

Los 10 errores más frecuentes al implantar IA en la industria alimentaria

Technical White Paper

José Manuel López / INTABIOTECH
DEPARTAMENTO TÉCNICO

INTABIOTECH

TECHNICAL WHITE PAPER

LOS 10 ERRORES MÁS FRECUENTES AL IMPLANTAR INTELIGENCIA ARTIFICIAL EN LA INDUSTRIA ALIMENTARIA

Por qué numerosos proyectos fracasan antes de llegar a producción y cómo construir una implantación técnicamente válida, regulatoriamente defendible y económicamente útil

José Manuel López, BSc, MD, PhD
Director Técnico — INTABIOTECH

Julio de 2026

Créditos y advertencia editorial

Este documento tiene finalidad técnica, científica y divulgativa. No sustituye una evaluación jurídica, regulatoria, de seguridad alimentaria, ciberseguridad o validación tecnológica adaptada al caso concreto. Las referencias normativas deben verificarse en su versión consolidada y vigente antes de adoptar decisiones empresariales.

La denominación MIA-FOOD 1.0* se utiliza en este manuscrito como nombre de trabajo de un modelo de autoevaluación de madurez. Forma parte de un proceso registrado como Propiedad Intelectual/Industrial de INTABIOTECH SL.

Índice

Créditos y advertencia editorial	2
Introducción	7
Error N.º 1. Empezar por la herramienta y no por el problema industrial.....	9
La pregunta que debe preceder al proyecto	9
La IA no crea necesidades industriales	9
El caso particular de la industria alimentaria	10
Un ejemplo habitual	10
Indicadores de éxito	10
Recomendaciones prácticas	10
Conclusión	11
Error N.º 2. Trabajar con datos abundantes, pero inadecuados, fragmentados o sin contexto tecnológico	12
El mito del Big Data.....	12
El contexto tecnológico es parte del dato	12
Datos correctos, pero científicamente inútiles.....	13
Fragmentación de la información	13
Deriva de los datos	13
Sesgos históricos	13
Trazabilidad de los datos	13
Recomendaciones prácticas	13
Conclusión	14
Error N.º 3. Confundir una prueba de concepto con un sistema validado para producción alimentaria	15
Del laboratorio a la fábrica	15
Validar no es únicamente medir precisión	15
Utilidad y fiabilidad	16
Validación continua.....	16
Visión artificial	16
Límites de utilización	16
Evidencia documental	16
Recomendaciones prácticas	16
Conclusión	17
Error N.º 4. Delegar decisiones críticas en la IA sin una supervisión humana efectiva.....	18

La falsa percepción de objetividad	18
Qué significa supervisión humana.....	18
Niveles de criticidad	19
La ilusión del piloto automático	19
La responsabilidad no se delega	19
Diseñar la supervisión	19
El valor de la discrepancia	19
Formación y cultura.....	19
Recomendaciones prácticas	19
Conclusión	20
Error N.º 5. Ignorar el marco regulatorio aplicable al caso de uso	21
Pensar que la IA es solo software	21
Superposición normativa	21
Enfoque basado en riesgo.....	21
Responsabilidad del operador alimentario	22
IA, APPCC y sistemas de gestión	22
Protección de datos y confidencialidad	22
Documentación y gobernanza.....	22
Recomendaciones prácticas	22
Conclusión	22
Error N.º 6. No integrar la IA en APPCC, calidad, trazabilidad y gestión del cambio.....	23
La IA como elemento del sistema.....	23
APPCC e IA.....	23
Validación y verificación	23
Trazabilidad de la decisión.....	23
Gestión del cambio	24
Competencias profesionales	24
Auditorías	24
Integración con normas certificables	24
Recomendaciones prácticas	24
Conclusión	24
Error N.º 7. Utilizar modelos opacos sin controlar explicabilidad, incertidumbre y deriva	25
La caja negra	25
Explicabilidad y transparencia	25

Incertidumbre	25
Falsa seguridad de los porcentajes	25
Detección fuera de distribución	25
Deriva del modelo	25
Explicabilidad y auditoría	25
IA explicable.....	26
Recomendaciones prácticas	26
Conclusión	26
Error N.º 8. Subestimar la ciberseguridad, la confidencialidad y la dependencia del proveedor	27
Los datos tienen valor.....	27
Plataformas externas.....	27
Protección del conocimiento industrial	27
Ataques específicos	27
Dependencia del proveedor	28
Actualizaciones no controladas	28
Convergencia IT/OT	28
Continuidad de negocio.....	28
Política corporativa	28
Recomendaciones prácticas	28
Conclusión	28
Error N.º 9. Pretender sustituir el conocimiento experto en lugar de estructurarlo y ampliarlo	29
Conocimiento explícito y tácito	29
La IA aprende correlaciones; el experto interpreta causalidad	29
Riesgo de <i>deskilling</i>	29
Patrimonio intelectual	29
Inteligencia aumentada	30
Captura de conocimiento	30
Modelos híbridos.....	30
Formación bidireccional	30
Recomendaciones prácticas	30
Conclusión	30
Error N.º 10. Medir el éxito por la novedad tecnológica y no por el valor industrial demostrado	31
Innovación tecnológica e innovación empresarial	31
Del entusiasmo al retorno industrial.....	31

ROI integral	31
<i>AI washing</i>	31
Integración estratégica	31
Indicadores relevantes	32
Ciclo de vida completo	32
El verdadero indicador	32
Recomendaciones prácticas	32
Conclusión	32
Conclusiones	33
Decálogo ejecutivo para implantar IA en la industria alimentaria.....	35
Anexo I. Modelo MIA-FOOD 1.0.....	36
A. Estrategia y gobernanza	36
B. Datos	36
C. Validación técnica.....	36
D. Seguridad alimentaria y calidad	37
E. Cumplimiento normativo	37
F. Ciberseguridad	37
G. Personas y cultura.....	37
Interpretación	38
Bibliografía técnica, científica y jurídica utilizada.....	39
Legislación de la Unión Europea.....	39
Normas y marcos técnicos	39
Estándares de seguridad alimentaria	39
Obras generales	39
Revistas recomendadas	39
Otras Referencias Bibliográficas.....	40
I. Legislación y normativa (11 referencias)	40
II. Documentos institucionales (8 referencias)	40
III. Obras fundamentales sobre IA (7 referencias)	41
IV. Inteligencia artificial aplicada a la industria alimentaria (12 referencias)	41
V. Gobernanza, derecho y ética de la IA (7 referencias).....	42

Introducción

Tabla 1. Aplicaciones representativas de IA y riesgo principal asociado.

Área	Aplicaciones habituales	Riesgo dominante
I+D y formulación	Diseño experimental, optimización de recetas, búsqueda técnica	Uso de información incompleta o no validada
Producción	Control de proceso, predicción de desviaciones, optimización energética	Automatización fuera del dominio de validez
Calidad y seguridad	Visión artificial, predicción microbiológica, priorización de controles	Falsos negativos y pérdida de trazabilidad
Mantenimiento	Predicción de fallos, planificación de intervenciones	Dependencia de sensores y datos históricos
Regulación y documentación	Vigilancia normativa, borradores, clasificación documental	Alucinaciones, desactualización y confidencialidad

La inteligencia artificial ha dejado de ser una tecnología periférica para convertirse en uno de los principales vectores de transformación de la industria alimentaria. Su campo potencial de aplicación abarca prácticamente toda la cadena de valor: selección y homologación de materias primas, formulación de alimentos, optimización de procesos, mantenimiento predictivo, inspección visual, control microbiológico, predicción de vida útil, gestión energética, trazabilidad, detección de fraude, planificación de la demanda, desarrollo de nuevos productos, revisión documental y vigilancia regulatoria.

No estamos ante una tecnología meramente experimental, sino ante una infraestructura cognitiva que comienza a integrarse en la gestión pública y privada de la cadena alimentaria. Sin embargo, la existencia de aplicaciones técnicamente prometedoras no significa que su implantación industrial sea sencilla. Una demostración ejecutada sobre un conjunto limitado de datos, una herramienta generativa capaz de producir un informe convincente o un modelo que alcanza una elevada precisión en condiciones de laboratorio no constituyen, por sí solos, un sistema apto para intervenir en decisiones relacionadas con alimentos, procesos, personas o consumidores.

La industria alimentaria presenta unas condiciones que hacen especialmente exigente cualquier proyecto de inteligencia artificial. Trabaja con materias primas biológicamente variables; procesos sometidos a desviaciones inevitables; productos cuya seguridad depende de interacciones entre tiempo, temperatura, pH, actividad de agua, composición, carga microbiana, envase y condiciones logísticas; instalaciones en las que conviven equipos de distintas generaciones; y cadenas de suministro que pueden extenderse por múltiples países y operadores.

A ello se añade una fuerte densidad normativa. Una solución de IA puede quedar simultáneamente afectada por el Reglamento europeo de inteligencia artificial, la legislación general alimentaria, las normas de higiene, los requisitos de trazabilidad, el régimen de responsabilidad por productos, la protección de datos personales, la propiedad intelectual, la normativa laboral, la ciberseguridad y las obligaciones contractuales asumidas frente a clientes y proveedores.

