LEGAL AUDITORS

AI SOFTWARE COMPLIANCE

Cumplimiento de IA para fabricantes de software

Diagnóstico, clasificación y expediente de conformidad de IA del producto

PREPARADO PARA

Fabricantes de software de gestión y punto de venta para hostelería

Luis Vilanova Blanco

Colegiado nº 498 del COIICV · CISA, AAIA y AAIR (ISACA) · ISO/IEC 42001 Lead Auditor (Zertia)

Legal & Digital Auditors, S.L. · Valencia y Madrid · 21 de septiembre de 2026

ACREDITACIONES

CISA Certified Information Systems Auditor. An ISACA® Certification

AAIA ISACA Advanced in AI Audit.

AAIR Advanced in AI Risk. An ISACA® Certification

ISO/IEC 42001 LEAD AUDITOR CERTIFIED — ISSUED BY ZERTIA CERTIFICATION FOR A SAFER WORLD

EL PUNTO DE PARTIDA

La IA ya está dentro del producto

La conversación no empieza en «cuando incorporéis IA», sino en lo que ya está publicado y en uso por los restaurantes clientes.

1

Asistente IA

Consultas en lenguaje natural sobre ventas, márgenes, clientes, inventario, productos, empleados y locales.

2

Conexión MCP

Asistentes externos (ChatGPT, Claude) acceden a datos del negocio a través de la integración MCP publicada.

3

Recomendaciones

Sugerencias operativas y de marketing que incorporan señales externas: calendario, clima o reseñas.

Y casi siempre hay un roadmap con nuevas funcionalidades de IA en desarrollo. Ese es exactamente el momento en el que el cumplimiento es barato: antes de que el diseño esté cerrado.

EL HORIZONTE

Hacia dónde evoluciona la IA en un TPV de hostelería

Predicción de ventas y demanda

Cubiertos, facturación y carga por franja horaria.

Previsión de stock y compras

Cuánto comprar según histórico, reservas, clima o eventos.

Detección de anomalías

Anulaciones, descuentos, devoluciones, aperturas de cajón.

Optimización de carta y precios

Rentabilidad por plato, ajustes de precio y de escandallo.

Marketing y segmentación

Promociones personalizadas y generación de campañas.

Asistencia en sala

Upselling y cross-selling sugeridos durante la comanda.

Reservas y no-show

Predicción de ausencias y optimización de mesas.

Automatización administrativa

Lectura de facturas de proveedor, clasificación, conciliación.

Análisis del rendimiento operativo

Locales, turnos y equipos de trabajo.

Cada una de estas capacidades tiene un perfil regulatorio propio. Agruparlas bajo la etiqueta «IA» es precisamente lo que impide gestionarlas.

LA TESIS

No toda funcionalidad de IA tiene el mismo riesgo

Dos funcionalidades que comercialmente parecen equivalentes pueden tener obligaciones muy distintas. Lo que decide la clasificación no es la tecnología empleada, sino cuatro variables:

Finalidad

Para qué se usa realmente la salida del sistema, no para qué se diseñó.

Contexto de uso

Sector, entorno y ámbito en el que se despliega la funcionalidad.

Efectos

Qué consecuencias concretas produce sobre personas identificables.

Autonomía

Si informa, recomienda o decide, y qué supervisión humana existe.

Salida agregada de negocio

«Los jueves la facturación cae un 18 %: valora una promoción.»

Informa sobre el negocio en su conjunto. Perfil regulatorio ligero, centrado en transparencia y calidad del dato.

Salida referida a personas

Evaluar, puntuar, clasificar o apoyar decisiones sobre personas identificadas — trabajadores o clientes.

Activa un análisis mucho más exigente: finalidad, contexto, efectos, datos personales y supervisión humana.

POR QUÉ AFECTA AL FABRICANTE

El cumplimiento no se queda en el restaurante

1 Rol regulatorio propio

Quien desarrolle un sistema de IA y lo comercialice bajo su marca asume el papel de proveedor, con obligaciones propias e independientes de las de sus clientes.

2 Obligaciones que se trasladan

El restaurante sólo puede cumplir lo que el fabricante le permite cumplir: información, trazabilidad, supervisión humana y documentación nacen en el producto.

