

Inteligencia Artificial, APPCC y Seguridad Alimentaria

Marco técnico, jurídico y operativo para integrar sistemas de IA en
la industria alimentaria

José Manuel López — INTABIOTECH

INTELIGENCIA ARTIFICIAL, APPCC Y SEGURIDAD ALIMENTARIA

Cómo integrar sistemas algorítmicos sin crear nuevos puntos ciegos
en el control de los peligros alimentarios

Marco técnico, jurídico y operativo para la industria alimentaria y de ingredientes

José Manuel López, BSc, MD, PhD

INTABIOTECH

Edición revisada y consolidada · Julio de 2026

Departamento Técnico · INTABIOTECH

NOTA EDITORIAL Y DE ACTUALIZACIÓN

Este manuscrito integra y consolida el trabajo desarrollado sobre inteligencia artificial, APPCC y sistemas de gestión de la seguridad alimentaria. Su finalidad es servir simultáneamente como artículo técnico-jurídico, guía de implantación, documento de formación y base de auditoría interna.

La revisión normativa se ha cerrado el 15 de julio de 2026. Debe verificarse cualquier modificación posterior antes de utilizar el documento como base de una decisión regulatoria, contractual o de certificación.

FSSC 22000 versión 7 fue publicada en mayo de 2026. El proceso de transición prevé auditorías de actualización entre el 1 de mayo de 2027 y el 30 de abril de 2028. Por ello, durante el periodo transitorio pueden coexistir organizaciones certificadas conforme a la versión 6 y organizaciones que preparan la versión 7 [17, 18].

La matriz de correspondencia con BRCGS, IFS y FSSC incluida en este documento es interpretativa. No sustituye los textos oficiales de los esquemas, sus doctrinas, guías de interpretación ni el criterio de la entidad de certificación.

RESUMEN

La incorporación de sistemas de inteligencia artificial en la industria alimentaria está modificando la forma en que se supervisan los procesos, se detectan desviaciones, se predice la vida útil, se clasifican materias primas y se adoptan decisiones relacionadas con la seguridad de los alimentos. Sin embargo, cuando el resultado de un modelo interviene en la identificación, evaluación, vigilancia o control de un peligro, la inteligencia artificial pasa a formar parte material del sistema de gestión de la seguridad alimentaria y debe quedar sometida a exigencias de validación, verificación, trazabilidad y supervisión equivalentes —o superiores— a las aplicables a cualquier otro elemento de control. El problema central reside en que la clasificación jurídica de un sistema conforme al Reglamento Europeo de Inteligencia Artificial no coincide necesariamente con su criticidad desde la perspectiva del análisis de peligros y puntos de control crítico. Una herramienta puede no ser considerada de alto riesgo conforme al AI Act y, al mismo tiempo, condicionar decisiones capaces de afectar directamente a la inocuidad del producto. Este trabajo propone un modelo de integración basado en la separación entre IA informativa, de apoyo, de vigilancia y de control autónomo; desarrolla un índice interno de criticidad algorítmica alimentaria; formula un protocolo de validación DQ–IQ–OQ–PQ; y establece evidencias auditables para BRCGS Food Safety Issue 9, IFS Food 8 y FSSC 22000 versión 7.

Palabras clave: inteligencia artificial; APPCC; HACCP; seguridad alimentaria; validación algorítmica; puntos de control crítico; AI Act; industria alimentaria; modelos predictivos; supervisión humana; auditoría.

ABSTRACT

The use of artificial intelligence in the food industry is changing process monitoring, deviation detection, shelf-life prediction, raw-material classification and food-safety decision-making. When an AI output materially affects hazard identification, assessment, monitoring or control, the system becomes part of the food-safety management architecture and must be subjected to validation, verification, traceability, human oversight and change-control requirements. This paper distinguishes legal classification under the EU AI Act from food-safety criticality under HACCP, proposes an internal Food Algorithmic Criticality Index, develops a DQ–IQ–OQ–PQ validation protocol, and maps expected evidence against BRCGS Food Safety Issue 9, IFS Food 8 and FSSC 22000 Version 7.

Keywords: *artificial intelligence; HACCP; food safety; algorithm validation; critical control points; EU AI Act; predictive models; human oversight; auditing.*

RESUMEN EJECUTIVO

- La clasificación de un sistema como de alto, limitado o mínimo riesgo bajo el AI Act no determina su criticidad para la inocuidad alimentaria.
- Todo sistema de IA que intervenga en un peligro significativo debe incorporarse formalmente al análisis APPCC, al control de cambios y al sistema documental.
- La validación del algoritmo por el proveedor no sustituye la validación local del sistema completo en producto, proceso, equipos, personal y condiciones reales.
- La exactitud global es insuficiente: deben analizarse sensibilidad, falsos negativos, rendimiento por subgrupos, incertidumbre, deriva y comportamiento ante fallos.
- Un sistema autónomo no debe constituir una barrera única invisible. Las funciones críticas requieren redundancia, modos seguros de fallo y capacidad real de intervención humana.
- La empresa debe poder reconstruir qué versión del modelo estaba activa, qué datos recibió, qué salida generó, quién actuó y qué producto quedó afectado.
- BRCGS, IFS y FSSC no contienen todavía un capítulo específico sobre IA industrial; sus requisitos de APPCC, validación, equipos, datos, cambios, competencia, trazabilidad y contingencia proporcionan, no obstante, una base auditora suficiente.
- La responsabilidad del operador alimentario no se transfiere a la máquina ni al proveedor tecnológico.

ABREVIATURAS

Sigla	Significado
AI Act	Reglamento (UE) 2024/1689 sobre inteligencia artificial
APPCC / HACCP	Análisis de Peligros y Puntos de Control Crítico
BPH / GHP	Buenas prácticas de higiene
CCP / PCC	<i>Critical Control Point</i> / Punto de Control Crítico
DQ	<i>Design Qualification</i> / Cualificación del diseño
FSMS / SGIA	<i>Food Safety Management System</i> / Sistema de gestión de la inocuidad alimentaria
ICAA	Índice de Criticidad Algorítmica Alimentaria
IQ	<i>Installation Qualification</i> / Cualificación de la instalación
ML	<i>Machine learning</i> / aprendizaje automático
OQ	<i>Operational Qualification</i> / Cualificación operacional
OPRP / PPRO	<i>Operational Prerequisite Programme</i> / Programa de prerequisites operativo
PQ	<i>Performance Qualification</i> / Cualificación del rendimiento
XAI	<i>Explainable Artificial Intelligence</i> / inteligencia artificial explicable

ÍNDICE

1. Introducción	4	14. Lista de comprobación APPCC	10
2. Dos conceptos de riesgo	4	15. Conclusiones doctrinales	12
3. El APPCC como arquitectura verificable	6	16. Casos prácticos	12
4. Formas de utilización de la IA	6	17. Matriz de criticidad ICAA	13
5. Nuevos peligros algorítmicos	6	18. Protocolo formal de validación	15
6. Principio rector	7	19. Evidencias para auditorías	17
7. Metodología de integración	7	20. Conclusión operativa	19
8. IA en un punto de control crítico	8	Anexo A. Ficha ICAA	19
9. Validación científica	9	Anexo B. Protocolo de validación	19
10. Supervisión humana	9	Anexo C. Cambios y revalidación	22
11. Responsabilidad del operador	9	Anexo D. Incidencias algorítmicas	22
12. Requisitos contractuales	10	Anexo E. Auditoría interna	23
13. Documentación mínima	10	Bibliografía y fuentes	24

ÍNDICE DE TABLAS Y FIGURAS

El documento contiene tres figuras conceptuales, matrices de clasificación y tablas operativas. Las tablas están diseñadas para ser copiadas o adaptadas a procedimientos internos, auditorías y expedientes de validación.