Una parte significativa de las empresas está adoptando IA mediante decisiones dispersas: un departamento contrata una plataforma generativa; mantenimiento incorpora un sistema predictivo; calidad prueba un modelo de visión artificial; I+D utiliza herramientas externas para formular productos; recursos humanos comienza a filtrar candidatos; y marketing automatiza contenidos. Cada iniciativa puede parecer limitada, pero su acumulación crea un ecosistema tecnológico que rara vez ha sido inventariado, clasificado o sometido a una gobernanza común.

El resultado es una paradoja. Las organizaciones pueden estar utilizando inteligencia artificial intensivamente y, al mismo tiempo, carecer de una verdadera estrategia de IA. Poseen herramientas, licencias y experimentos, pero no necesariamente una arquitectura de datos, un sistema de responsabilidades, criterios de validación, controles de uso, indicadores de desempeño ni una visión clara de qué decisiones pueden automatizarse y cuáles deben permanecer bajo control humano.

Los errores más graves tampoco suelen aparecer en la fase de presentación. Surgen cuando el sistema se enfrenta a materias primas distintas de las utilizadas en su entrenamiento, cuando cambia una formulación, cuando un sensor pierde calibración, cuando se introduce una nueva línea, cuando el proveedor actualiza el modelo, cuando se produce una alerta sanitaria o cuando la empresa necesita explicar retrospectivamente por qué adoptó una determinada decisión.

En ese momento, una herramienta que parecía eficiente puede revelar problemas estructurales: datos sin trazabilidad suficiente; variables críticas omitidas; correlaciones interpretadas como causalidad; modelos que no distinguen entre incertidumbre y ausencia de riesgo; resultados imposibles de reproducir; decisiones no documentadas; dependencia excesiva de un proveedor externo; ausencia de responsables identificados; integración deficiente con los sistemas de calidad; o falta de evidencia que permita defender la actuación ante un cliente, auditor, autoridad o tribunal.

Implantar inteligencia artificial no consiste en adquirir un programa ni en conectar un modelo a una base de datos. Consiste en introducir un nuevo componente decisonal dentro de un sistema sociotécnico regulado. Ese componente debe convivir con operadores, tecnólogos, responsables de calidad, personal de mantenimiento, laboratorios, proveedores, clientes, sistemas de gestión y autoridades competentes.

La pregunta correcta no es únicamente si la IA puede realizar una tarea. Hay que determinar qué decisión pretende mejorar; qué datos utiliza y qué representan; bajo qué condiciones mantiene su validez; qué consecuencias tendría un error; quién supervisa el resultado; quién puede modificar el sistema; qué evidencia queda registrada; y cómo se integra todo ello en los procedimientos ordinarios de la empresa.

Desde esta perspectiva, los diez errores analizados no son fallos aislados. Constituyen manifestaciones de una misma deficiencia: abordar la inteligencia artificial como una adquisición tecnológica y no como una transformación del sistema industrial, organizativo y regulatorio.

La ventaja competitiva no pertenecerá necesariamente a la empresa que adopte más herramientas de inteligencia artificial. Pertenecerá a aquella que sea capaz de integrarlas con mayor criterio, gobernarlas con mayor rigor y convertir sus resultados en decisiones industriales reproducibles, auditables y económicamente justificadas.

Error N.º 1. Empezar por la herramienta y no por el problema industrial

IDEA CLAVE: La tecnología debe seleccionarse después de cuantificar el problema, no antes.

De la necesidad industrial al valor demostrado

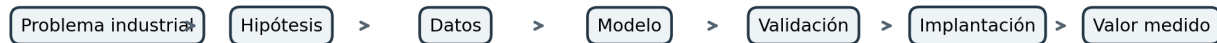


Figura 1. Secuencia correcta para convertir una necesidad industrial en valor medible.

Existe una constante que se repite en una parte significativa de los proyectos de inteligencia artificial desarrollados en la industria alimentaria: la organización decide implantar IA antes de haber definido con precisión qué problema pretende resolver. La decisión tecnológica precede al análisis industrial. En lugar de identificar un proceso susceptible de mejora y evaluar posteriormente si la inteligencia artificial constituye la solución más adecuada, el razonamiento se invierte. Se adquiere una plataforma, se contrata un servicio o se incorpora un modelo generativo y, únicamente después, se intenta encontrar una aplicación que justifique la inversión.

La adopción de una tecnología no genera valor por sí misma. Una organización no es más eficiente por utilizar inteligencia artificial; únicamente lo será si esa tecnología mejora de manera objetiva un proceso previamente identificado, medible y económicamente relevante.

La pregunta que debe preceder al proyecto

Desde el punto de vista de la ingeniería industrial, cualquier proyecto debería comenzar respondiendo a una pregunta sencilla: ¿qué problema concreto estamos intentando resolver?

Expresiones como «queremos incorporar inteligencia artificial», «necesitamos digitalizarnos», «queremos utilizar un modelo generativo» o «nuestros competidores ya trabajan con IA» no describen problemas industriales. Son declaraciones de intención tecnológica.

Un proyecto correctamente planteado debería formular objetivos como reducir falsas alarmas microbiológicas; disminuir mermas durante el envasado; mejorar la predicción de vida útil; detectar desviaciones de color antes del rechazo del lote; optimizar el consumo energético de una línea UHT; anticipar averías críticas; o reducir el tiempo necesario para revisar documentación regulatoria.

La IA no crea necesidades industriales

La inteligencia artificial no constituye un objetivo empresarial. Es una herramienta de apoyo a la decisión. Del mismo modo que una empresa no compra un cromatógrafo simplemente porque sea una tecnología avanzada, tampoco debería implantar IA sin determinar qué hipótesis pretende validar, qué variable desea optimizar o qué decisión necesita mejorar.

La secuencia lógica debería ser: problema, hipótesis, datos, modelo, validación, implantación y seguimiento. Muchas organizaciones siguen la secuencia inversa: modelo, licencia, formación, búsqueda de aplicaciones, frustración y abandono.

El caso particular de la industria alimentaria

La industria alimentaria trabaja con sistemas biológicos variables. Dos lotes de una misma materia prima nunca son completamente idénticos. Las variaciones pueden deberse a origen geográfico, campaña agrícola, genética, alimentación animal, climatología, almacenamiento, transporte, humedad, actividad de agua, composición mineral o carga microbiológica inicial.

Cuando una empresa afirma que desea implantar IA, debería preguntarse qué parte de esta variabilidad pretende comprender mejor. No todos los problemas requieren aprendizaje automático. En muchas ocasiones, una mejora del APPCC, una recalibración de sensores, una reorganización del flujo documental o una optimización estadística convencional producen beneficios superiores con una inversión menor.

Un ejemplo habitual

Una empresa de platos preparados refrigerados observa variabilidad excesiva en la vida útil y concluye que necesita un modelo predictivo. Antes de entrenar un algoritmo debe comprobar si existe homogeneidad entre líneas, si se registran temperaturas reales durante el enfriamiento, si las mediciones microbiológicas siguen protocolos uniformes, si hay datos históricos suficientes, si las materias primas mantienen especificaciones constantes y si se conocen las causas de las desviaciones.

Si estas cuestiones permanecen sin respuesta, la IA aprenderá a reproducir el desorden existente. Un modelo sofisticado no corrige datos deficientes; únicamente produce errores más sofisticados.

Indicadores de éxito

Tabla 2. Indicadores mínimos para evaluar el valor industrial de un proyecto.

Dimensión	Indicador recomendado	Criterio de éxito
Producción	Merma, OEE, tiempo de parada	Mejora frente a línea base y estabilidad en el tiempo
Calidad	No conformidades, repetición de análisis	Reducción sin deterioro de sensibilidad
Seguridad alimentaria	Alertas útiles, falsos negativos, tiempo de respuesta	Riesgo controlado y evidencia trazable
I+D	Tiempo hasta prototipo, ensayos evitados	Aceleración sin pérdida de rigor experimental
Economía	Ahorro neto, payback, coste total de propiedad	Retorno positivo incluyendo mantenimiento

Todo proyecto debería incorporar indicadores definidos de antemano: reducción de mermas, incremento del OEE, disminución de reclamaciones, reducción de tiempo de formulación, ahorro energético por tonelada, reducción de tiempos de parada, incremento de precisión predictiva o disminución de desperdicio.

Sin indicadores resulta imposible calcular el retorno de la inversión, comparar soluciones o justificar ampliaciones.

Recomendaciones prácticas

1. Definir con precisión el problema industrial.

2. Cuantificar su magnitud económica.
3. Identificar las consecuencias técnicas de no actuar.
4. Determinar las variables que intervienen.
5. Evaluar calidad y disponibilidad de datos.
6. Analizar el riesgo asociado a una decisión incorrecta.
7. Fijar indicadores de éxito.
8. Designar responsable del proyecto.
9. Designar responsable de validación técnica.
10. Establecer criterios de continuidad, modificación o cancelación.

