RETECH Redes Territoriales de Especialización Tecnológica

RED ARGOS

Roles y obligaciones regulatorias del RIA para sistemas de IA en entornos de Salud y Smart Cities

Octubre de 2025

Versión 1.0

Junta de Andalucía

Financiado por la Unión Europea NextGenerationEU

Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales

Plan de Recuperación, Transformación y Resiliencia

incibe_ Instituto Nacional de Ciberseguridad

Junta de Andalucía

Agencia Digital de Andalucía

Objeto del Expediente:

"ELABORACIÓN DE GUÍAS DE CIBERSEGURIDAD IA PARA ENTORNOS DE SMART CITIES Y SALUD" (CONTR 2024 829535).

Esta guía forma parte de la colección Guías de Ciberseguridad en IA para las Smart Cities y el sector Salud creada por la Agencia Digital de Andalucía como parte del Proyecto Red Argos, perteneciente al programa RETECH, de Redes Inteligentes de Especialización Tecnológica, en el marco del Plan de Recuperación, Transformación y Resiliencia, financiado por la Unión Europea-NextGenerationEU, a través de INCIBE.

Autor del documento: Agencia Digital de Andalucía

Tipo de documento: Guía

Fecha de elaboración: 13/10/2025

Fecha de última actualización: 05/11/2025

ÍNDICE DE CONTENIDOS

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

ÍNDICE DE TABLAS

1. Introducción

La inteligencia artificial (IA) se ha convertido en un componente esencial de los entornos críticos contemporáneos, especialmente en los sectores de **Salud y Smart Cities**, donde su adopción está transformando la forma en que se diagnostican enfermedades, se gestionan recursos sanitarios, se planifican infraestructuras urbanas o se administran los servicios públicos.

En el ámbito sanitario, la IA contribuye a mejorar la precisión diagnóstica, reducir los errores clínicos y optimizar la atención personalizada, mientras que en las ciudades inteligentes posibilita la gestión predictiva del tráfico, la eficiencia energética y la sostenibilidad de los servicios urbanos. No obstante, el uso de estas tecnologías también genera riesgos significativos: decisiones automatizadas que afectan a los derechos fundamentales, posibles sesgos en la evaluación de personas, o vulnerabilidades que pueden comprometer la seguridad de infraestructuras críticas.

Con el fin de garantizar que el desarrollo y uso de la inteligencia artificial en Europa se produzca dentro de un marco de seguridad, transparencia y responsabilidad, la Unión Europea adoptó el **Reglamento (UE) 2024/1689**, relativo a la inteligencia artificial (en adelante, Reglamento de inteligencia artificial o RIA). Este Reglamento de inteligencia artificial introduce un sistema regulatorio basado en el riesgo y **define los roles y obligaciones** de los agentes que intervienen en el ciclo de vida de los sistemas de IA.

El presente documento forma parte de dicho **marco de implementación** y constituye la segunda fase de la *Guía de Clasificación de Sistemas de IA en base al RIA en entornos de Salud y Smart Cities*. Si la primera guía se centró en la clasificación de los sistemas según su nivel de riesgo, esta segunda aborda la **identificación de los roles regulados por el RIA** y la **determinación de las obligaciones** que corresponden a cada uno de ellos en función del tipo de sistema y su nivel de riesgo.

De este modo, la guía proporciona a las organizaciones una herramienta práctica para:

- Reconocer su rol dentro del ecosistema regulatorio del RIA.
- Comprender las responsabilidades y obligaciones que deben asumir en relación con el ciclo de vida del sistema de IA.
- Aplicar mecanismos de cumplimiento, trazabilidad y control proporcionales al nivel de riesgo del sistema y coherentes con los principios de transparencia, seguridad y supervisión humana establecidos por el Reglamento.

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

2. Objetivo y alcance

2.1. Objetivo

El documento busca facilitar el cumplimiento normativo de las entidades que desarrollan, integran o utilizan sistemas de IA, mediante la definición clara de las figuras establecidas en el Reglamento de inteligencia artificial incluyendo el proveedor, responsable del despliegue, fabricante, importador, distribuidor y representante autorizado, y la descripción de las responsabilidades que cada una de ellas debe asumir a lo largo del ciclo de vida del sistema.

Este marco tiene como finalidad:

- Garantizar una interpretación uniforme del RIA en los entornos de Salud y Smart Cities.
- Proporcionar criterios operativos verificables para determinar las obligaciones aplicables a cada actor.
- Integrar las exigencias del RIA en los sistemas internos de gestión de riesgos, calidad y cumplimiento normativo de las organizaciones.

En el sector de la Salud, la guía se aplica de forma complementaria al Reglamento (UE) 2017/745 (MDR) y al Reglamento (UE) 2017/746 (IVDR), garantizando la coherencia entre la evaluación de conformidad de productos sanitarios y las obligaciones de gobernanza derivadas del RIA.

En el ámbito de las Smart Cities, su aplicación permite armonizar la adopción de soluciones basadas en IA en áreas como la movilidad, la energía, la sostenibilidad o la seguridad pública, dentro de un marco común de fiabilidad, ética y supervisión pública.