1. Introducción: digitalizar el APPCC no significa reforzarlo

La industria alimentaria está adoptando sistemas capaces de analizar grandes volúmenes de datos procedentes de sensores, cámaras, equipos de laboratorio, LIMS, ERP, MES, registros de producción, controles ambientales y cadenas logísticas. La inteligencia artificial puede reconocer patrones que una supervisión convencional difícilmente detectaría, anticipar desviaciones, identificar anomalías en tiempo real y optimizar el uso de recursos.

Estas capacidades ofrecen oportunidades indudables, pero existe una tendencia preocupante a equiparar automáticamente digitalización con mejora del control. La incorporación de un algoritmo no hace que un proceso sea más seguro por sí misma. Puede introducir nuevas vulnerabilidades si el sistema funciona con datos incompletos, sensores mal calibrados, modelos no validados, cambios de proceso no comunicados, interfaces confusas o criterios de decisión opacos.

La pregunta correcta no es si el modelo supera a una persona en una demostración, sino si puede demostrarse que funciona de forma suficientemente fiable en las condiciones reales, variables y potencialmente adversas de la instalación alimentaria.

El APPCC es una arquitectura preventiva de razonamiento y control. Obliga a relacionar cada peligro significativo con medidas de control concretas, límites verificables, procedimientos de vigilancia, acciones correctivas, validación y verificación [8–10]. No es un programa informático ni un conjunto de formularios.

El Reglamento (CE) n.º 852/2004 exige que los operadores mantengan procedimientos permanentes basados en los principios del APPCC y confirma que la responsabilidad primaria de la seguridad alimentaria corresponde al operador [2]. Esa responsabilidad no desaparece cuando una función se automatiza o se externaliza. El Reglamento (CE) n.º 178/2002 obliga al operador a asegurar el cumplimiento de la legislación alimentaria en las actividades bajo su control [1].

Cadena de control de un sistema IA integrado en APPCC



La validación debe cubrir el sistema completo: sensores, datos, algoritmo, interfaz, personas, actuadores y trazabilidad.

Figura 1. Cadena de control que debe validarse cuando la IA se integra en el APPCC.

2. Dos conceptos de riesgo que no deben confundirse

2.1. Riesgo regulatorio conforme al AI Act

El Reglamento (UE) 2024/1689 establece un marco horizontal basado en categorías de riesgo y obligaciones diferenciadas. Los sistemas de alto riesgo quedan sujetos, entre otras exigencias, a gestión de riesgos, gobernanza de datos, documentación técnica, registro de actividad, transparencia, supervisión humana, precisión, robustez y ciberseguridad [6]. La calificación depende de la finalidad prevista y de las categorías legales, no de una apreciación intuitiva de que una tecnología resulte “importante”.

Muchas aplicaciones industriales en fábricas de alimentos no serán automáticamente sistemas de alto riesgo conforme al AI Act. Un modelo que anticipe una desviación térmica o clasifique defectos puede quedar fuera de esas categorías, según su configuración, integración y finalidad prevista. Esta conclusión jurídica no autoriza a tratarlo como irrelevante para la inocuidad.

2.2. Riesgo alimentario conforme al APPCC

La criticidad alimentaria depende de las consecuencias que un error puede producir sobre un peligro biológico, químico, físico o alérgico. Un sistema que determine si un tratamiento térmico ha sido suficiente, interprete una señal de contaminación, acepte un lote o modifique un parámetro puede tener relevancia extraordinaria, aunque no sea jurídicamente de alto riesgo.

La ausencia de clasificación como sistema de alto riesgo conforme al AI Act no equivale a ausencia de criticidad dentro del APPCC.

2.3. Matriz de doble clasificación

Dimensión	Pregunta principal	Resultados posibles
Clasificación AI Act	¿El sistema pertenece a una categoría regulada o de alto riesgo por su finalidad prevista?	Alto riesgo; obligaciones de transparencia; riesgo limitado o mínimo.
Clasificación alimentaria	¿Puede un error comprometer la prevención, detección o control de un peligro significativo?	Crítico; relevante; auxiliar; sin impacto directo.

Doble clasificación del riesgo: AI Act y APPCC

CRITICIDAD APPCC

Riesgo AI Act bajo / Criticidad APPCC baja Gobierno ordinario y control documental	Riesgo AI Act alto / Criticidad APPCC baja Cumplimiento digital reforzado, impacto alimentario indirecto
Riesgo AI Act bajo / Criticidad APPCC alta Validación alimentaria reforzada aunque no sea “alto riesgo” legal	Riesgo AI Act alto / Criticidad APPCC alta Máxima exigencia jurídica, técnica y operativa

CLASIFICACIÓN AI ACT

Clasificación jurídica y criticidad alimentaria son análisis independientes y acumulativos.

Figura 2. Clasificación jurídica y criticidad alimentaria como análisis independientes.

3. El APPCC como arquitectura de decisión verificable

Los Principios Generales de Higiene de los Alimentos del Codex CXC 1-1969 articulan la identificación de peligros, la determinación de PCC, los límites críticos, la vigilancia, las medidas

correctivas, la validación, la verificación y los registros [9]. La Comunicación 2022/C 355/01 de la Comisión Europea desarrolla la implantación de sistemas de gestión de seguridad alimentaria basados en BPH y APPCC [8].

La inteligencia artificial no constituye un octavo principio del APPCC. Puede participar en la identificación preliminar de peligros, análisis de tendencias, vigilancia de parámetros, detección de anomalías, predicción de desviaciones, recomendación de acciones o verificación. Pero debe quedar subordinada a la lógica preventiva y a criterios científicamente sustentados.

Un modelo no debe declarar por sí solo que un peligro es insignificante. Tampoco puede fijar un límite crítico porque una correlación estadística optimice el rendimiento productivo. Los límites críticos separan condiciones aceptables e inaceptables para la seguridad y deben apoyarse en evidencia normativa, científica, técnica o experimental [9–11].

4. Formas de utilización de la inteligencia artificial dentro del APPCC

Nivel	Función	Ejemplos	Control mínimo
IA informativa	Organiza, resume o localiza información sin decidir sobre la inocuidad.	Resúmenes de auditoría; búsqueda documental; clasificación de registros.	Control de fuentes, confidencialidad, revisión humana y versiones.
IA de apoyo	Emite predicción o recomendación; la decisión final es humana.	Riesgo microbiológico; proveedores; vida útil; priorización de muestras.	Validación, límites de uso, explicación suficiente y revisión competente.
IA de vigilancia	Participa directamente en la monitorización de una medida de control, PPRO o PCC.	Visión artificial; perfiles térmicos; variables ambientales.	Validación del sistema completo, alarmas, registros y contingencia.
IA de control autónomo	Modifica parámetros, desvía producto, detiene la línea o ejecuta acciones.	Rechazo automático; ajuste de proceso; liberación o bloqueo.	Redundancia, modo seguro de fallo, intervención manual y trazabilidad total.

La supervisión humana no puede consistir en una aceptación rutinaria. El responsable debe conocer la finalidad, las limitaciones, las señales de funcionamiento anormal y las circunstancias que obligan a ignorar o detener el sistema. Las guías generales de gestión de riesgos de IA destacan la necesidad de gobernar, mapear, medir y gestionar los riesgos a lo largo del ciclo de vida [19, 20, 26].

5. Los nuevos peligros algorítmicos

5.1. Datos no representativos

Un modelo entrenado durante periodos estables puede degradarse ante estacionalidad, nuevos proveedores, reformulaciones, cambios de envase, velocidad, equipos o condiciones higiénicas raras. La precisión media puede ocultar fallos precisamente en los casos de mayor riesgo.

5.2. Errores de etiquetado del conjunto de entrenamiento

Si la verdad de referencia es defectuosa, el sistema aprenderá relaciones incorrectas. La clasificación realizada por inspectores humanos debe someterse, cuando sea relevante, a criterios objetivos, consenso y análisis de concordancia.