Conclusión

La primera decisión de un proyecto de IA nunca debería consistir en elegir un algoritmo, plataforma o proveedor. Debe consistir en comprender con exactitud el problema industrial. Cuando este paso se omite, la organización convierte la IA en una solución en busca de un problema. Cuando el análisis previo es riguroso, la IA deja de ser marketing tecnológico y se convierte en una herramienta de apoyo a la decisión.

Error N.º 2. Trabajar con datos abundantes, pero inadecuados, fragmentados o sin contexto tecnológico

RIESGO: Un gran volumen de datos no compensa la falta de contexto tecnológico, trazabilidad o calidad metrológica.

Cadena de gobernanza del dato



Figura 2. Cadena mínima de gobernanza del dato en aplicaciones alimentarias.

La calidad de un sistema de inteligencia artificial nunca será superior a la calidad de los datos con los que ha sido construido. Aunque parezca elemental, sigue siendo una de las causas más frecuentes de fracaso en proyectos de IA dentro de la industria alimentaria.

Muchas empresas consideran que poseen una gran cantidad de información porque llevan años registrando datos en ERP, LIMS, SCADA, MES, hojas de cálculo, sistemas de mantenimiento, laboratorios externos o registros APPCC. Sin embargo, acumular datos no equivale a disponer de información útil, del mismo modo que almacenar miles de documentos no implica disponer de conocimiento.

El mito del Big Data

El volumen de datos no es el principal requisito para desarrollar modelos robustos. Un modelo entrenado con millones de registros inconsistentes suele comportarse peor que otro construido sobre un conjunto reducido, pero cuidadosamente validado.

En alimentación, una misma variable puede aparecer registrada como temperatura objetivo, máxima, media, de consigna, del núcleo, superficial, medida por PLC o anotada manualmente. Desde el punto de vista del algoritmo pueden parecer equivalentes. Desde el punto de vista tecnológico, no lo son.

El contexto tecnológico es parte del dato

Un valor aislado, por ejemplo pH 5,25, informa poco si no se conoce el tipo de alimento, formulación, momento del proceso, temperatura de medición, método analítico, incertidumbre, lote, operador, equipo, fecha y condiciones de conservación.

La inteligencia artificial necesita el mismo contexto que un tecnólogo experimentado. Eliminarlo convierte los datos en números sin significado industrial.

Datos correctos, pero científicamente inútiles

Un sistema de visión artificial puede disponer de cientos de miles de imágenes y, aun así, ser científicamente débil si la iluminación cambia entre turnos, las cámaras se sustituyen, los criterios de aceptación evolucionan o diferentes inspectores etiquetan con criterios distintos. El algoritmo aprenderá defectos, pero también diferencias de iluminación, posición, exposición y hábitos de clasificación.

Fragmentación de la información

Predecir la vida útil de un alimento refrigerado puede requerir información del ERP, MES, SCADA, laboratorio microbiológico, laboratorio fisicoquímico, APPCC, mantenimiento, cámaras, transporte, reclamaciones y estudios históricos. En muchas empresas estos sistemas nunca fueron diseñados para comunicarse. El modelo recibe una parte de la realidad e intenta resolver un problema complejo con información incompleta.

Deriva de los datos

Los datos cambian por nuevos proveedores, campañas, formulaciones, ingredientes, líneas, sensores, condiciones climáticas o hábitos de consumo. El modelo sigue funcionando, pero sobre una realidad distinta de aquella para la que fue entrenado. Un sistema de IA debe entenderse como un sistema vivo que requiere supervisión, recalibración y revalidación.

Sesgos históricos

La IA reproduce los sesgos presentes en los datos. Si una empresa ha rechazado lotes aplicando criterios inconsistentes, el algoritmo aprenderá esos criterios. Si determinados parámetros nunca se midieron, el modelo tampoco podrá utilizarlos.

Debe distinguirse entre datos observados, medidos, estimados, inferidos, corregidos, imputados y faltantes.

Trazabilidad de los datos

La empresa debe poder responder de dónde procede el dato, quién lo registró, cómo se obtuvo, con qué instrumento, cuál era su incertidumbre, si fue modificado, si forma parte del entrenamiento y si puede reproducirse el resultado.

Recomendaciones prácticas

11. Inventario de fuentes de datos.
12. Definición normalizada de variables.
13. Eliminación de duplicidades.
14. Identificación de datos faltantes.
15. Evaluación de sesgos históricos.
16. Homogeneización de unidades y formatos.
17. Verificación metrológica de sensores e instrumentos.
18. Documentación del contexto tecnológico.
19. Procedimientos de actualización y recalibración.
20. Monitorización permanente de deriva y rendimiento.

Conclusión

La IA no transforma datos deficientes en conocimiento fiable. Amplifica las fortalezas y debilidades de la información con la que fue entrenada. La gobernanza del dato deja de ser una cuestión informática y se convierte en un elemento esencial de la gestión tecnológica.

Error N.º 3. Confundir una prueba de concepto con un sistema validado para producción alimentaria

RECOMENDACIÓN: Toda prueba de concepto debe tener criterios de salida, validación externa y plan de revalidación.

Ciclo de vida de un sistema de IA industrial

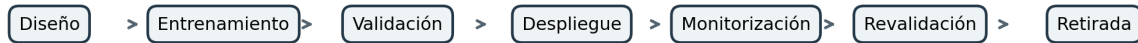


Figura 3. Ciclo de vida y control continuo de un sistema de IA industrial.

Uno de los errores más costosos consiste en asumir que un modelo que funciona durante una demostración o prueba piloto está preparado para operar en un entorno industrial real. Esta confusión entre viabilidad técnica y validación operacional explica numerosos proyectos que generan entusiasmo inicial y terminan abandonados.

Una prueba de concepto demuestra que una idea es técnicamente posible. No acredita robustez, escalabilidad, reproducibilidad ni aptitud para soportar condiciones cambiantes de planta.

Del laboratorio a la fábrica

Durante una prueba de concepto se trabaja con datos seleccionados, sensores calibrados, operarios experimentados y supervisión continua. En producción aparecen nuevos proveedores, variaciones estacionales, cambios de formulación, velocidades distintas, sustituciones de sensores, rotación de personal, incidencias logísticas y cambios de envase.

Una precisión del 98 % en entorno controlado puede reducirse significativamente en funcionamiento continuo.

Validar no es únicamente medir precisión

Tabla 3. Métricas estadísticas y su interpretación industrial.

Métrica	Qué mide	Limitación industrial
Exactitud	Proporción total de aciertos	Puede ocultar clases minoritarias críticas
Sensibilidad	Detección de positivos reales	Debe priorizarse cuando el falso negativo es grave
Especificidad	Detección de negativos reales	Un valor bajo genera rechazo o intervención innecesaria
F1-score	Equilibrio entre precisión y sensibilidad	No incorpora por sí solo el coste de cada error
Calibración	Correspondencia entre confianza y frecuencia real	Esencial para interpretar probabilidades

Exactitud, sensibilidad, especificidad, precisión y F1 son necesarias, pero insuficientes. La validación industrial debe comprobar si el modelo mantiene el rendimiento entre campañas, cómo responde a materias primas fuera de rango, datos incompletos, fallos de comunicación, situaciones fuera de dominio y niveles altos de incertidumbre.

No basta demostrar que acierta. Debe demostrarse que falla de forma predecible, controlada y segura.

Utilidad y fiabilidad

Un modelo puede ser útil para generar hipótesis o priorizar estudios y no ser suficientemente fiable para adoptar decisiones críticas de manera autónoma. Una predicción de vida útil puede ayudar a diseñar estudios, pero no debería sustituir la validación microbiológica y tecnológica necesaria para establecer una fecha de caducidad.

Validación continua

La validación no es un trámite único. Actualizaciones, nuevos datos, nuevas variables, cambios de hardware, ampliación a otros productos o plantas pueden exigir revalidación.

Visión artificial

Un modelo de inspección puede rendir bien en piloto y deteriorarse por cambios de iluminación, polvo sobre cámaras, vibraciones, velocidad de cinta o superposición de productos. El algoritmo no cambia; cambia el entorno.

Límites de utilización

Todo sistema debería documentar productos incluidos y excluidos, rangos de funcionamiento, variables obligatorias, condiciones ambientales, límites de incertidumbre y actuaciones cuando se excedan.

Evidencia documental

Debe conservarse evidencia de cómo se entrenó el modelo, qué datos se utilizaron, qué criterios de aceptación se fijaron, qué resultados obtuvo, qué limitaciones se identificaron, cuándo se validó, quién aprobó su uso y qué revisiones posteriores se realizaron.

Recomendaciones prácticas

21. Validar con datos independientes.
22. Ensayar durante periodos suficientemente prolongados.
23. Evaluar bajo condiciones reales.
24. Definir indicadores mínimos.
25. Establecer recalibración y revalidación.
26. Mantener supervisión humana inicial.
27. Registrar errores y desviaciones.
28. Identificar límites de utilización.
29. Disponer de contingencia.
30. Revisar el comportamiento durante todo el ciclo de vida.

Conclusión

Una prueba de concepto demuestra que una tecnología puede funcionar. Una validación industrial demuestra que puede seguir funcionando de manera fiable, segura y reproducible en producción real.