3 Exigencia contractual creciente

Cadenas, grupos y franquicias ya incorporan cláusulas de IA y de seguridad en la contratación de software. El cliente pregunta antes de comprar.

4 Modelos de terceros

Integrar IA de terceros por API no traslada la responsabilidad: hay que documentar proveedor, condiciones de uso, datos enviados y controles aplicados.

El objetivo del servicio es que el fabricante pueda acreditar lo que hace su IA — y no sólo afirmar que «usa un proveedor que cumple».

NUESTRO PLANTEAMIENTO

No una «auditoría del Reglamento de IA»

Una auditoría genérica sobre un producto vivo sirve de poco. El valor está en trabajar funcionalidad a funcionalidad y dejar el resultado documentado de forma permanente.

1

Diagnóstico

Inventario completo de funcionalidades de IA existentes y en roadmap.

2

Clasificación

Régimen aplicable a cada caso de uso, rol del fabricante y obligaciones concretas.

3

Expediente

Documentación permanente y auditada por sistema, viva y actualizable.

Dos fases de trabajo y un modelo de acompañamiento continuo, pensados para un producto que sigue evolucionando mientras se audita.

FASE 1

Diagnóstico de Cumplimiento de IA

Reunión técnica con producto y desarrollo, y análisis de todas las funcionalidades de IA existentes y previstas.

Qué hacemos

- Inventario de funcionalidades de IA, en producción y en roadmap
- Clasificación regulatoria de cada caso de uso
- Determinación del rol regulatorio en cada funcionalidad
- Mapa de riesgos por funcionalidad y por dato tratado
- Identificación de la normativa aplicable al caso concreto
- GAP analysis frente a los requisitos exigibles
- Recomendaciones de diseño para el desarrollo en curso

Qué se entrega

- Informe de diagnóstico con el inventario y la clasificación de cada funcionalidad
- Matriz de obligaciones aplicables por caso de uso
- Mapa de riesgos priorizado
- Plan de adecuación con acciones, responsables y orden de ejecución
- Requisitos de diseño para las funcionalidades aún no desarrolladas

EL NÚCLEO DEL DIAGNÓSTICO

Qué analizamos de cada funcionalidad de IA

Once campos por funcionalidad. Esta cadena es la que convierte una lista de features en un inventario defendible.

01 Función de IA

02 Finalidad

03 Modelo o proveedor

04 Datos utilizados

05 Usuarios afectados

06 Decisiones que produce

07 Grado de autonomía

08 Datos personales tratados

09 Rol del fabricante

10 Clasificación regulatoria

11 Obligaciones aplicables

Las dos últimas casillas —clasificación y obligaciones— sólo pueden rellenarse con rigor si las nueve anteriores están documentadas.

LO QUE HAY QUE DETERMINAR

Las preguntas que el diagnóstico deja contestadas

- ¿Se desarrollan modelos propios?
- ¿Se integra IA de terceros mediante API?
- ¿Se expone el negocio vía MCP a asistentes externos?
- ¿El sistema recomienda, o llega a decidir por sí mismo?
- ¿Se tratan datos de clientes del restaurante?
- ¿Se utilizan modelos de terceros (OpenAI, Anthropic, Google u otros)?
- ¿Se utiliza RAG sobre datos del cliente?
- ¿Se realiza elaboración de perfiles?
- ¿Se tratan datos de personas trabajadoras?
- ¿Se usan datos de varios restaurantes para entrenar o mejorar modelos?

La última pregunta es crítica en un TPV con miles de establecimientos: el uso transversal de datos de clientes para mejorar modelos cambia por completo el análisis.

FASE 2

Auditoría y Expediente de Conformidad de IA

El diagnóstico se convierte en un expediente permanente por cada funcionalidad o sistema de IA. Contenido de cada ficha:

Identificación

- Ficha del sistema y finalidad
- Clasificación regulatoria
- Roles y responsabilidades

Arquitectura

- Diseño técnico de la funcionalidad
- Modelos utilizados y versiones
- Fuentes y flujos de datos

Controles

- Evaluación de riesgos
- Privacidad y transparencia
- Supervisión humana y seguridad

Evidencias

- Logging y trazabilidad
- Gestión de proveedores y contratos
- Pruebas y conclusiones de auditoría

El resultado es algo defendible ante un cliente, una cadena, un auditor o una autoridad — muy distinto de afirmar «utilizamos un proveedor que cumple».