5.3. Falsos negativos

En seguridad alimentaria el falso negativo suele ser más grave que el falso positivo. La exactitud global debe desagregarse en sensibilidad, especificidad, valores predictivos, calibración, rendimiento por subgrupos y tasas de error cercanas al límite de control.

5.4. Deriva del modelo

La relación entre datos de entrada y fenómeno puede cambiar por materias primas, desgaste de sensores, flora ambiental, prácticas de limpieza, clima, velocidad o formulación. La deriva puede degradar el rendimiento sin una avería visible [35–37].

5.5. Automatización complaciente

La repetición de resultados aparentemente correctos puede generar confianza excesiva y convertir la supervisión en ratificación formal. La interfaz y la formación deben combatir el sesgo de automatización.

5.6. Pérdida de trazabilidad

Si no puede reconstruirse la versión activa, los datos recibidos, el umbral, la salida, la persona que revisó y la decisión adoptada, no puede demostrarse que el control funcionó.

5.7. Dependencia del proveedor

El proveedor puede modificar modelos, retirar funcionalidades, impedir exportar registros o dejar de prestar servicio. La dependencia tecnológica debe tratarse como riesgo de continuidad del sistema de inocuidad.

5.8. Manipulación y ciberataques

La alteración de sensores, cámaras, parámetros o bases de datos puede modificar conclusiones sin producir un fallo visible. Cuando la IA interviene en un control alimentario, la integridad del dato se convierte en condición de seguridad del producto [25, 43, 44].

6. Principio rector: la IA debe reforzar una barrera, no convertirse en una barrera única e invisible

La organización debe determinar si el sistema actúa como fuente de información, alerta complementaria, medida de vigilancia, componente de una medida de control, control autónomo o herramienta de verificación. En fases iniciales, el modelo debería operar como barrera adicional junto al procedimiento existente.

La eliminación de una barrera previa solo puede justificarse después de una comparación suficiente con métodos convencionales, pruebas de desafío, revisión manual, análisis de discrepancias y evidencia de estabilidad. La demostración comercial del proveedor no equivale a validación en planta.

7. Metodología para integrar IA en el sistema APPCC

Fase 1. Definir la finalidad prevista

Describir exactamente qué hace, qué no hace, qué peligro o parámetro aborda, dónde se utiliza, quién emplea la salida, qué decisiones se derivan y qué condiciones quedan fuera del alcance.

Fase 2. Ubicarlo en el diagrama de flujo

Identificar instalación, entradas de datos, conexiones, operaciones anteriores y posteriores, destino del producto rechazado, medidas alternativas e indisponibilidad. Verificar físicamente la ubicación.

Fase 3. Analizar modos de fallo

Contemplar ausencia o incorrección de datos, sensores descalibrados, iluminación, conectividad, latencia, versión equivocada, umbral incorrecto, saturación, manipulación, fallo del actuador o alarmas ignoradas.

Fase 4. Establecer requisitos de rendimiento

Definir sensibilidad mínima, máximo de falsos negativos, especificidad, repetibilidad, reproducibilidad, tiempo de respuesta, disponibilidad, rango de operación y frecuencia de comprobación.

Fase 5. Validar antes de implantar

Utilizar producto, equipos, velocidad, variabilidad, escenarios desfavorables, muestras positivas y negativas y personal habitual. Evitar depender exclusivamente de evidencia del fabricante.

Fase 6. Implantar en paralelo

Comparar la IA con el procedimiento existente para detectar discrepancias, ajustar umbrales, evaluar la respuesta humana y verificar los registros.

Fase 7. Aprobar formalmente

Documentar la decisión del equipo competente con participación de seguridad alimentaria, calidad, producción, mantenimiento, IT, ciberseguridad, regulación y dirección técnica.

Fase 8. Integrar la vigilancia

Definir responsable, frecuencia, criterios, alarmas, escalado, registros, resultados dudosos e indisponibilidad.

Fase 9. Definir acciones correctivas

Controlar producto afectado, delimitar periodos, bloquear lotes, activar alternativas, investigar causa, reparar, revalidar y comunicar.

Fase 10. Verificar periódicamente

Realizar pruebas de desafío, revisión de falsos negativos, comparación independiente, auditoría de versiones, sensores, tendencias y alarmas anuladas.

Fase 11. Gestionar los cambios

Evaluar actualizaciones, reentrenamientos, formulaciones, materias primas, envases, velocidades, sensores, software, ubicación, iluminación y umbrales.

Fase 12. Retirar de forma controlada

Prever procedimiento alternativo, acceso a datos históricos, exportación de registros, revocación de accesos y reevaluación APPCC.

8. ¿Puede utilizarse inteligencia artificial en un punto de control crítico?

La respuesta no debe ser una prohibición absoluta ni una aceptación indiscriminada. La IA puede participar en la vigilancia o el control de un PCC si la finalidad está definida; el límite crítico se sustenta

en evidencia independiente; las variables son adecuadas; el rendimiento ha sido validado localmente; la tasa de falsos negativos es compatible con el nivel de protección; existe trazabilidad, supervisión, modo seguro de fallo, alternativa y revalidación.

8.1. El límite crítico no es el umbral algorítmico

El límite crítico separa aceptabilidad e inaceptabilidad respecto del control del peligro. El umbral algorítmico determina cuándo el modelo clasifica, alerta o actúa. Un algoritmo puede alertar de forma anticipada, pero esa predicción no sustituye la demostración del cumplimiento del límite salvo validación específica.

8.2. Mantener mecanismos deterministas de seguridad

En procesos de alta criticidad deben considerarse controles deterministas independientes: termostatos, válvulas, relés, enclavamientos, temporizadores, alarmas redundantes, detectores convencionales o parada segura. Las buenas prácticas de seguridad funcional y de diseño de sistemas de mando resultan relevantes cuando la IA ejecuta acciones físicas [42].

9. Validación científica del sistema

La validación de medidas de control se diferencia de la vigilancia y de la verificación. Debe obtener evidencia de que la medida, aplicada correctamente, es capaz de controlar el peligro con el resultado especificado [10]. Para IA, la validación debe responder a cinco preguntas:

1. ¿Detecta o estima realmente la variable que afirma detectar?
2. ¿Funciona en la población real de productos, lotes, turnos y condiciones?
3. ¿Mantiene rendimiento en los casos difíciles y cercanos al límite?
4. ¿Se mantiene estable durante un periodo suficiente?
5. ¿Falla de forma detectable y segura?

La validación debe utilizar un conjunto independiente del empleado en entrenamiento o ajuste. Debe documentar origen, selección, representatividad, exclusiones, datos faltantes, balance, subgrupos, calidad de referencia y posibles sesgos. En modelos de vida útil y microbiología predictiva, la IA puede mejorar la selección de escenarios y el análisis de datos, pero no elimina la necesidad de evidencia experimental cuando esta sea necesaria [30–34].

10. Supervisión humana efectiva

La *AI Act* exige supervisión humana para sistemas jurídicamente de alto riesgo [6]. En alimentación, la necesidad debe determinarse también por la criticidad material. La persona designada debe comprender finalidad y limitaciones, identificar anomalías, cuestionar resultados, detener el proceso, activar el método alternativo y disponer de autoridad y formación.

Pulsar “aceptar” no constituye supervisión humana efectiva.

La interfaz debería mostrar, cuando sea útil, nivel de confianza, calidad del dato, advertencias, condiciones fuera de rango, versión del modelo, momento del cálculo y necesidad de revisión. Las técnicas de explicabilidad como LIME o SHAP pueden ser útiles, pero no sustituyen la validación empírica ni garantizan causalidad [38, 39].