Error N.º 4. Delegar decisiones críticas en la IA sin una supervisión humana efectiva

GOBERNANZA: La supervisión humana debe ser competente, efectiva y capaz de detener o corregir el sistema.

Supervisión humana proporcional al riesgo

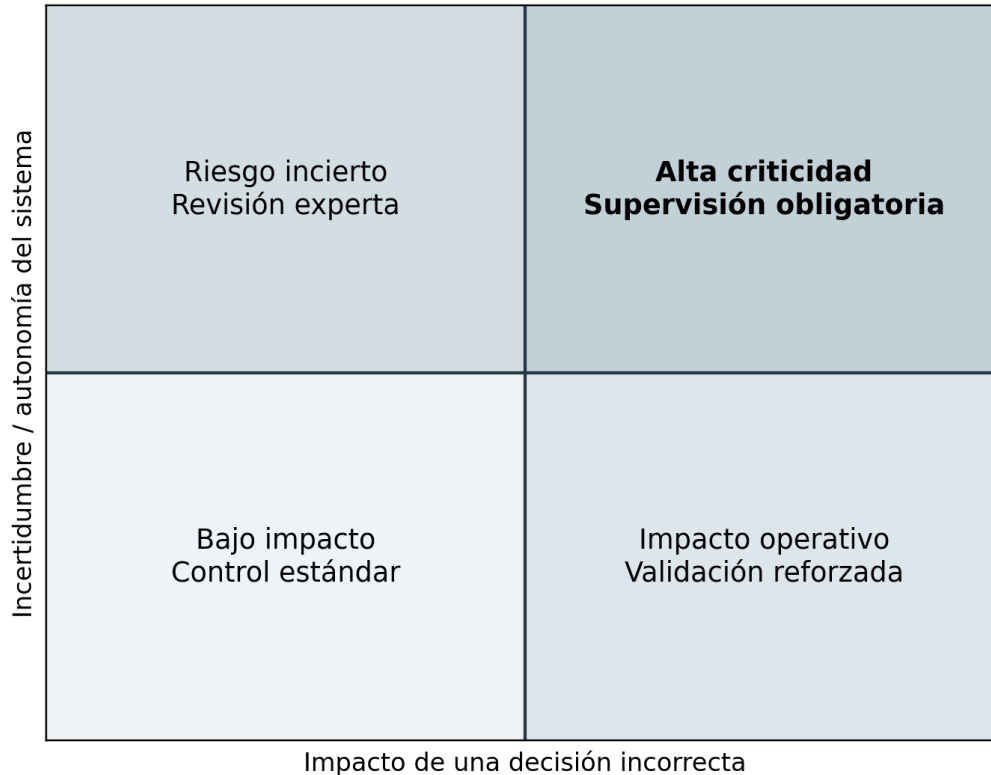


Figura 4. Matriz orientativa para determinar la intensidad de la supervisión humana.

Automatizar un proceso no significa eliminar la responsabilidad humana sobre las decisiones que genera. La confianza creciente en sistemas aparentemente eficaces puede reducir la supervisión y producir sesgo de automatización: la tendencia a aceptar recomendaciones automatizadas sin aplicar el mismo análisis crítico que se aplicaría a otro profesional.

La falsa percepción de objetividad

Los algoritmos dependen de datos de entrenamiento, variables seleccionadas, criterios de etiquetado, arquitectura y parámetros de optimización. Aceptar automáticamente sus recomendaciones equivale a aceptar sin revisión las decisiones implícitas incorporadas durante el diseño.

Qué significa supervisión humana

No basta con que una persona figure formalmente como responsable. Debe poder comprender el funcionamiento general, interpretar resultados, detectar anomalías, cuestionar recomendaciones, suspender el sistema y modificar o rechazar la decisión propuesta. Una supervisión nominal, basada en confirmar sistemáticamente lo que propone la IA, carece de valor.

Niveles de criticidad

Tabla 4. Niveles orientativos de criticidad y supervisión humana.

Nivel	Ejemplos	Supervisión
Bajo	Clasificación documental, búsqueda interna, traducción preliminar	Revisión por muestreo
Medio	Planificación, predicción de demanda, mantenimiento	Revisión de excepciones y umbrales
Alto	Liberación de lotes, vida útil, peligros microbiológicos	Aprobación humana obligatoria y evidencia completa

Las decisiones pueden clasificarse orientativamente en bajo impacto —clasificación documental, organización de archivos o generación de borradores—; impacto operativo —planificación, demanda, mantenimiento, logística o energía—; y alta criticidad —liberación de lotes, riesgos microbiológicos, límites APPCC, aceptación de materias primas, vida útil, caducidad o retirada de producto—.

En el último grupo, la supervisión humana constituye una condición esencial de buena práctica profesional.

La ilusión del piloto automático

El sistema suele funcionar bien dentro del rango observado. El problema aparece con materias primas desconocidas, contaminantes no vistos, combinaciones inéditas, averías simultáneas, incidentes infrecuentes o cambios legislativos.

La responsabilidad no se delega

La utilización de IA no desplaza automáticamente la responsabilidad del operador económico. La empresa alimentaria sigue siendo responsable de la seguridad y conformidad de sus productos. La IA puede asistir, pero no sustituye el deber de diligencia.

Diseñar la supervisión

Debe definirse quién revisa, qué cualificación necesita, qué decisiones puede aceptar, cuáles requieren revisión, qué umbral de confianza exige intervención, cómo se documentan discrepancias, cómo se suspende el sistema y cómo se gestionan errores.

El valor de la discrepancia

Las discrepancias entre experto e IA no son un problema que deba ocultarse. Permiten investigar si el algoritmo detectó un patrón nuevo, si el experto conoce una circunstancia omitida, si hay un error de datos o si el proceso cambió.

Formación y cultura

Los responsables deben comprender las limitaciones, reconocer situaciones fuera de dominio, evitar confianza excesiva y mantener criterio técnico independiente.

Recomendaciones prácticas

31. Política formal de supervisión humana.
32. Clasificación de decisiones según riesgo.
33. Umbrales de intervención obligatoria.
34. Procedimientos para aceptar, modificar o rechazar.

35. Registro de decisiones y fundamentos.
36. Protocolos ante comportamientos anómalos.
37. Formación específica.
38. Auditorías periódicas.
39. Revisión de discrepancias.
40. Asignación clara de responsabilidades.

Conclusión

La supervisión humana no es un obstáculo para la automatización, sino la condición que permite utilizarla de forma segura, responsable y defendible.

Error N.º 5. Ignorar el marco regulatorio aplicable al caso de uso

CUMPLIMIENTO: La clasificación jurídica depende del caso de uso y de sus efectos, no de la etiqueta comercial del software.

La IA no opera en un vacío normativo. Cuando se incorpora a una empresa alimentaria pasa a formar parte de un ecosistema regulado por disposiciones que afectan al diseño, implantación, utilización y supervisión.

El riesgo no consiste únicamente en incumplir el Reglamento europeo de IA, sino en desconocer que un mismo sistema puede quedar sometido a marcos diferentes.

Pensar que la IA es solo software

Cuando un sistema participa en decisiones de producción, calidad, seguridad alimentaria, gestión documental, selección de personal o evaluación de riesgos, deja de ser un software auxiliar y se convierte en un elemento que influye en obligaciones legales existentes.

La regulación no se activa únicamente porque exista IA; se activa porque la IA interviene en actividades jurídicamente relevantes.

Superposición normativa

Tabla 5. Superposición regulatoria típica en proyectos de IA alimentaria.

Marco	Cuándo puede aplicar	Implicación práctica
AI Act	Según finalidad y clasificación del sistema	Inventario, alfabetización, gobernanza y obligaciones proporcionales
Legislación alimentaria	Cuando la IA influye en alimentos o procesos	La responsabilidad del operador permanece
RGPD	Cuando se tratan datos personales	Base jurídica, minimización, seguridad y derechos
NIS2 / ciberseguridad	Entidades y actividades dentro de su ámbito	Gestión de riesgos, incidentes y cadena de suministro
Contratos / secreto empresarial	Uso de proveedores y plataformas externas	Control de datos, propiedad, auditoría y salida

Un proyecto puede verse afectado por el Reglamento (UE) 2024/1689, el Reglamento (CE) 178/2002, el paquete de higiene, el Reglamento (UE) 2017/625, el RGPD, NIS2 cuando proceda, la normativa laboral, la responsabilidad por productos y requisitos contractuales de certificación.

La evaluación exige colaboración entre tecnólogos, calidad, APPCC, datos, ciberseguridad, asesoría jurídica y dirección.

Enfoque basado en riesgo

Las obligaciones dependen del uso previsto y de las consecuencias. La clasificación debe documentarse caso por caso. Muchas aplicaciones alimentarias serán de riesgo limitado o mínimo, pero usos relacionados con empleo, infraestructuras críticas o personas pueden activar obligaciones superiores.

Responsabilidad del operador alimentario

La responsabilidad de garantizar el cumplimiento de la legislación alimentaria permanece en el operador. Si un algoritmo recomienda liberar un lote no conforme, la existencia del sistema no exime a la empresa.

