qualoom®

Inspiring Technology
for People

GUÍA DE CUMPLIMIENTO DE IA

ISO + ENS + AI Act + ISO/IEC 42001

Cómo convertir las obligaciones de IA en controles, evidencias y procesos verificables

Área de Inteligencia Artificial Corporativa
Fecha 27/10/2026
Versión 1.0
Clasificación: Público

Copyright @2026 Qualoom Expertise Technology

Más información www.qualoom.es

qualoom®

Inspiring Technology
for People

ÍNDICE

01 El cumplimiento de la IA cambia de escala

02 Cuatro referencias con funciones sinérgicas

03 AI ACT: Determinar que obligaciones aplican

04 2026 marca una nueva etapa de cumplimiento

05 Obligaciones de transparencia ya aplicables

06 Modelos de IA de propósito general (GPAI)

07 ISO/IEC 42001: Arquitectura Documental

08 Integrar la seguridad en el cumplimiento de IA

Copyright @2026 Qualoom Expertise Technology

qualoom®

Inspiring Technology
for People

ÍNDICE

09 ENS: IA en servicios públicos y cadena de suministro

10 Una matriz única para conectar cuatro marcos

11 Reconstruir la historia operativa del sistema

12 Proveedores: El cumplimiento fuera de casa

13 ¿Puedes demostrar que estás preparado?

14 Construir una cadena de evidencia verificable

15 Del diagnóstico a la evidencia continua

16 Integración de IA Generativa

Copyright @2026 Qualoom Expertise Technology

qualoom®

Inspiring Technology
for People

ÍNDICE

17 El cumplimiento exige evidencias sostenibles

18 Convierte los requisitos en un modelo verificable

Copyright @2026 Qualoom Expertise Technology

qualoom®

Inspiring Technology
for People

El cumplimiento de la IA cambia de escala

La utilización empresarial de Inteligencia Artificial activa requisitos procedentes de múltiples fuentes regulatorias, normativas y contractuales. La dificultad principal radica en evitar la fragmentación documental.

El objetivo operativo

Pasar de una obligación abstracta a una evidencia verificable mediante una cadena lógica estructurada:

1. **Requisito**
   ¿Qué exige el marco aplicable (AI Act, ISO, ENS)?
2. **Interpretación**
   ¿Qué impacto real tiene sobre nuestros procesos?
3. **Control**
   ¿Qué medida técnica u organizativa implantamos?
4. **Evidencia**
   ¿Cómo demostramos su cumplimiento ante una auditoría?

Copyright @2026 Qualoom Expertise Technology

qualoom®

Inspiring Technology
for People

Cuatro referencias con funciones sinérgicas

La arquitectura de cumplimiento combina cuatro instrumentos normativos adaptados al contexto tecnológico y de negocio de la organización:

AI Act (Reglamento UE)

Naturaleza: Reglamento europeo armonizado.
Función: Establece obligaciones jurídicas basadas en niveles de riesgo, prohibiciones y transparencia.

ISO/IEC 42001

Naturaleza: Norma internacional de gestión.
Función: Estructura políticas, objetivos, roles y mejora continua específicos para sistemas de IA.

ISO/IEC 27001

Naturaleza: SGSI internacional.
Función: Gestiona la seguridad de la información, accesos, activos tecnológicos y ciberseguridad.

ENS (España)

Naturaleza: Marco regulatorio (RD 311/2022).
Función: Principios de protección y resiliencia aplicables a servicios públicos y su cadena de valor privada.

Copyright @2026 Qualoom Expertise Technology

qualoom®

Inspiring Technology
for People

Determinar qué obligaciones aplican

El primer paso metodológico exige un análisis riguroso para evitar asunciones incorrectas sobre el alcance de la regulación europea:

Sistema

Identificar la solución, modelo o aplicación concreta.

Finalidad

Contexto y finalidad de utilización prevista.

Rol

Determinar si se actúa como Proveedor, Deployer, Importador o Distribuidor.

Riesgo

Clasificar en Práctica prohibida, Alto riesgo, Transparencia o Riesgo mínimo.

Punto de Control:

Documentar formalmente el razonamiento técnico antes de concluir que un sistema está exento de obligaciones.

Copyright @2026 Qualoom Expertise Technology

qualoom®

Inspiring Technology
for People

2026 marca una nueva etapa de cumplimiento

El reglamento despliega sus obligaciones de manera progresiva, situando hitos críticos en la gobernanza tecnológica corporativa:

Febrero - Agosto 2025

Prohibiciones y Alfabetización (Art. 4)

Aplicación de prácticas prohibidas y obligación de promover competencias en IA entre el personal operario y gestor.

02 Agosto 2026

Obligaciones de Transparencia (Artículo 50)

Entrada en vigor general de los requisitos de transparencia para sistemas interactivos, contenido sintético y deepfakes.

Diciembre 2027 - Agosto 2028

Sistemas de Alto Riesgo

Plena exigencia para sistemas de alto riesgo en ámbitos específicos y productos regulados bajo periodo transitorio.