11. Responsabilidad del operador alimentario

La empresa no puede exonerarse alegando que el software era comercial, estaba certificado, procedía de un proveedor reconocido, había sido entrenado con millones de datos o adoptaba decisiones automáticamente. La diligencia propia comprende selección, aptitud para el uso, integración, vigilancia, mantenimiento y actuación ante desviaciones [1, 2].

Debe distinguirse entre responsabilidad por diseño, datos, integración, uso, supervisión, mantenimiento y decisión final. La Directiva (UE) 2024/2853 moderniza el régimen de responsabilidad por productos defectuosos e incluye el software dentro del concepto de producto; su interacción con la responsabilidad alimentaria y contractual exigirá análisis caso por caso [7].

12. Requisitos contractuales para proveedores de IA

Materia contractual	Contenido mínimo
Finalidad y alcance	Uso autorizado, productos, líneas, condiciones y exclusiones.
Rendimiento	Métricas, umbrales, condiciones de ensayo, disponibilidad y tiempos de respuesta.
Datos	Fuentes, calidad, propiedad, uso para reentrenamiento, exportación y conservación.
Cambios	Autorización previa, notificación, versiones, revalidación y reversibilidad.
Ciberseguridad	Accesos, vulnerabilidades, actualizaciones, copias, incidentes y recuperación.
Trazabilidad	Registros, logs, sello temporal, explicación disponible e identificación de versión.
Auditoría	Derecho a evidencias, pruebas, subcontratistas y cooperación con auditores o autoridades.
Continuidad	Niveles de servicio, soporte, salida, transferencia de datos y plan de contingencia.
Responsabilidad	Asignación de obligaciones, seguros, cooperación en retiradas e indemnidad contractual.

Debe prohibirse, salvo autorización documentada, la modificación automática de modelos, umbrales o funcionalidades que afecten a la seguridad alimentaria. La empresa debe conocer si el modelo permanece bloqueado tras la validación o aprende durante el uso.

13. Documentación mínima exigible

- Descripción y finalidad del sistema.
- Clasificación AI/ Act e ICAA.
- Responsable interno y proveedor.
- Versión, fuentes y flujo de datos.
- Análisis de modos de fallo.
- Protocolo e informe de validación.
- Criterios de aceptación y limitaciones.
- Vigilancia, acciones correctivas y contingencia.
- Formación, accesos y ciberseguridad.
- Historial de cambios, incidentes, verificaciones y revalidaciones.
- Aprobación, suspensión y retirada.

La deuda técnica asociada a modelos, dependencias, datos y configuración puede crecer de forma invisible si no se mantiene documentación y control de ciclo de vida [40, 41].

14. Lista de comprobación para el equipo APPCC

N.º	Pregunta	Sí	No	Evidencia / acción
1	¿Sabemos exactamente qué función realiza?	☐	☐	
2	¿Hemos identificado el peligro relacionado?	☐	☐	
3	¿Conocemos los datos utilizados y su calidad?	☐	☐	
4	¿Existe una verdad de referencia fiable?	☐	☐	
5	¿El conjunto de validación es independiente y representativo?	☐	☐	

6	¿Se ha evaluado la tasa de falsos negativos?	☐	☐	
7	¿Se ha probado en condiciones reales y adversas?	☐	☐	
8	¿Se conocen las limitaciones y condiciones excluidas?	☐	☐	
9	¿Sabemos qué versión está instalada?	☐	☐	
10	¿Puede actualizarse sin autorización?	☐	☐	
11	¿Existe registro de cada decisión relevante?	☐	☐	
12	¿Puede reconstruirse una incidencia?	☐	☐	
13	¿Existe supervisión humana efectiva?	☐	☐	
14	¿El personal puede detener o anular el sistema?	☐	☐	
15	¿Existe un método alternativo?	☐	☐	
16	¿El fallo conduce a una condición segura?	☐	☐	
17	¿Se han evaluado riesgos de ciberseguridad?	☐	☐	
18	¿El proveedor debe comunicar cambios e incidentes?	☐	☐	
19	¿Se verifica periódicamente el rendimiento?	☐	☐	
20	¿Existe criterio documentado de revalidación?	☐	☐	

15. Conclusiones doctrinales

La inteligencia artificial puede reforzar la prevención, detectar señales débiles, procesar variables simultáneas y anticipar desviaciones. También puede crear una falsa sensación de control. El principal peligro no es que la IA se equivoque —todos los sistemas presentan error—, sino que la empresa desconozca dónde, cuándo, por qué y con qué consecuencias puede equivocarse.

Deben abandonarse tres ideas simplificadoras: que una tecnología avanzada es necesariamente más segura; que la validación del proveedor sirve para cualquier instalación; y que la clasificación del AI Act determina la criticidad alimentaria.

Ningún sistema de IA debe asumir una función relevante para la seguridad alimentaria sin que la empresa pueda demostrar su finalidad, rendimiento, límites, trazabilidad, supervisión y comportamiento en caso de fallo.

16. Casos prácticos de integración

La criticidad depende de la función, del peligro, de la posición en el proceso y de las barreras independientes. Los siguientes casos muestran cómo debe realizarse el análisis material.

16.1. Visión artificial para detección de cuerpos extraños

Las cámaras convencionales, hiperespectrales, infrarrojas o de rayos X, combinadas con algoritmos, pueden detectar fragmentos de plástico, vidrio, piedras, insectos, defectos de integridad, contaminación visible o envases incorrectos. El sistema puede limitarse a alertar o activar un rechazo automático.

Configuración	Función en el sistema
Clasificación estética	Control de calidad.
Detección complementaria	Medida de apoyo.
Sustitución de inspección manual	Medida de vigilancia.
Rechazo automático	Componente de una medida de control.
Única barrera frente a peligro físico	Posible PCC u otra medida crítica.

La validación debe cubrir contaminantes de materiales, tamaños, orientaciones y posiciones diferentes; superficies irregulares; iluminación; condensación; vibración; velocidad; suciedad; superposición; cambios de formato, color y humedad. BRCGS Issue 9 contempla expresamente la justificación, localización, validación y pruebas de equipos de detección de cuerpos extraños, incluida la

clasificación óptica [13, 14]. FSSC v7 exige evaluación de riesgo y procedimientos documentados para equipos de detección [17].

Los criterios deben incluir sensibilidad por contaminante, límite de detección, falsos negativos, rechazos incorrectos, tiempo de respuesta, eficacia de expulsión, destino del producto rechazado, detección de fallo y pérdida de comunicación.

16.2. Predicción de desviaciones en tratamientos térmicos

Un modelo puede combinar temperatura inicial, caudal, presión, viscosidad, tamaño de partícula, medio calefactor, ensuciamiento y comportamiento de válvulas para predecir una desviación. Debe distinguirse entre alerta predictiva, estimación de variable, control automático y sustitución de la medición directa.

Una predicción de cumplimiento no equivale a evidencia de que el límite crítico se alcanzó. La sustitución de mediciones físicas por estimaciones requiere validación específica y arquitectura en capas: sensor calibrado, control determinista, alarma independiente, modelo predictivo, operador, derivación de producto y registro. IFS *Food 8* exige límites críticos validados, vigilancia capaz de detectar pérdida de control, registros y revalidación ante modificaciones [15, 16].

16.3. Control ambiental microbiológico

La IA puede analizar resultados ambientales, zonas, turnos, humedad, flujos, limpiezas, mantenimientos, drenajes y resultados de producto para identificar tendencias, persistencia y dispersión. Su utilidad no consiste en declarar una zona libre de patógenos, sino en priorizar puntos, detectar patrones e intensificar investigaciones.

Existe riesgo de circularidad si el modelo aprende solo de los puntos ya muestreados y perpetúa los puntos ciegos. La ausencia de positivos donde no se muestrea no es evidencia de ausencia de contaminación. El resultado no debe reducir automáticamente frecuencias, eliminar puntos, cerrar investigaciones o liberar producto.