IA, APPCC y sistemas de gestión

Cuando la IA influye en decisiones operativas debe integrarse en análisis de peligros, procedimientos APPCC, programas de prerrequisitos, gestión documental, gestión del cambio, validación y auditoría interna.

Protección de datos y confidencialidad

Las herramientas generativas pueden recibir formulaciones, especificaciones, informes microbiológicos, contratos, reclamaciones y datos de proveedores. Aunque no haya datos personales, puede existir secreto empresarial o confidencialidad contractual. Si hay datos personales, entra en juego el RGPD.

Documentación y gobernanza

La empresa debe conservar finalidad, evaluación de riesgos, clasificación, responsables, validación, controles, limitaciones, supervisión y cambios. Una gobernanza madura incluye inventario, política corporativa, criterios de clasificación, evaluación de proveedores, controles de acceso y auditorías.

Recomendaciones prácticas

41. Identificar normas aplicables.
42. Clasificar el riesgo conforme al AI Act.
43. Analizar impacto sobre seguridad alimentaria y APPCC.
44. Evaluar protección de datos y confidencialidad.
45. Revisar contratos.
46. Integrar la IA en calidad.
47. Documentar riesgos.
48. Designar responsables técnicos y jurídicos.
49. Establecer revisión periódica.
50. Mantener evidencia documental.

Conclusión

La IA modifica la forma en que se gestionan riesgos ya existentes. El cumplimiento no es un coste añadido, sino un elemento de competitividad y confianza.

Error N.º 6. No integrar la IA en APPCC, calidad, trazabilidad y gestión del cambio

AUDITORÍA: La IA que influye en decisiones operativas debe formar parte del sistema documental y de gestión del cambio.

Integración de la IA en el sistema APPCC

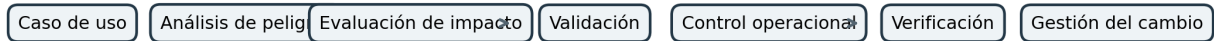


Figura 5. Integración de la IA en APPCC, validación, verificación y gestión del cambio.

Tratar la IA como un proyecto independiente de informática o innovación constituye un error estratégico. Toda tecnología que influya en materias primas, procesos, controles, liberación de lotes, mantenimiento, trazabilidad o documentación pasa a formar parte del sistema de gestión.

La IA como elemento del sistema

Las normas ISO 22000, FSSC 22000, BRCGS *Food Safety*, IFS Food e ISO 9001 parten de procesos definidos, documentados, controlados y sometidos a mejora. Cuando un algoritmo participa en decisiones, introduce un nuevo proceso que debe ser gobernado.

APPCC e IA

El APPCC regula peligros, no tecnologías. La pregunta relevante es si la IA influye en identificación, evaluación o control de peligros. Un algoritmo que modifica tiempo de cocción, que ajusta enfriamiento, prioriza análisis, evalúa proveedores o estima vida útil puede afectar a seguridad alimentaria.

No significa convertir el algoritmo automáticamente en PCC, sino analizar cómo modifica la evaluación de peligros y los controles existentes.

Validación y verificación

La validación demuestra que el método es adecuado; la verificación confirma que continúa funcionando. La empresa debe validar modelo, variables, datos, dominio y criterios; y verificar rendimiento, estabilidad, desviaciones, cambios y pérdida de precisión.

Trazabilidad de la decisión

Además de la trazabilidad del producto, se necesita trazabilidad de la decisión: qué información recibió el sistema, qué versión operaba, qué recomendación emitió, quién la revisó, qué decisión se adoptó y qué evidencia quedó registrada.

Gestión del cambio

La IA puede modificar procedimientos, responsabilidades, tiempos de respuesta, necesidades formativas, criterios de aceptación y flujos de comunicación. Debe gestionarse mediante un procedimiento formal.

Competencias profesionales

Los responsables de producción y calidad deben comprender limitaciones, indicadores de confianza, situaciones fuera de dominio y actuación ante errores. La IA transforma el perfil competencial de la organización.

Auditorías

Los auditores pueden preguntar qué sistemas existen, qué decisiones apoyan, quién autorizó, cómo se validaron, qué evidencias hay, cómo se gestionan actualizaciones y qué ocurre ante discrepancias.

Integración con normas certificables

Tabla 6. Integración de la IA en sistemas de gestión y certificación.

Sistema	Punto de integración de IA	Evidencia esperable
APPCC / Codex	Análisis de peligros, validación y verificación	Evaluación de impacto, límites y registros
ISO 22000 / FSSC 22000	Control operacional, riesgos y mejora	Procedimientos, responsabilidades y revisión
BRCGS Food Safety	Control de procesos, cultura y gestión del cambio	Aprobación, formación y auditoría interna
IFS Food	Análisis de riesgos, trazabilidad y competencias	Registros de decisión y cualificación
ISO 9001	Enfoque a procesos y desempeño	KPIs, acciones correctivas y mejora continua

ISO 22000/FSSC aportan análisis de contexto, gestión del riesgo, control operacional, validación y mejora. BRCGS aporta cultura, documentación, control de procesos, acciones correctivas y revisión. IFS aporta análisis de riesgos, competencias, cambio y trazabilidad. ISO 9001 aporta enfoque de procesos y evaluación del desempeño.

Recomendaciones prácticas

51. Inventario corporativo.
52. Evaluación formal de impacto sobre APPCC.
53. Integración documental.
54. Validación y verificación periódica.
55. Gestión formal de cambios.
56. Registro de versiones.
57. Trazabilidad de decisiones.
58. Formación específica.
59. Auditorías internas.
60. Revisión por la dirección.

Conclusión

La IA no es una herramienta aislada, sino un proceso que interactúa con el sistema de gestión. Su integración documental y operativa constituye una exigencia de buena práctica industrial.

Error N.º 7. Utilizar modelos opacos sin controlar explicabilidad, incertidumbre y deriva

CONTROL: Una predicción sin incertidumbre, límites de uso y monitorización de deriva no es una decisión industrialmente segura.

La precisión no es el único criterio de calidad. Un algoritmo puede alcanzar excelentes resultados estadísticos y ser inaceptable desde el punto de vista técnico, regulatorio o pericial si la organización no comprende cuándo acierta, por qué puede equivocarse y en qué circunstancias deja de ser fiable.

La caja negra

Los modelos complejos pueden producir una respuesta sin que el proceso interno sea interpretable. Si un algoritmo recomienda rechazar un lote de leche por riesgo de alteración, calidad necesita saber qué variables influyeron, qué evidencia apoya la conclusión, qué confianza tiene, si existen precedentes y si puede verificarse por métodos convencionales.

Un porcentaje aislado de probabilidad no basta.

Explicabilidad y transparencia

Explicar no exige revelar todas las ecuaciones ni el secreto industrial del proveedor. Exige comprender variables relevantes, influencia, limitaciones, situaciones de cautela y circunstancias en que el sistema dispone de poca información.

Incertidumbre

Todo modelo debería responder cuál es la predicción y con qué nivel de confianza se formula. Una vida útil estimada de 24 días con 98 % de confianza no es equivalente a la misma cifra con 58 %. La incertidumbre es información.

Falsa seguridad de los porcentajes

Porcentajes con decimales generan sensación de exactitud, pero la precisión numérica no equivale a validez científica. Un algoritmo puede mostrar enorme confianza en una respuesta errónea, especialmente con datos fuera de distribución.

Detección fuera de distribución

El sistema debería reconocer cuándo recibe un ingrediente, materia prima, formulación, sensor, campaña o proceso no observado previamente y advertir de que su fiabilidad puede reducirse.

Deriva del modelo

Además de *data drift*, el rendimiento puede deteriorarse por cambios tecnológicos, proveedores, métodos analíticos, software o hábitos. Este deterioro puede pasar desapercibido si no se monitoriza.

Explicabilidad y auditoría

Audidores, clientes y autoridades pueden solicitar variables, validación, limitaciones, actualizaciones, controles de pérdida de rendimiento y supervisión de decisiones críticas.

IA explicable

Las técnicas XAI permiten estimar importancia de variables, contribución de parámetros, sensibilidad, escenarios alternativos y motivos principales de una predicción. No eliminan la complejidad, pero hacen el sistema más gobernable.

Recomendaciones prácticas

61. Documentar el dominio de aplicación.
62. Medir rendimiento periódicamente.
63. Registrar incertidumbre.
64. Detectar situaciones OOD.
65. Supervisar *model drift*.
66. Supervisar *data drift*.
67. Incorporar XAI cuando sea viable.
68. Registrar actualizaciones.
69. Definir umbrales de intervención humana.
70. Revisar la validez científica.

Conclusión

La madurez no se mide solo por aciertos, sino por la capacidad de reconocer limitaciones, comunicar incertidumbre y mantener estabilidad a lo largo del tiempo.

Error N.º 8. Subestimar la ciberseguridad, la confidencialidad y la dependencia del proveedor

CONFIDENCIALIDAD: Las formulaciones, parámetros y datos experimentales constituyen patrimonio empresarial, no simples entradas de software.