Copyright @2026 Qualoom Expertise Technology

Más información www.qualoom.es

qualoom®

Inspiring Technology
for People

Obligaciones de transparencia ya aplicables

Desde agosto de 2026, el artículo 50 exige mecanismos operativos claros en tres escenarios tecnológicos principales:

Chat e interacción

Obligación de informar explícitamente a las personas físicas de que interactúan con un sistema de IA, salvo contexto evidente.

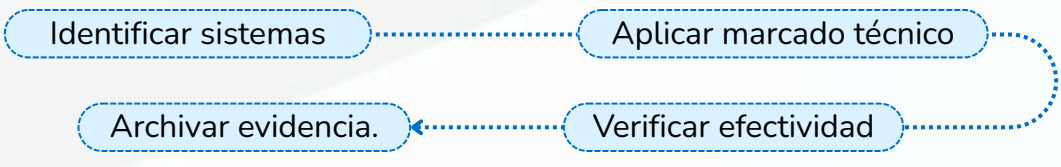
Contenido sintético

Marcado y etiquetado legible por máquina para contenidos generados o manipulados artificialmente.

Deepfakes e interés público

Divulgación obligatoria en imágenes, audio o vídeo hiperrealistas que simulen personas reales, así como en textos informativos de interés público generados por algoritmos.

Flujo de Verificación



Copyright @2026 Qualoom Expertise Technology

Más información www.qualoom.es

qualoom®

Inspiring Technology
for People

Modelos de IA de propósito general (GPAI)

Los proveedores de modelos base afrontan exigencias rigurosas de documentación técnica y derechos de autor. Las organizaciones integradoras deben gestionar su cadena de suministro tecnológica.

Documentación a solicitar al proveedor GPAI:

- Ficha técnica del modelo y versiones de lanzamiento.
- Condiciones de uso y restricciones operativas conocidas.
- Información sobre los conjuntos de datos de entrenamiento (resumen detallado)
- Medidas de ciberseguridad y robustez aplicadas.

Cadena de suministro

Copyright @2026 Qualoom Expertise Technology

Más información www.qualoom.es

qualoom®

Inspiring Technology
for People

ISO/IEC 42001: Arquitectura Documental

1

Políticas

Política de IA, uso responsable, directrices éticas y criterios de proveedores.

2

Procedimientos

Procesos formales de evaluación de riesgos, aprobación y gestión de incidentes.

3

Registros

Actas de revisión directiva, resultados de pruebas algorítmicas y formaciones.

4

Evidencias

Logs de actividad, capturas de control, informes de auditoría y aprobaciones firmadas.

Copyright @2026 Qualoom Expertise Technology

qualoom®

Inspiring Technology
for People

Integrar la seguridad en el cumplimiento de IA

Área SGSI / ISO 27001	Aplicación en Sistemas de IA	Evidencia Reutilizable
Control de Accesos	Restricción de privilegios a modelos y datos.	Matriz IAM y registros de log.
Gestión de Proveedores	Evaluación de APIs y servicios externos.	Cuestionarios due diligence y contratos.
Gestión de Incidentes	Detección de fallos, fugas o respuestas tóxicas.	Tickets de incidencia y análisis post-mortem.
Protección de Datos	Clasificación de información de entrenamiento.	Inventario de activos y políticas de cifrado.

Copyright @2026 Qualoom Expertise Technology

Más información www.qualoom.es

qualoom®

Inspiring Technology for People

ENS: IA en servicios públicos

Regulado por el Real Decreto 311/2022, el ENS exige que las soluciones tecnológicas privadas integradas en servicios públicos cumplan estrictos estándares de resiliencia.

Dimensiones Clave

- Clasificación y origen de datos.
- Infraestructura cloud y servidores.
- Seguridad en proveedores terceros.
- Planes de continuidad y respaldo

Conformidad ENS

Las entidades públicas y contratistas pueden exigir declaraciones o certificados oficiales de conformidad ENS para validar algoritmos y servicios de IA.

Una matriz única para conectar cuatro marcos

Evita duplicidades operativas relacionando requisitos normativos y evidencias comunes:

Área de Cumplimiento	AI Act	ISO 42001	ISO 27001	ENS	Evidencia Principal
Transparencia	●	●	○	○	Interfaz etiquetada / Avisos
Alfabetización	●	●	○	○	Registros de formación
Documentación	●	●	●	●	Expediente técnico del sistema
Seguridad	●	●	●	●	Controles SGSI y logs de acceso
Proveedores	●	●	●	●	Auditorías y contratos

Copyright @2026 Qualoom Expertise Technology

qualoom®

Inspiring Technology
for People

Reconstruir la historia operativa del sistema

Para cada sistema de IA en producción, se debe mantener un expediente documental estructurado en 7 secciones clave:

01. Identificación
Nombre, proveedor, modelo y versión exacta.

02. Finalidad
Usos previstos, usuarios y procesos afectados

03. Aplicabilidad
Rol de la empresa y normativa vinculante.

04. Evaluaciones
Análisis de riesgo, decisiones y aprobaciones.

05. Controles
Medidas técnicas, organizativas y contractuales.

06. Evidencias
Documentos, registros, logs e informes de prueba.

Copyright @2026 Qualoom Expertise Technology

qualoom®

Inspiring Technology
for People

Proveedores: El cumplimiento fuera de casa

La dependencia tecnológica de terceros obliga a auditar la cadena de suministro antes de contratar y durante todo el ciclo de vida del servicio:

Antes de Contratar

- Jurisdicciones y ubicación del cloud.
- Tratamiento de datos y privacidad.
- Subproveedores y dependencias API.
- Medidas de seguridad del tercero.