16.4. Predicción de vida útil

Los modelos pueden integrar pH, actividad de agua, conservantes, envase, tratamiento, carga inicial, microbiota, temperatura y datos sensoriales. Debe separarse vida útil comercial de vida útil segura. Un modelo sensorialmente preciso puede no ser adecuado para predecir patógenos.

La extrapolación entre formulaciones, proveedores, procesos, envases, temperaturas o instalaciones requiere validación. La IA puede seleccionar escenarios críticos, diseñar *challenge tests* y comparar alternativas, pero no sustituye universalmente los estudios microbiológicos o de vida útil [3, 31–34].

16.5. Verificación de etiquetado y alérgenos

La visión y el procesamiento de texto pueden comprobar correspondencia producto-etiqueta, alérgenos, lote, fecha, idioma, ingredientes, código de barras y versión gráfica. El peligro puede residir en la base maestra, una versión obsoleta, cambios no actualizados, formatos similares o fallo del rechazo.

El sistema debe comparar con una fuente maestra controlada. El Reglamento (UE) 1169/2011 establece las responsabilidades de información alimentaria y los requisitos de declaración de alérgenos [4]. BRCGS, IFS y FSSC exigen controles de etiquetado, cambios, verificación y métodos alternativos cuando falla la comprobación en línea [13–17].

16.6. Homologación de proveedores y materias primas

Un modelo puede combinar analíticas, incidencias, auditorías, alertas, certificaciones, origen y vulnerabilidad al fraude. Debe evitar penalizar por escasez de datos, confundir certificación con ausencia

de riesgo, atribuir causalidad a correlaciones geográficas o interpretar ausencia de información como bajo riesgo. La IA debe priorizar auditorías y muestreos; la aprobación o exclusión de proveedores críticos requiere criterios documentados y revisión competente.

17. Matriz APPCC–IA de criticidad algorítmica

Se propone el Índice de Criticidad Algorítmica Alimentaria (ICAA). Es una herramienta interna y no constituye una clasificación legal ni sustituye el análisis de peligros.

Variable	Escala	Criterio resumido
S. Severidad	1–5	Desde ausencia de impacto hasta daño grave, brote o exposición alérgica.
I. Influencia	0–4	Desde función informativa hasta ejecución autónoma.
D. Detectabilidad	0–4	Desde error evidente hasta no detectable antes del consumo.
B. Barrera independiente	0–3	Desde barrera eficaz hasta ausencia de redundancia.
E. Exposición	1–4	Desde ensayo limitado hasta múltiples centros o gran volumen.

$$ICAA = S + I + D + B + E$$

ICAA	Clase	Interpretación
2–6	I	Sistema auxiliar.
7–10	II	Sistema relevante.
11–15	III	Sistema crítico.
16–20	IV	Sistema esencial o autónomo de máxima criticidad.

Reglas de escalado obligatorio:

1. Todo sistema que intervenga directamente en la vigilancia de un PCC será, como mínimo, Clase III.
2. Todo sistema que pueda liberar automáticamente producto será, como mínimo, Clase III.
3. Todo sistema que modifique autónomamente un parámetro crítico será Clase IV.
4. Todo sistema cuya salida pueda ocultar un peligro alérgico será, como mínimo, Clase III.
5. Todo sistema utilizado como única barrera frente a un peligro significativo será Clase IV.
6. Un sistema no validado localmente será no aprobable, con independencia de la puntuación.
7. La falta de acceso a registros, versiones o datos invalida su uso crítico.

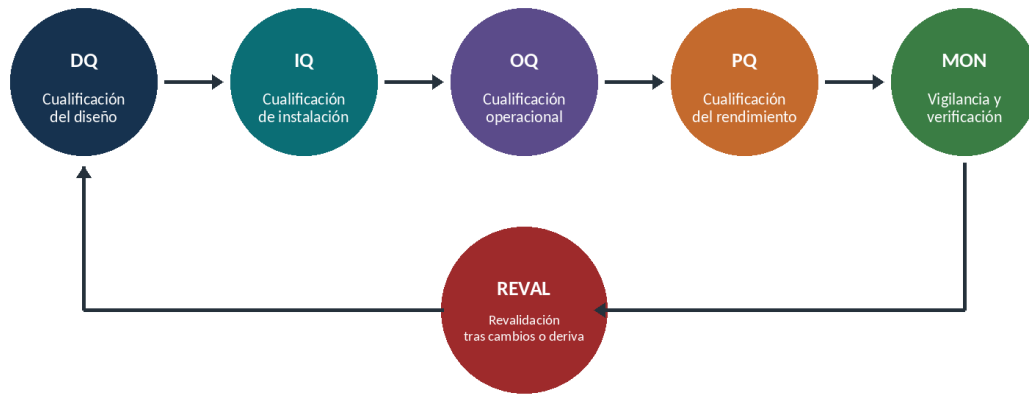
Requisito	Clase I	Clase II	Clase III	Clase IV
Inventario y responsable	Sí	Sí	Sí	Sí
Validación local	Según uso	Sí	Sí	Sí, independiente
Operación en paralelo	No	Recomendada	Inicialmente obligatoria	Obligatoria
Falsos negativos	Según uso	Sí	Reforzada	Por escenario
Registro individual	No siempre	Según riesgo	Sí	Sí
Supervisión humana	General	Específica	Definida y efectiva	Permanente/autoridad
Contingencia	Básica	Documentada	Probada	Probada y redundante
Pruebas de fallo	No siempre	Sí	Sí	Exhaustivas
Ciberseguridad	Básica	Sí	Reforzada	Reforzada
Revalidación	Según impacto	Sí	Sí	Antes de re-uso

Aplicación	S	I	D	B	E	Total	Clase
Resúmenes de auditoría	1	1	1	0	2	5	I
Priorización de proveedores	3	2	2	1	3	11	III
Predicción de vida útil	4	2	3	1	3	13	III
Visión complementaria	4	2	2	0	3	11	III
Visión como única barrera	5	4	4	3	4	20	IV
Alerta de desviación térmica	5	2	2	0	3	12	III
Control térmico autónomo	5	4	4	3	4	20	IV

18. Protocolo formal de validación

La validación debe cubrir el sistema sociotécnico completo: datos, sensores, modelo, interfaces, personas, decisiones, actuadores, registros y contingencias. No debe confundirse la validación del algoritmo por el proveedor con la validación del uso específico en planta.

Ciclo de vida de validación y control del sistema IA



La aprobación no cierra el proceso: el rendimiento debe mantenerse bajo control durante toda la vida útil.

Figura 3. Ciclo DQ–IQ–OQ–PQ, vigilancia y revalidación.

18.1. Contenido del protocolo

Identificación, versión, finalidad, productos, peligro, diagrama de flujo, ICAA, responsables, datos, método de referencia, hipótesis, limitaciones, métricas, criterios, diseño experimental, escenarios adversos, plan estadístico, discrepancias, contingencia y aprobación.

18.2. Cualificación del diseño — DQ

Confirma que la tecnología, rango, velocidad, ambiente, datos, registros, arquitectura, alarmas, documentación, bloqueo de versión y modo manual son adecuados antes de instalar.

18.3. Cualificación de la instalación — IQ

Verifica hardware, software, versión, sensores, conexiones, red, iluminación, sincronización, copias, accesos, configuración, umbrales, PLC/MES/LIMS/ERP, alarmas, rechazo y calibración.

18.4. Cualificación operacional — OQ

Prueba entradas válidas e inválidas, límites, pérdida de señal, latencia, reinicio, alarmas, bloqueo, recuperación, modo manual y exportación de registros.

18.5. Cualificación del rendimiento — PQ

Demuestra desempeño en producción real con turnos, operarios, lotes, proveedores, formatos, velocidades, estaciones, limpiezas, arranques, paradas y producción prolongada.

