M. T., Singh, S., & Guestrin, C. (2016). "Why should I trust you?" Explaining the predictions of any classifier. Proceedings of KDD 2016, 1135-1144. Fuente oficial / DOI

Sculley, D., Holt, G., Golovin, D., et al. (2015). Hidden technical debt in machine learning systems. Advances in Neural Information Processing Systems, 28. Fuente oficial / DOI

Servicio de publicaciones de INTABIOTECH

Botiguers, 3, 2ª P, 46980, Paterna, Valencia, España

Parque Empresarial Táctica

www.intabiotech.com

Serie: Inteligencia artificial en la industria alimentaria · Publicación n.º 7

La incorporación de sistemas de inteligencia artificial a la industria alimentaria no crea una zona de irresponsabilidad jurídica. Cuando un algoritmo participa en la liberación de un lote, en la estimación de una vida útil, en el etiquetado de alérgenos, en la interpretación de un resultado analítico o en la retirada de un producto, la pregunta decisiva no es qué decidió la máquina, sino quién controlaba el riesgo y tenía el deber de evitar el daño.

TEMAS CLAVE

- Operador alimentario y posición de garante
- Proveedor tecnológico, integrador y laboratorio
- Director Técnico, administradores y persona jurídica
- Responsabilidad civil, contractual, administrativa y penal
- Prueba, trazabilidad algorítmica y gestión de incidentes
- Contratación, seguros y dimensión transfronteriza

> “La decisión puede estar automatizada; la responsabilidad, no.”