Durante la Relación

- Revisar cambios de servicio.
- Actualizardocumentación técnica
- Verificar eficacia de controles.
- Registrar incidencias algorítmicas.

Copyright @2026 Qualoom Expertise Technology

Más información www.qualoom.es

qualoom®

Inspiring Technology
for People

¿Puedes demostrar que estás preparado?

Verifica el estado de preparación de tu organización frente a auditorías regulatorias:

- Rol y finalidad del sistema de IA perfectamente definidos.
- Categoría de riesgo analizada conforme al AI Act.
- Requisitos de transparencia (Artículo 50) implantados.
- Políticas y objetivos del SGIA (ISO 42001) vigentes y firmados.
- Controles de seguridad (ISO 27001 / ENS) operativos.
- Proveedores tecnológicos evaluados con due diligence.
- Cada requisito normativo cuenta con una evidencia asignada y auditable.

Pregunta clave: ¿Cuántos requisitos críticos de tu IA puedes acreditar hoy mismo ante una inspección?

Copyright @2026 Qualoom Expertise Technology

Más información www.qualoom.es

qualoom®

Inspiring Technology
for People

Construir una cadena de evidencia verificable

Requisito
Identificar la obligación legal aplicable.

Control
Implantar la medida técnica u organizativa

Evidencia
Generar y archivar la prueba documental o log.

Auditoria
Verificación periódica y validación de validez.

Copyright @2026 Qualoom Expertise Technology

Más información www.qualoom.es

qualoom®

Inspiring Technology
for People

Del diagnóstico a la evidencia continua

Modelo de despliegue estructurado en seis fases iterativas:

F1. Determinar
Mapa de aplicabilidad y roles regulatorios.

F2. Interpretar
Matriz de cumplimiento y traducción de requisitos.

F3. Documentar
Estructuración del sistema documental SGIA.

F4. Implantar
Puesta en marcha de controles técnicos y formativos.

F5. Verificar
Auditorías internas y análisis de evidencias.

F6. Actualizar
Iteración continua ante cambios normativos y tecnológicos.

Copyright @2026 Qualoom Expertise Technology

Más información www.qualoom.es

qualoom®

Inspiring Technology
for People

Integración de IA Generativa

Aplicación real del modelo ante la incorporación de una herramienta generativa externa:

Fases de ejecución práctica.

Identificar

FASE 1

Proveedor cloud externo y personal usuario.

Determinar

FASE 2

Rol de deployer, finalidad profesional y datos de entrada.

Controles

FASE 3

Restricción de datos confidenciales y supervisión de outputs.

Evidencias

FASE 4

Expediente con evaluación y registros de formación interna.

Copyright @2026 Qualoom Expertise Technology

Más información www.qualoom.es

qualoom®

Inspiring Technology
for People

El cumplimiento exige evidencias sostenibles

Un modelo sólido de gobernanza de IA permite responder con absoluta solidez a cinco cuestiones directivas clave:

¿Que obligaciones aplican?

Marcos legales y contractuales.

¿Qué controles responden?

Medidas técnicas y organizativas.

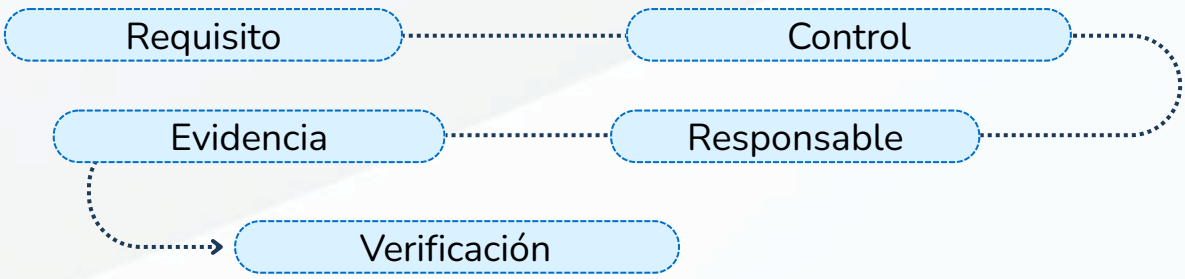
¿Quién es el responsable?

Funciones asignadas claramente.

¿Qué evidencia existe?

Registros e informes auditables.

Modelo final:



Copyright @2026 Qualoom Expertise Technology

Más información www.qualoom.es

qualoom®

Inspiring Technology
for People

Convierte los requisitos en un modelo verificable

CONTACTA CON NOSOTROS

www.qualoom.es

contacto@qualoom.es

(+34) 91 236 4808

Copyright @2026 Qualoom Expertise Technology

Más información www.qualoom.es