18.6. Conjunto de validación

Debe ser independiente del entrenamiento y documentar origen, periodo, selección, representatividad, exclusiones, faltantes, balance, subgrupos, referencia y sesgos.

18.7. Métricas

Seleccionar sensibilidad, especificidad, falsos negativos y positivos, valores predictivos, calibración, F1, errores, sesgo, repetibilidad, reproducibilidad, latencia, disponibilidad y rechazo según el daño relevante.

18.8. Criterios de aceptación

Fijarlos antes del estudio, vinculados al peligro, por subgrupos, con incertidumbre, límites de falsos negativos y comportamiento ante fallos. No existe un porcentaje universal.

18.9. Pruebas de desafío

Incluir valores cercanos al límite, productos atípicos, interferencias, sensores degradados, lentes sucias, pérdida parcial de datos, saturación, entradas fuera de distribución y fallo del actuador.

18.10. Seguridad funcional

Comprobar alarma, identificación de producto, persistencia del estado de fallo, conservación de registros, modo manual, reinicio controlado, recuperación autorizada y rechazo físico.

18.11. Factores humanos

Evaluar comprensión, respuesta, probabilidades, automatización complaciente, fatiga por alarmas, autoridad, instrucciones, turno nocturno y personal sustituto.

18.12. Operación en paralelo

Obligatoria inicialmente en clases III y IV durante un periodo que capture variabilidad, discrepancias, fallos poco frecuentes y actuación humana.

18.13. Informe final

Debe indicar finalidad, alcance, versión, datos, método, resultados, incertidumbre, discrepancias, limitaciones, condiciones autorizadas y excluidas, acciones y firmas.

18.14. Revalidación

Se activa por actualización, reentrenamiento, umbral, sensor, iluminación, traslado, nueva línea, formulación, envase, velocidad, proveedor, deriva, incidente, retirada, reclamación, finalidad o cambio normativo.

Conclusión correcta de validación: “Sistema validado para la finalidad, productos, formatos, velocidades, condiciones, versión y umbrales descritos en el informe”.

19. Evidencias para auditorías BRCGS, IFS y FSSC 22000

La tabla siguiente no constituye una equivalencia oficial. Es una matriz interpretativa de preparación de auditoría que conecta la gestión de IA con requisitos existentes de seguridad alimentaria, calidad, equipos, información documentada, cambio y competencia.

Área	Evidencia IA	BRCGS Issue 9	IFS Food 8	FSSC 22000 V7
Inventario y gobierno	Aplicaciones, propietario, finalidad, versión, ICAA, política y aprobación.	Compromiso, responsabilidades, sistema documentado.	Gobierno, responsabilidades, documentación.	ISO 22000 y requisitos de gestión.
Integración APPCC	Diagrama, peligro, función y análisis de fallo.	Sección 2: plan de seguridad alimentaria.	2.2–2.3: plan APPCC.	ISO 22000: análisis de peligros y control.
Validación	Protocolo, datos, criterios, resultados, aprobación.	Validación APPCC, equipos y vida útil según uso.	2.3.8; 2.3.11; 5.3.	ISO 22000 y requisitos adicionales.
Revalidación	Cambios, deriva, incidentes y evaluación de impacto.	Revisión y validación de cambios.	2.2.1.4; 2.3.11.1; 5.3.5.	Gestión del cambio y equipos.
Documentos y registros	Versión, integridad, acceso, copias, sello temporal.	3.2–3.3.	2.1.2 y registros.	Información documentada ISO 22000.
Datos y sensores	Fuentes, calibración, calidad, trazabilidad.	6.4 y equipos de medición.	5.4 y equipo.	PRP y requisitos de equipos.
Cuerpos extraños	Riesgo, sensibilidad, pruebas, rechazo.	4.10.	5.2–5.4 según uso.	Requisito adicional de detección.
Etiquetado/alérgenos	Maestro, versión, prueba y método manual.	6.2.4 y etiquetado.	Etiquetado y parámetros.	Control de impresión/etiquetado.
Vigilancia PCC	Método, frecuencia, alarmas y registros.	Plan APPCC.	2.3.9.	Control de PCC/PPRO.
Acciones correctivas	Producto, bloqueo, investigación y restablecimiento.	2.11 y 3.7.	2.3.10 y no conformidades.	ISO 22000.
Fallo y contingencia	Simulación, alternativa, recuperación.	Continuidad y equipo.	Fallo de equipos y procesos.	Preparación y respuesta.
Proveedor tecnológico	Evaluación, contrato, cambios, incidentes.	3.5 y servicios.	4.4.	2.5.1 y proveedores.
Competencia y supervisión	Formación, autoridad, respuesta, sesgo de automatización.	7.1 y responsabilidades.	3.3 y competencias.	Competencia, cultura y control.
Ciberseguridad	Accesos, red, vulnerabilidades, copias, recuperación.	Registros electrónicos y continuidad.	Protección frente a cambios no autorizados.	Gestión del sistema e incidentes.
Auditoría interna	Muestreo de decisiones, versiones y pruebas.	3.4.	5.1.	ISO 22000 y verificación.
Revisión por dirección	Indicadores, deriva, incidentes y recursos.	1.1 y revisión.	Responsabilidades de dirección.	Revisión y mejora.
Retirada del sistema	Migración, datos, alternativa y reevaluación APPCC.	Cambio y continuidad.	Revisión del APPCC.	Gestión del cambio del SGIA.

19.1. Evidencias que debe solicitar un auditor

- Expediente de aprobación.
- Finalidad prevista y límites de uso.
- Evaluación e integración APPCC.
- Clasificación ICAA.
- Contrato con el proveedor.
- Especificaciones técnicas.
- Versión instalada.
- Datos de validación.
- Método de referencia.
- Resultados por subgrupos.
- Tasa de falsos negativos.
- Pruebas de desafío.
- Pruebas de fallo.
- Registros de alarmas.
- Decisiones humanas.
- Registros de rechazo.
- Mantenimiento.
- Calibración.
- Control de accesos.
- Copias de seguridad.
- Incidentes.
- Cambios.
- Revalidaciones.
- Formación.
- Simulaciones de contingencia.
- Auditorías internas.
- Indicadores de rendimiento.
- Revisión por dirección.

19.2. Preguntas de auditoría

- ¿Qué peligro controla o ayuda a controlar?
- ¿Qué sucede si no detecta la desviación?
- ¿Cuál fue la tasa de falsos negativos?
- ¿Qué versión estaba activa en un lote?
- ¿Quién modifica el umbral?
- ¿Cómo se detecta un sensor descalibrado?
- ¿Qué cambio obliga a revalidar?
- ¿Puede el proveedor actualizar remotamente?
- ¿Cómo se conserva la trazabilidad?
- ¿Qué sucede al perder conexión?
- ¿Cuándo se probó la contingencia?
- ¿Quién puede contradecir al sistema?
- ¿Se comparó con método independiente?
- ¿Se investigaron alarmas ignoradas?
- ¿Se evaluó la deriva?
- ¿Qué producto quedó afectado?
- ¿Puede reconstruirse sin depender del proveedor?

19.3. No conformidades previsibles

- Ausencia de validación local.
- Uso fuera del alcance validado.
- Cambios o actualizaciones no controlados.
- Falta de calibración.
- Ausencia o insuficiencia de registros.
- Imposibilidad de reconstruir decisiones.
- Umbrales sin control de acceso.
- Ausencia de contingencia.
- Personal sin formación suficiente.
- Dependencia excesiva del proveedor.
- Métricas limitadas a exactitud global.
- Falta de evaluación de falsos negativos.
- Reducción de controles sin equivalencia demostrada.
- Sistema activo fuera del APPCC.
- Falta de evaluación del producto tras un fallo.

20. Conclusión operativa

La integración de inteligencia artificial en APPCC debe abordarse como una modificación del sistema de control, no como una compra informática. La empresa debe demostrar una cadena lógica completa desde el peligro hasta el registro. Cada eslabón puede fallar.