Capas de protección de un sistema de IA



Figura 6. Capas de protección frente a riesgos de ciberseguridad y dependencia tecnológica.

La seguridad del ecosistema digital suele permanecer infravalorada hasta que se produce un incidente. Cuando la IA participa en decisiones, un ataque puede alterar no solo la infraestructura, sino también decisiones sobre materias primas, procesos, calidad, logística o seguridad alimentaria.

Los datos tienen valor

La IA utiliza formulaciones, especificaciones, parámetros de proceso, estudios microbiológicos, curvas térmicas, protocolos APPCC, resultados analíticos, reclamaciones, datos de proveedores e históricos de producción. Este patrimonio informacional constituye uno de los principales activos de la empresa.

Plataformas externas

Copiar recetas, formulaciones, métodos, especificaciones de clientes, contratos o estrategias en una plataforma externa puede comprometer el control sobre la información. La cuestión forma parte de la gestión del secreto empresarial.

Protección del conocimiento industrial

El valor puede residir en formulaciones, procesos de extracción, parámetros de fermentación, bases experimentales, modelos, resultados y know-how no patentado. La gobernanza de IA debe integrarse con la protección del conocimiento.

Ataques específicos

Tabla 7. Riesgos de ciberseguridad específicos de los sistemas de IA.

Amenaza	Efecto posible	Medida prioritaria
Data <i>poisoning</i>	Aprendizaje manipulado	Control de procedencia e integridad de datos
Ataques adversarios	Clasificación errónea ante entradas alteradas	Pruebas de robustez y detección de anomalías
Extracción de modelo	Pérdida de propiedad intelectual	Limitación de consultas y monitorización

Prompt injection / fuga	Exposición o manipulación de información	Aislamiento, filtros, permisos y revisión
Indisponibilidad del proveedor	Interrupción operativa	Plan de contingencia y portabilidad

El *data poisoning* introduce datos manipulados durante el entrenamiento. Los ataques adversariales alteran entradas para inducir respuestas erróneas. La extracción de modelos intenta reconstruir su funcionamiento. La inversión de modelos puede inferir información del entrenamiento.

Dependencia del proveedor

Deben evaluarse alojamiento, acceso, cese de actividad, recuperación de datos, migración, cambios contractuales, control de actualizaciones y auditoría independiente. Una dependencia excesiva constituye riesgo estratégico.

Actualizaciones no controladas

Un servicio SaaS puede modificar algoritmo, prioridades, clasificación, interfaz e indicadores. Si afecta a decisiones industriales, la actualización debe evaluarse como cambio significativo.

Convergencia IT/OT

La IA puede interactuar con PLC, SCADA, MES, robots, sensores y líneas automatizadas. Un incidente puede repercutir sobre procesos físicos.

Continuidad de negocio

La empresa debe saber qué ocurrirá si el sistema deja de estar disponible: responsables, procedimientos manuales, criterios provisionales, acceso a registros y recuperación.

Política corporativa

Debe definir herramientas autorizadas y prohibidas, información compartible, clasificación documental, uso de cuentas corporativas, conservación de registros, autenticación y autorización de nuevos servicios.

Recomendaciones prácticas

71. Inventario de información crítica.
72. Clasificación de confidencialidad.
73. Evaluación de riesgos específicos.
74. Revisión contractual.
75. Copias y recuperación.
76. Continuidad de negocio.
77. Política sobre IA generativa.
78. Formación periódica.
79. Auditoría de proveedores.
80. Revisión de dependencia y migración.

Conclusión

La IA debe contemplarse como infraestructura crítica de conocimiento. Proteger datos, know-how y continuidad es tan importante como proteger instalaciones.

Error N.º 9. Pretender sustituir el conocimiento experto en lugar de estructurarlo y ampliarlo

PERSONAS: Automatizar sin preservar competencias críticas puede aumentar la fragilidad de la organización.

Modelo de inteligencia aumentada

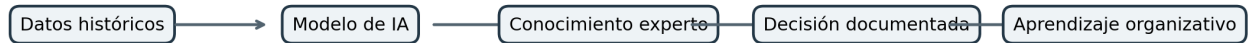


Figura 7. Inteligencia aumentada: integración de datos, algoritmos y conocimiento experto.

La IA genera mayor valor cuando potencia el conocimiento experto, no cuando intenta reemplazarlo. Esta diferencia es crítica en la industria alimentaria, donde muchas decisiones dependen de conocimiento tácito adquirido durante años.

Conocimiento explícito y tácito

Los procedimientos y registros contienen conocimiento explícito. El conocimiento tácito incluye reconocer una fermentación anómala, detectar una desviación sensorial, anticipar problemas de campaña, ajustar procesos por humedad o integrar señales débiles de múltiples fuentes.

La IA aprende correlaciones; el experto interpreta causalidad

Un modelo puede detectar que ciertos lotes duran menos cuando aumenta la conductividad de una materia prima. El tecnólogo debe determinar si la causa es mineralógica, estacional, analítica, de proveedor, contaminación o coincidencia.

Riesgo de *deskilling*

Cuando las personas dejan de intervenir, sus capacidades se deterioran. Si durante años un algoritmo evalúa proveedores, clasifica resultados o interpreta riesgos, los profesionales pueden perder práctica para actuar cuando falle.

Patrimonio intelectual

Décadas de experiencia sobre formulaciones, estabilidad, materias primas, procesos, ingredientes, regulación e incidencias pueden residir en pocas personas. La jubilación o salida de expertos crea una vulnerabilidad estructural.

Inteligencia aumentada

La IA puede aumentar la capacidad para analizar información, detectar relaciones, revisar documentación, acceder al conocimiento histórico, reducir tareas repetitivas y dedicar más tiempo al razonamiento de alto valor.

Captura de conocimiento

Entrevistas estructuradas, árboles de decisión, bases enriquecidas, sistemas RAG, bibliotecas de casos y modelos híbridos permiten convertir conocimiento individual en corporativo.

Modelos híbridos

Los mejores resultados pueden combinar modelos estadísticos, reglas tecnológicas, límites regulatorios, microbiología y experiencia. El algoritmo estima, las reglas limitan y el experto revisa situaciones de alta incertidumbre.

Formación bidireccional

Los especialistas aportan experiencia y criterio; los profesionales de IA aportan modelización, automatización y análisis. La convergencia de ambos perfiles es un factor de éxito.

Recomendaciones prácticas

81. Identificar conocimiento crítico.
82. Localizar expertos estratégicos.
83. Capturar conocimiento tácito.
84. Integrar IA y documentación.
85. Implantar modelos híbridos.
86. Mantener supervisión humana.
87. Formar continuamente.
88. Evitar pérdida de competencias.
89. Ampliar la capacidad analítica.
90. Medir preservación del conocimiento.

Conclusión

El objetivo no debe ser crear empresas con menos expertos, sino organizaciones capaces de aprovechar mejor el talento que poseen.

Error N.º 10. Medir el éxito por la novedad tecnológica y no por el valor industrial demostrado

DIRECCIÓN: El número de herramientas implantadas no es un KPI; el valor neto y el riesgo controlado sí lo son.

Evaluar el éxito por la sofisticación tecnológica en lugar de por el valor real es uno de los errores más trascendentes. Incorporar asistentes, visión artificial o modelos predictivos no garantiza impacto sobre la actividad industrial.

Innovación tecnológica e innovación empresarial

Tecnologías sencillas como un intercambiador, una mejora higiénica, una optimización APPCC o un cambio de logística pueden generar más valor que proyectos sofisticados. La pregunta correcta no es si se utiliza IA, sino qué problema se resolvió y cómo se demuestra.

Del entusiasmo al retorno industrial

Tras las demostraciones iniciales deben responderse preguntas concretas: si disminuyó el desperdicio, las reclamaciones, las desviaciones, el consumo energético, los tiempos de formulación o si mejoró el margen.

ROI integral

Tabla 8. Evaluación multidimensional del retorno de la IA.

Dimensión	Valor generado	Ejemplo de evidencia
Económica	Reducción de costes o incremento de margen	Ahorro anual neto y coste total de propiedad
Tecnológica	Mejor capacidad predictiva	Comparación contra método de referencia
Regulatoria	Mayor trazabilidad y control	Registros auditables y reducción de desviaciones
Organizativa	Preservación y difusión del conocimiento	Uso de bases de casos y menor dependencia individual
Estratégica	Mayor velocidad de innovación	Tiempo de lanzamiento y tasa de éxito

La evaluación debe incluir **valor económico** —costes, productividad, pérdidas—; **tecnológico** —capacidad predictiva y robustez—; **regulatorio** —trazabilidad y evidencia—; **organizativo** —conocimiento y colaboración—; y **estratégico** —diferenciación, innovación y adaptación—.

AI washing

Presentar iniciativas con utilidad limitada, pero alto valor comunicativo, dispersa recursos, frustra al personal y reduce credibilidad. La mejor comunicación se basa en resultados verificables.

Integración estratégica

La IA debe apoyar objetivos corporativos como seguridad alimentaria, eficiencia energética, innovación, reducción de desperdicio, trazabilidad, cumplimiento o experiencia de cliente.