MARCO DE TRABAJO

Normativa y referencias que aplicamos

Reglamento (UE) 2024/1689

Reglamento de Inteligencia Artificial: clasificación del sistema, rol del operador y obligaciones asociadas, incluidas las de transparencia.

RGPD y LOPDGDD

Cuando haya datos personales: base jurídica, información, decisiones automatizadas, evaluación de impacto y encargados de tratamiento.

Normativa sectorial y de consumo

Prácticas comerciales, información al usuario y, cuando proceda, propiedad intelectual sobre datos y contenidos generados.

Seguridad del producto

Requisitos de seguridad, trazabilidad y gestión de vulnerabilidades aplicables a un producto software comercializado.

ISO/IEC 42001 e ISO/IEC 27001

Referencias de gestión para estructurar los controles de IA y de seguridad de la información de forma certificable.

Marcos de ISACA

Metodología de auditoría, evidencias y trabajo de campo conforme a la práctica profesional (CISA, AAIA).

El alcance normativo concreto se fija en la reunión de inicio, en función de las funcionalidades y de los datos efectivamente tratados.

EL MODELO DE ACOMPAÑAMIENTO

AI Compliance by Design

En lugar de auditar la IA cuando ya está terminada, clasificamos cada nueva funcionalidad antes de desarrollarla e indicamos qué requisitos deben incorporarse al diseño.

1

El fabricante plantea

Una nueva funcionalidad de IA o un cambio sustancial en una existente.

2

Legal Auditors clasifica

Riesgos, régimen aplicable y requisitos que debe cumplir el diseño.

3

Desarrollo implementa

Con los requisitos ya incorporados desde el primer sprint.

4

Legal Auditors verifica

Revisión de la implementación y recogida de evidencias.

5

Se actualiza el expediente

La funcionalidad nace documentada y auditada.

Se revisa el expediente cada vez que se añade una funcionalidad de IA, se cambia de modelo o proveedor, se incorporan nuevos datos o se modifica sustancialmente una funcionalidad existente.

Legal Auditors como función externa de cumplimiento de IA del producto.

EL RESULTADO

Qué obtiene el fabricante al final del proceso

1

Informe AI Software Compliance

Inventario, clasificación y conclusiones de auditoría por funcionalidad.

2

Matriz de cumplimiento

Obligación por obligación, con su estado y su evidencia asociada.

3

Plan de adecuación

Acciones priorizadas, con responsables y orden de ejecución.

4

Revisión de subsanaciones

Verificación de las correcciones aplicadas tras el informe.

Certificado privado y sello

«AI SOFTWARE COMPLIANT — Audited by Legal Auditors»

Emitido por auditores CISA, AAIA y AAIR de ISACA y auditores ISO/IEC 42001 acreditados por Zertia. Utilizable en la comunicación comercial del fabricante y en respuestas a cuestionarios de clientes.

AI SOFTWARE COMPLIANT

Audited by Legal Auditors

El certificado y el sello son privados, emitidos por Legal & Digital Auditors, S.L. No sustituyen a una certificación acreditada, a una evaluación de conformidad ni a ningún marcado oficialmente exigible al producto.

SIGUIENTES PASOS

Cómo empezamos

1 Listado de funcionalidades

El cliente nos facilita las funcionalidades de IA ya operativas y las previstas en los próximos 12 meses.

2 Reunión técnica de inicio

Sesión con producto y desarrollo para delimitar el producto, los modelos y los datos en alcance.

3 Propuesta cerrada

Con el alcance delimitado, emitimos la propuesta económica y el calendario de ejecución.

Quién lo hace

- CISA — Certified Information Systems Auditor (ISACA)
- AAIA — Advanced in AI Audit (ISACA)
- AAIR — Advanced in AI Risk (ISACA)
- ISO/IEC 42001 Lead Auditor (Zertia)
- Perito judicial informático, colegiado nº 498 COIICV

LEGAL AUDITORS | CEO www.legalauditors.es

CIF B44622520 · Valencia y Madrid · luis.vilanova@legalauditors.es · 911 277 300