Un modelo estadísticamente correcto puede ser inadecuado si recibe un dato erróneo, está mal instalado, utiliza un umbral no autorizado, presenta el resultado de forma confusa, activa un mecanismo defectuoso o impide identificar el producto afectado. La auditoría no debe limitarse al algoritmo: debe evaluar la arquitectura técnica, documental, humana y organizativa.

Cuanto mayor sea la influencia de la IA sobre la aceptación, rechazo, tratamiento o liberación de un alimento, mayor deberá ser la independencia de la validación, la trazabilidad, la redundancia y la capacidad de intervención humana.

ANEXO A. Ficha de evaluación ICAA

Campo	Información / puntuación
Sistema / aplicación	
Proveedor	
Versión	
Finalidad prevista	
Producto / línea	
Peligro relacionado	
Posición en el diagrama de flujo	
Severidad S (1–5)	
Influencia I (0–4)	
Detectabilidad D (0–4)	
Barrera B (0–3)	
Exposición E (1–4)	
ICAA total	
Regla de escalado aplicable	
Clase final	
Responsable	
Fecha y aprobación	

ANEXO B. Plantilla de protocolo de validación

B.1. Objeto y alcance

Contenido requerido	Desarrollo
Describir y aportar evidencia relativa a: objeto y alcance.	

B.2. Equipo responsable

Contenido requerido	Desarrollo
Describir y aportar evidencia relativa a: equipo responsable.	

B.3. Descripción y versión

Contenido requerido	Desarrollo
Describir y aportar evidencia relativa a: descripción y versión.	

B.4. Finalidad y límites de uso

Contenido requerido	Desarrollo
Describir y aportar evidencia relativa a: finalidad y límites de uso.	

B.5. Peligro y función APPCC

Contenido requerido	Desarrollo
Describir y aportar evidencia relativa a: peligro y función APPCC.	

B.6. Datos y verdad de referencia

Contenido requerido	Desarrollo
Describir y aportar evidencia relativa a: datos y verdad de referencia.	

B.7. Diseño experimental

Contenido requerido	Desarrollo
Describir y aportar evidencia relativa a: diseño experimental.	

B.8. Métricas y criterios de aceptación

Contenido requerido	Desarrollo
Describir y aportar evidencia relativa a: métricas y criterios de aceptación.	

B.9. Pruebas de desafío y fallo

Contenido requerido	Desarrollo
Describir y aportar evidencia relativa a: pruebas de desafío y fallo.	

B.10. DQ

Contenido requerido	Desarrollo
Describir y aportar evidencia relativa a: DQ.	

B.11. IQ

Contenido requerido	Desarrollo
Describir y aportar evidencia relativa a: IQ.	

B.12. OQ

Contenido requerido	Desarrollo
Describir y aportar evidencia relativa a: OQ.	

B.13. PQ

Contenido requerido	Desarrollo
Describir y aportar evidencia relativa a: PQ.	

B.14. Operación en paralelo

Contenido requerido	Desarrollo
Describir y aportar evidencia relativa a: operación en paralelo.	

B.15. Resultados y análisis estadístico

Contenido requerido	Desarrollo
Describir y aportar evidencia relativa a: resultados y análisis estadístico.	

B.16. Desviaciones

Contenido requerido	Desarrollo
Describir y aportar evidencia relativa a: desviaciones.	

B.17. Limitaciones

Contenido requerido	Desarrollo
Describir y aportar evidencia relativa a: limitaciones.	

B.18. Plan de vigilancia

Contenido requerido	Desarrollo
Describir y aportar evidencia relativa a: plan de vigilancia.	

B.19. Criterios de revalidación

Contenido requerido	Desarrollo
Describir y aportar evidencia relativa a: criterios de revalidación.	

B.20. Decisión y firmas

Contenido requerido	Desarrollo
Describir y aportar evidencia relativa a: decisión y firmas.	

ANEXO C. Registro de cambios y revalidación

Fecha	Cambio	Motivo	Impacto APPCC	Versión (prev./nueva)	Acción	Revalidación	Aprobación

ANEXO D. Registro de incidencias algorítmicas

Fecha/hora	Lote/línea	Versión	Incidencia	Producto afectado	Decisión	Causa	Cierre

ANEXO E. Guion de auditoría interna

Área	Pregunta	Conforme	Hallazgo / evidencia	Acción / plazo
Gobierno	¿Existe inventario y propietario de cada sistema?	☐ Sí ☐ No		
Finalidad	¿Está definido el uso autorizado y lo que queda fuera de alcance?	☐ Sí ☐ No		
APPCC	¿Se ha incorporado al diagrama, análisis y medidas de control?	☐ Sí ☐ No		
Datos	¿Se conocen fuentes, calidad, sesgos y transformaciones?	☐ Sí ☐ No		
Validación	¿Existe evidencia local e independiente del entrenamiento?	☐ Sí ☐ No		
Rendimiento	¿Se controlan falsos negativos, subgrupos y condiciones límite?	☐ Sí ☐ No		
Versión	¿Puede identificarse la versión activa por lote y fecha?	☐ Sí ☐ No		
Cambios	¿Se bloquean y aprueban actualizaciones y umbrales?	☐ Sí ☐ No		
Supervisión	¿El personal comprende y puede intervenir?	☐ Sí ☐ No		
Contingencia	¿Se ha probado el método alternativo?	☐ Sí ☐ No		
Ciberseguridad	¿Accesos, integridad, copias y recuperación están controlados?	☐ Sí ☐ No		
Proveedor	¿Contrato, incidentes, auditoría y salida están regulados?	☐ Sí ☐ No		
Deriva	¿Existen indicadores y umbrales de revalidación?	☐ Sí ☐ No		
Trazabilidad	¿Puede reconstruirse una decisión completa?	☐ Sí ☐ No		
CAPA	¿Las incidencias se investigan y cierran con eficacia?	☐ Sí ☐ No		

BIBLIOGRAFÍA Y FUENTES

Las referencias normativas se citan en su versión consolidada o en la edición identificada. Las normas ISO y los estándares privados deben consultarse en sus textos oficiales; la referencia bibliográfica no reproduce su contenido protegido.

1. 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. Versión consolidada. [Acceso](#)
2. Parlamento Europeo y Consejo. Reglamento (CE) n.º 852/2004, de 29 de abril de 2004, relativo a la higiene de los productos alimenticios. Versión consolidada. [Acceso](#)
3. Comisión Europea. Reglamento (CE) n.º 2073/2005, de 15 de noviembre de 2005, relativo a los criterios microbiológicos aplicables a los productos alimenticios. Versión consolidada a 1 de julio de 2026. [Acceso](#)
4. Parlamento Europeo y Consejo. Reglamento (UE) n.º 1169/2011, de 25 de octubre de 2011, sobre la información alimentaria facilitada al consumidor. Versión consolidada. [Acceso](#)
5. Parlamento Europeo y Consejo. Reglamento (UE) 2017/625, de 15 de marzo de 2017, relativo a los controles oficiales y otras actividades oficiales. [Acceso](#)
6. 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. [Acceso](#)
7. Parlamento Europeo y Consejo. Directiva (UE) 2024/2853, de 23 de octubre de 2024, sobre responsabilidad por los daños causados por productos defectuosos. [Acceso](#)
8. Comisión Europea. Comunicación 2022/C 355/01 sobre la aplicación de sistemas de gestión de la seguridad alimentaria que contemplan buenas prácticas de higiene y procedimientos basados en los principios del APPCC. DOUE C 355, 16.9.2022. [Acceso](#)
9. FAO y OMS, Comisión del Codex Alimentarius. Principios Generales de Higiene de los Alimentos, CXC 1-1969. Revisión 2022. Roma: FAO/OMS. [Acceso](#)
10. FAO y OMS, Comisión del Codex Alimentarius. Directrices para la validación de medidas de control de la inocuidad de los alimentos, CXG 69-2008; modificaciones de redacción 2013. [Acceso](#)
11. ISO. ISO 22000:2018, Sistemas de gestión de la inocuidad de los alimentos — Requisitos para cualquier organización en la cadena alimentaria, con Enmienda 1:2024. Ginebra: ISO. [Acceso](#)
12. ISO. ISO 19011:2018, Directrices para la auditoría de los sistemas de gestión. Ginebra: ISO. [Acceso](#)
13. BRCGS. Global Standard Food Safety, Issue 9. Londres: BRCGS; 2022. [Acceso](#)