Indicadores relevantes

Producción: OEE, rendimiento, paradas, energía. Calidad: reclamaciones, no conformidades, repeticiones. Seguridad: incidencias, retiradas y tiempos de respuesta. I+D: tiempo de desarrollo y formulaciones. Gestión: tiempos documentales y revisión regulatoria.

Ciclo de vida completo

El proyecto no termina con la puesta en marcha. Requiere mantenimiento, actualizaciones, formación, auditorías, recalibración, adaptación normativa y evolución.

El verdadero indicador

Si el sistema dejara de funcionar mañana, ¿la organización perdería una capacidad significativa? Si la respuesta es negativa, probablemente la IA aún no está integrada.

Recomendaciones prácticas

91. Indicadores objetivos.
92. Impacto económico cuantificado.
93. Mejora técnica validada.
94. Beneficios regulatorios demostrables.
95. Conocimiento retenido.
96. Integración estratégica.
97. Recursos de mantenimiento.
98. Plan de evolución.
99. Uso habitual.
100. Pérdida clara de eficiencia si el sistema desaparece.

Conclusión

La IA debe juzgarse por su capacidad para mejorar seguridad, calidad, eficiencia, innovación y competitividad, no por la complejidad del algoritmo ni por su impacto mediático.

Conclusiones

La implantación de inteligencia artificial en la industria alimentaria representa una de las transformaciones tecnológicas más profundas desde la generalización de la automatización, los sistemas APPCC y la digitalización de la gestión. A diferencia de procesos anteriores, la IA no se limita a ejecutar tareas más rápido: interviene sobre la toma de decisiones.

Esta circunstancia modifica la naturaleza del riesgo empresarial. La industria ha desarrollado sistemas robustos para controlar materias primas, procesos, instalaciones, contaminación, trazabilidad y documentación. La IA añade la necesidad de gobernar sistemas capaces de analizar información, establecer relaciones, formular recomendaciones e incluso ejecutar actuaciones con autonomía creciente.

El debate ya no puede reducirse a determinar si la IA funciona. La cuestión relevante es: en qué condiciones resulta técnicamente fiable, jurídicamente defendible y organizativamente sostenible.

Los diez errores presentan una característica común. Ninguno deriva exclusivamente de una limitación inherente de la IA. Todos responden a deficiencias en la forma en que las organizaciones diseñan, implantan, gobiernan y supervisan estas tecnologías.

Comenzar por la herramienta; utilizar datos insuficientemente gobernados; confundir pilotos con sistemas validados; delegar decisiones críticas; ignorar el marco regulatorio; mantener la IA al margen del APPCC y la calidad; utilizar modelos opacos; descuidar ciberseguridad y conocimiento; sustituir criterio experto; o medir éxito por novedad son manifestaciones de un mismo problema: ausencia de gobernanza.

Desde esta perspectiva, la IA deja de ser un proyecto tecnológico para convertirse en una cuestión de dirección empresarial. Exige colaboración entre ingeniería, tecnología de alimentos, microbiología, química, estadística, ciencia de datos, ciberseguridad, derecho, calidad, auditoría y estrategia.

La ventaja competitiva no dependerá exclusivamente de mejores algoritmos, sino de integrar esos algoritmos en organizaciones capaces de garantizar que cada decisión siga siendo científicamente sólida, técnicamente verificable y jurídicamente justificable.

Adquiere especial importancia la gobernanza algorítmica. Del mismo modo que las empresas desarrollaron sistemas para seguridad alimentaria, trazabilidad y calidad, deberán desarrollar sistemas equivalentes para gobernar modelos: políticas, responsabilidades, ciclo de vida, trazabilidad de decisiones, validación, calidad de datos, gestión del cambio e intervención humana proporcional al riesgo.

La IA tampoco elimina la importancia del conocimiento experto; aumenta su valor. En un entorno de automatización, la capacidad diferencial residirá en profesionales capaces de interpretar resultados, identificar anomalías, formular hipótesis, integrar disciplinas y asumir responsabilidad final.

Desde el punto de vista regulatorio, el panorama europeo continuará evolucionando mediante directrices, estándares, normas técnicas y criterios de auditoría. Las empresas que cumplan con los cánones y documenten, clasifiquen, supervisen y gobiernen desde ahora estarán mejor posicionadas.

La historia demuestra que las tecnologías transformadoras terminan integrándose de forma casi invisible. En el futuro dejará de hablarse de empresas que utilizan IA. Habrá empresas bien gestionadas y empresas peor gestionadas. Las primeras integrarán la IA como componente natural de sus procesos; las segundas mantendrán herramientas dispersas sin estrategia.

La innovación tecnológica nunca ha sustituido la buena ingeniería, el rigor científico ni la responsabilidad profesional. La IA tampoco lo hará. Su auténtico potencial reside en permitir que el juicio humano se ejerza con más información, rapidez, consistencia y capacidad analítica.

Decálogo ejecutivo para implantar IA en la industria alimentaria

Diez principios para una implantación técnicamente sólida, regulatoriamente segura y empresarialmente rentable.

Principio	Pregunta clave	Recomendación
1. Definir primero el problema	¿Qué queremos resolver?	No implantar IA sin objetivo concreto, medible y relevante.
2. Gobernar los datos	¿Son fiables, trazables y representativos?	Priorizar calidad y contexto sobre volumen.
3. Validar antes de producir	¿Funciona en condiciones reales?	No confundir PoC con validación industrial.
4. Mantener supervisión humana	¿Quién asume la decisión?	Control humano efectivo en decisiones críticas.
5. Analizar el marco regulatorio	¿Qué obligaciones se aplican?	Evaluar AI Act, legislación alimentaria, datos, ciberseguridad y contratos.
6. Integrar en el sistema de gestión	¿Forma parte de APPCC y calidad?	No crear procesos paralelos.
7. Exigir explicabilidad y monitorización	¿Puede entenderse y revisarse?	Controlar incertidumbre, deriva, dominio y XAI.
8. Proteger conocimiento corporativo	¿Se preservan datos y procesos?	Ciberseguridad, confidencialidad, continuidad y control de proveedor.
9. Potenciar conocimiento experto	¿Complementa o sustituye criterio?	Capturar y ampliar conocimiento; evitar <i>deskilling</i> .
10. Medir valor generado	¿Qué beneficios verificables aporta?	Evaluar seguridad, calidad, productividad, cumplimiento y rentabilidad.

Anexo I. Modelo MIA-FOOD 1.0

Modelo MIA-FOOD 1.0: niveles de madurez

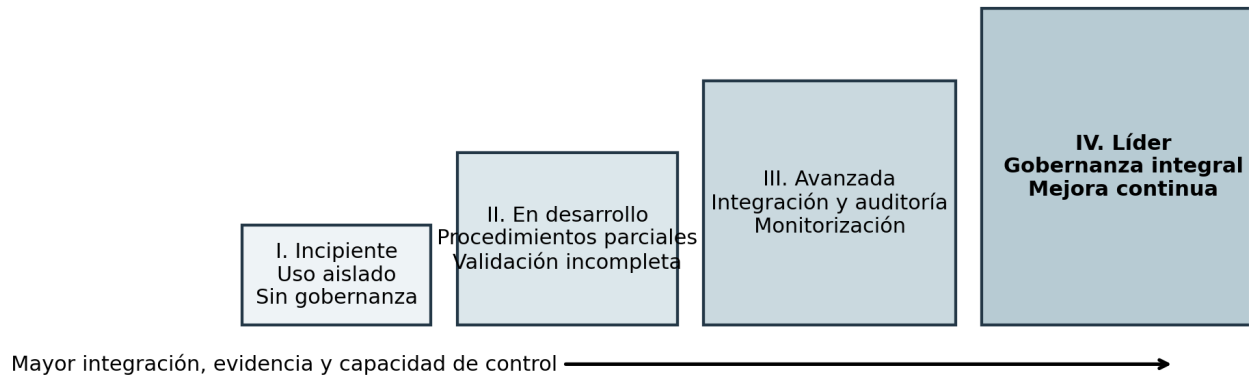


Figura 8. Representación del modelo de madurez MIA-FOOD 1.0.

Modelo de evaluación de la madurez en la implantación de inteligencia artificial en la industria alimentaria.

Escala: 0 = inexistente; 1 = informal o parcial; 2 = existente pero incompleto; 3 = implantado y documentado; 4 = implantado, auditado y sometido a mejora continua.