14. BRCGS. *Food Safety Issue 9 Auditor Checklist and Site Self-Assessment Tool, F904a*. [Acceso](#)
15. IFS Management GmbH. *IFS Food Standard, Version 8*. Berlín: IFS; abril de 2023. [Acceso](#)
16. IFS Management GmbH. *IFS Food Version 8 Doctrine, Version 5*. Abril de 2026. [Acceso](#)
17. Foundation FSSC. *FSSC 22000 Scheme, Version 7.0*. Mayo de 2026. [Acceso](#)
18. Foundation FSSC. *FSSC 22000 Version 7 Upgrade Process Requirements*. Mayo de 2026. [Acceso](#)
19. ISO/IEC. *ISO/IEC 42001:2023, Information technology — Artificial intelligence — Management system*. Ginebra: ISO. [Acceso](#)
20. ISO/IEC. *ISO/IEC 23894:2023, Information technology — Artificial intelligence — Guidance on risk management*. Ginebra: ISO. [Acceso](#)
21. ISO/IEC. *ISO/IEC 22989:2022, Information technology — Artificial intelligence — Artificial intelligence concepts and terminology*. [Acceso](#)
22. ISO/IEC. *ISO/IEC 23053:2022, Framework for Artificial Intelligence Systems Using Machine Learning*. [Acceso](#)
23. ISO/IEC. *ISO/IEC 25059:2023, Software engineering — SQuaRE — Quality model for AI systems*. [Acceso](#)
24. ISO/IEC. *ISO/IEC TR 24029-1:2021, Artificial Intelligence — Assessment of the robustness of neural networks — Part 1: Overview*. [Acceso](#)
25. ISO/IEC. *ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. [Acceso](#)
26. Tabassi, E. *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*. NIST AI 100-1. Gaithersburg: National Institute of Standards and Technology; 2023. doi:10.6028/NIST.AI.100-1. [Acceso](#)
27. World Health Organization. *Digitalization, Food Safety and Trade*. Geneva: WHO; 2019. [Acceso](#)
28. European Food Safety Authority. *Machine Learning Techniques Applied in Risk Assessment Related to Food Safety*. EFSA Supporting Publication 2017:EN-1254. [Acceso](#)
29. European Food Safety Authority. *AI@EFSA. Predictive modelling, evidence and responsible use of artificial intelligence*. Parma: EFSA; 2025. [Acceso](#)
30. Taiwo OR, Onyeaka H, Oladipo EK, Oloke JK, Chukwugozie DC. *Advancements in Predictive Microbiology: Integrating New Technologies for Efficient Food Safety Models*. *International Journal of Microbiology*. 2024;2024:6612162. doi:10.1155/2024/6612162. [Acceso](#)
31. Rashvand M, Ren Y, Sun D-W, et al. *Artificial intelligence for prediction of shelf-life of various food products: Recent advances and ongoing challenges*. *Trends in Food Science & Technology*. 2025;159:104989. doi:10.1016/j.tifs.2025.104989. [Acceso](#)
32. Li D, et al. *Research Progress of Machine Learning in Extending and Predicting the Shelf Life of Fruits and Vegetables*. *Foods*. 2024;13(19):3025. doi:10.3390/foods13193025. [Acceso](#)
33. Chhetri KB. *Applications of Artificial Intelligence and Machine Learning in Food Quality Control and Safety Assessment*. *Food Engineering Reviews*. 2024;16:1–21. doi:10.1007/s12393-023-09363-1. [Acceso](#)
34. Cui F, Zheng S, Wang D, et al. *Recent advances in shelf life prediction models for monitoring food quality*. *Comprehensive Reviews in Food Science and Food Safety*. 2023;22(2):1257–1284. doi:10.1111/1541-4337.13110. [Acceso](#)
35. Lu J, Liu A, Dong F, Gu F, Gama J, Zhang G. *Learning under Concept Drift: A Review*. *IEEE Transactions on Knowledge and Data Engineering*. 2019;31(12):2346–2363. doi:10.1109/TKDE.2018.2876857. [Acceso](#)
36. Hinder F, Vaquet V, Hammer B. *One or two things we know about concept drift: a survey on monitoring evolving environments*. *Frontiers in Artificial Intelligence*. 2024;7:1330258. doi:10.3389/frai.2024.1330258. [Acceso](#)
37. Hovakimyan G, Bravo JM, et al. *A Systematic Review of Concept Drift Detection*. *Information*. 2024;15(12):786. doi:10.3390/info15120786. [Acceso](#)
38. Ribeiro MT, Singh S, Guestrin C. *“Why Should I Trust You?” Explaining the Predictions of Any Classifier*. *Proceedings of KDD 2016*. doi:10.1145/2939672.2939778. [Acceso](#)
39. Lundberg SM, Lee S-I. *A Unified Approach to Interpreting Model Predictions*. *Advances in Neural Information Processing Systems* 30. 2017. [Acceso](#)
40. Sculley D, Holt G, Golovin D, et al. *Hidden Technical Debt in Machine Learning Systems*. *Advances in Neural Information Processing Systems* 28. 2015. [Acceso](#)

41. Amershi S, Begel A, Bird C, et al. *Software Engineering for Machine Learning: A Case Study*. 2019 IEEE/ACM 41st ICSE-SEIP. doi:10.1109/ICSE-SEIP.2019.00042. [Acceso](#)
42. ISO. ISO 13849-1:2023, *Safety of machinery — Safety-related parts of control systems — Part 1: General principles for design*. [Acceso](#)
43. Parlamento Europeo y Consejo. Reglamento (UE) 2024/2847, de 23 de octubre de 2024, relativo a los requisitos horizontales de ciberseguridad para productos con elementos digitales (Cyber Resilience Act). [Acceso](#)
44. Parlamento Europeo y Consejo. Directiva (UE) 2022/2555, de 14 de diciembre de 2022, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión (NIS2). [Acceso](#)
45. ISO/IEC. ISO/IEC 42005:2025, *Information technology — Artificial intelligence — AI system impact assessment*. [Acceso](#)
46. ISO/IEC. ISO/IEC 42006:2025, *Artificial intelligence — Requirements for bodies providing audit and certification of artificial intelligence management systems*. [Acceso](#)
47. Avila-Sosa R, Nevárez-Moorillón GV. Editorial: *Machine learning and predictive microbiology: enhancing food safety models*. *Frontiers in Sustainable Food Systems*. 2025;9:1655908. doi:10.3389/fsufs.2025.1655908. [Acceso](#)

Fecha de consulta de fuentes electrónicas: Julio de 2026.

NOTA TÉCNICA FINAL

Este documento ha sido preparado como base técnica y editorial. La aplicación a una instalación concreta exige conocer el producto, el proceso, el diagrama de flujo, los peligros, la arquitectura tecnológica, el contrato con el proveedor y la evidencia de validación disponible. No sustituye el juicio profesional del equipo APPCC, la consulta del texto normativo vigente ni el asesoramiento jurídico especializado.



Edita: Servicio de Publicaciones y Estudios de INTABIOTECH

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

Parque Empresarial Táctica

www.intabiotech.com