A. Estrategia y gobernanza

Criterio	Puntuación (0-4)	Evidencia / observaciones
Estrategia formal de IA		
Inventario actualizado de sistemas		
Responsable funcional por sistema		
Revisión periódica por la dirección		
Política corporativa de uso responsable		

B. Datos

Criterio	Puntuación (0-4)	Evidencia / observaciones
Inventario de fuentes		
Trazabilidad de datos de entrenamiento		
Control de faltantes, inconsistencias y duplicados		
Detección de data drift		
Revisión periódica de calidad		

C. Validación técnica

Criterio	Puntuación (0-4)	Evidencia / observaciones
Validación con datos independientes		
Límites de utilización conocidos		

Monitorización continua		
Control de <i>model drift</i>		
Procedimiento formal de revalidación		

D. Seguridad alimentaria y calidad

Criterio	Puntuación (0-4)	Evidencia / observaciones
Evaluación dentro de APPCC		
Procedimientos de calidad actualizados		
Registro de decisiones automatizadas		
Trazabilidad de recomendaciones		
Auditorías internas de IA		

E. Cumplimiento normativo

Criterio	Puntuación (0-4)	Evidencia / observaciones
Clasificación conforme al AI/Act		
Evaluación jurídica previa		
Análisis de protección de datos		
Contratos específicos de IA		
Documentación para auditorías		

F. Ciberseguridad

Criterio	Puntuación (0-4)	Evidencia / observaciones
Política para herramientas generativas		
Control de información compartida		
Plan de continuidad		
Copias y pruebas de recuperación		
Evaluación de dependencia del proveedor		

G. Personas y cultura

Criterio	Puntuación (0-4)	Evidencia / observaciones
Formación específica		
Supervisión humana efectiva		
Preservación del conocimiento experto		
Análisis de discrepancias		
Cultura de mejora continua		

Interpretación

0–35 puntos — Nivel I: Organización incipiente

Elevado riesgo organizativo y regulatorio. Prioridad: crear gobernanza antes de ampliar aplicaciones.

36–70 puntos — Nivel II: Organización en desarrollo

Existen iniciativas, pero la integración es incompleta. Prioridad: validación, documentación y supervisión.

71–105 puntos — Nivel III: Organización avanzada

Estructura razonablemente madura. Prioridad: auditoría y mejora continua.

106–140 puntos — Nivel IV: Organización líder

IA integrada en estrategia, calidad, seguridad alimentaria y conocimiento.

Bibliografía técnica, científica y jurídica utilizada

Legislación de la Unión Europea

- Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial.
- Reglamento (CE) n.º 178/2002, por el que se establecen los principios y requisitos generales de la legislación alimentaria y se crea la EFSA.
- Reglamento (CE) n.º 852/2004, relativo a la higiene de los productos alimenticios.
- Reglamento (CE) n.º 853/2004, sobre normas específicas de higiene de alimentos de origen animal.
- Reglamento (UE) 2017/625, relativo a los controles oficiales.
- Reglamento (UE) 2016/679, Reglamento General de Protección de Datos.
- Directiva (UE) 2022/2555, NIS2.

Normas y marcos técnicos

- ISO 22000, Food safety management systems.
- ISO 9001, Quality management systems.
- ISO/IEC 27001, Information security management systems.
- ISO/IEC 23894, Artificial intelligence — Risk management.
- ISO/IEC 42001, Artificial intelligence management system.
- ISO 31000, Risk management.
- Codex Alimentarius, General Principles of Food Hygiene (CXC 1-1969).
- NIST, Artificial Intelligence Risk Management Framework (AI RMF 1.0).
- NIST, Cybersecurity Framework 2.0.

Estándares de seguridad alimentaria

- BRCGS Global Standard Food Safety.
- IFS Food Standard.
- FSSC 22000 Scheme Requirements.
- Global Food Safety Initiative Benchmarking Requirements.

Obras generales

- Russell, S.; Norvig, P. Artificial Intelligence: A Modern Approach.
- Goodfellow, I.; Bengio, Y.; Courville, A. Deep Learning.
- Bishop, C. M. Pattern Recognition and Machine Learning.
- Hastie, T.; Tibshirani, R.; Friedman, J. The Elements of Statistical Learning.
- Molnar, C. Interpretable Machine Learning.
- Pearl, J. Causality.

Revistas recomendadas

- Trends in Food Science & Technology.
- Comprehensive Reviews in Food Science and Food Safety.
- Food Control.
- Food Chemistry.
- Journal of Food Engineering.

- LWT — Food Science and Technology.
- Innovative Food Science and Emerging Technologies.
- Computers and Electronics in Agriculture.
- npj Science of Food.

Otras Referencias Bibliográficas

I. Legislación y normativa (11 referencias)

[1] Parlamento Europeo y Consejo. Reglamento (UE) 2024/1689, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial (Artificial Intelligence Act).

[2] Parlamento Europeo y Consejo. 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.

[3] Parlamento Europeo y Consejo. Reglamento (CE) n.º 853/2004, relativo a la higiene de los productos alimenticios.

[4] Parlamento Europeo y Consejo. Reglamento (CE) n.º 853/2004, por el que se establecen normas específicas de higiene de los alimentos de origen animal.

[5] Parlamento Europeo y Consejo. Reglamento (UE) 2017/625, relativo a los controles oficiales.

[6] Parlamento Europeo y Consejo. Reglamento (UE) 2016/679 (RGPD).

[7] Parlamento Europeo y Consejo. Directiva (UE) 2022/2555 (NIS2).

[8] Codex Alimentarius Commission. *General Principles of Food Hygiene (CXC 1-1969)*.

[9] ISO. *ISO 22000:2018. Food Safety Management Systems*.

[10] ISO/IEC. *ISO/IEC 23894:2023. Artificial Intelligence — Risk Management*.

[11] ISO/IEC. *ISO/IEC 42001:2023. Artificial Intelligence — Management System*.

II. Documentos institucionales (8 referencias)

[12] European Commission. *Artificial Intelligence Act – Official Documentation*.

[13] European Food Safety Authority (EFSA). *Artificial Intelligence Roadmap*.

[14] European Food Safety Authority (EFSA). *Artificial Intelligence Strategy*.

[15] FAO. *The State of Food and Agriculture*.

[16] National Institute of Standards and Technology (NIST). *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*.

[17] OECD. *OECD Principles on Artificial Intelligence*.

[18] UNESCO. *Recommendation on the Ethics of Artificial Intelligence*.

[19] World Health Organization. *Ethics and Governance of Artificial Intelligence for Health*.

III. Obras fundamentales sobre IA (7 referencias)

[20] Russell, S.; Norvig, P. *Artificial Intelligence: A Modern Approach*. 4th ed., Pearson, 2021.

[21] Goodfellow, I.; Bengio, Y.; Courville, A. *Deep Learning*. MIT Press, 2016.

[22] Bishop, C. M. *Pattern Recognition and Machine Learning*. Springer, 2006.

[23] Murphy, K. P. *Machine Learning: A Probabilistic Perspective*. MIT Press, 2012.

[24] Hastie, T.; Tibshirani, R.; Friedman, J. *The Elements of Statistical Learning*. Springer.

[25] Molnar, C. *Interpretable Machine Learning*. 2nd ed.

[26] Pearl, J. *Causality: Models, Reasoning and Inference*. Cambridge University Press.

IV. Inteligencia artificial aplicada a la industria alimentaria (12 referencias)

[27] Amanatidou, E., et al. *Artificial intelligence applications in the food industry: Current status and future perspectives*. *Trends in Food Science & Technology*.

[28] Bousselmi, L., et al. *Artificial intelligence in food safety: Applications, opportunities and regulatory challenges*. *Food Control*.

[29] *A comprehensive review on artificial intelligence assisted technologies in food industry*. *Food Bioscience*, 2023.

[30] *Artificial Intelligence in Food Safety: A Decade Review and Bibliometric Analysis*. *Foods*, 2023.

[31] *Revolutionizing the food industry: The transformative power of artificial intelligence – A review*. *Food Science & Nutrition*, 2024.

[32] Chen, Y., et al. *Machine learning for predictive food microbiology: A systematic review*.

[33] Hassoun, A., et al. *Artificial intelligence in food processing and quality assessment*.

[34] Kotsiantis, S., et al. *Artificial intelligence in food manufacturing: A review*.

[35] Othman, S., et al. *Artificial intelligence-based techniques for adulteration and defect detection in food and agricultural industry: A review*. *Smart Agricultural Technology*, 2023.

[36] Namkhah, Z., et al. *Advancing sustainability in the food and nutrition system: A review of artificial intelligence applications*. *Frontiers in Nutrition*, 2023.

[37] Chen, T., et al. *Empowering Agrifood System with Artificial Intelligence: A Survey of the Progress, Challenges and Opportunities*, 2023.

[38] Min, W., et al. *From Plate to Production: Artificial Intelligence in Modern Consumer-Driven Food Systems*, 2023.

V. Gobernanza, derecho y ética de la IA (7 referencias)

[39] Sartor, G. *Artificial Intelligence and Law*.

[40] Barfield, W. *The Cambridge Handbook of the Law of Algorithms*.

[41] Brownsword, R. *Law, Technology and Society*.

[42] Pagallo, U. *The Laws of Robots*.

[43] Yeung, K.; Lodge, M. *Algorithmic Regulation*.

[44] ENISA. *Threat Landscape Reports for Artificial Intelligence*.

[45] ENISA. *Artificial Intelligence Cybersecurity Challenges*.

Edita: Servicio de Publicaciones y Estudios de INTABIOTECH

Botiguers, 3, 1ª Planta, 46980 · Paterna, Valencia, España

Parque Empresarial Táctica

www.intabiotech.com