Esta guía, por tanto, no introduce nuevas obligaciones legales, sino que traduce los requisitos del Reglamento en pautas prácticas y verificables, reforzando la capacidad de las entidades para demostrar su cumplimiento ante las autoridades competentes y ante la Oficina Europea de Inteligencia Artificial.

2.2. Alcance

La presente guía es aplicable a todas las entidades públicas y privadas que desarrollen, integren, desplieguen, comercialicen o utilicen sistemas de inteligencia artificial en los sectores de Salud y Smart Cities, dentro del ámbito territorial de la Unión Europea.

Su contenido abarca todas las fases del ciclo de vida de los sistemas de IA, desde el diseño y desarrollo inicial hasta su uso operativo, seguimiento posterior al mercado y eventual retirada, incluyendo tanto los aspectos técnicos como organizativos del cumplimiento regulatorio.

Las orientaciones aquí recogidas se dirigen a los distintos operadores económicos y entidades usuarias definidos por el Reglamento (UE) 2024/1689, y tienen por objeto facilitar la interpretación y aplicación práctica de sus disposiciones en contextos donde la inteligencia artificial desempeña funciones críticas para la salud pública, la seguridad o el bienestar social.

La guía no sustituye al Reglamento ni a la normativa sectorial aplicable, sino que actúa como instrumento complementario de apoyo para su implementación coordinada en los sectores de Salud y Smart Cities.

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

Quedan excluidos de su alcance los sistemas de IA desarrollados o utilizados con fines militares, de defensa o de seguridad nacional, así como los destinados exclusivamente a investigación científica o experimental que no se introduzcan en el mercado ni se utilicen en entornos reales dentro de la Unión Europea.

3. Definiciones

Acrónimo/Término	Definición
RIA	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 (Ley de Inteligencia Artificial). Establece el marco jurídico de la Unión Europea para el desarrollo, la comercialización, la puesta en servicio y la utilización de sistemas de inteligencia artificial, con un enfoque basado en el riesgo y en los principios de seguridad, transparencia, trazabilidad, supervisión humana y responsabilidad.
Sistema de inteligencia artificial (Sistema de IA)	Software que, para un conjunto determinado de objetivos definidos por el ser humano, genera resultados como contenidos, predicciones, recomendaciones o decisiones que influyen en entornos físicos o virtuales y que está diseñado para funcionar con distintos niveles de autonomía mediante técnicas como el aprendizaje automático, la lógica o los métodos estadísticos. Conforme al artículo 3, apartado 1, del Reglamento (UE) 2024/1689.
Proveedor	Persona física o jurídica, autoridad pública, agencia u otro organismo que desarrolla un sistema de inteligencia artificial o encarga su desarrollo y lo pone en el mercado o en servicio bajo su propio nombre o marca, con independencia de que lo haga de forma onerosa o gratuita. Es el responsable principal de la conformidad del sistema con el Reglamento (UE) 2024/1689, incluida la evaluación de conformidad, la documentación técnica, el marcado CE, la gestión del riesgo y la vigilancia posterior al mercado.
Responsable del despliegue	Persona física o jurídica, autoridad pública, agencia u otro organismo que utiliza un sistema de inteligencia artificial bajo su autoridad, salvo cuando el uso sea exclusivamente personal y no profesional. Debe garantizar el uso conforme a la finalidad prevista, la existencia de supervisión humana efectiva y las condiciones de seguridad y transparencia establecidas en el Reglamento (UE) 2024/1689.

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

Usuario	Persona física o jurídica, autoridad pública, agencia u otro organismo que emplea un sistema de inteligencia artificial en su actividad, tanto si actúa como responsable del despliegue como si lo utiliza de forma indirecta. Incluye operadores, gestores y entidades que aplican los resultados generados por el sistema.
Fabricante	Persona física o jurídica que fabrica o manda fabricar un producto que incorpora o utiliza un sistema de inteligencia artificial como componente, con vistas a su puesta en el mercado o en servicio bajo su nombre o marca. Debe asegurar que la integración del sistema de inteligencia artificial no afecta a la conformidad del producto con la normativa sectorial aplicable.
Importador	Persona física o jurídica establecida en la Unión Europea que introduce en el mercado de la Unión un sistema de inteligencia artificial procedente de un tercer país. Es responsable de garantizar que el sistema cumple el Reglamento (UE) 2024/1689, dispone de la documentación técnica y de la declaración de conformidad y lleva el marcado CE correspondiente.
Distribuidor	Persona física o jurídica de la cadena de suministro, distinta del proveedor o del importador, que pone a disposición en el mercado un sistema de inteligencia artificial sin ser su proveedor ni su importador. Su función es garantizar que los sistemas comercializados sean conformes y mantengan la integridad documental y técnica exigida por la normativa europea.
Representante autorizado	Persona física o jurídica establecida en la Unión Europea que ha recibido un mandato escrito de un proveedor para actuar en su nombre respecto de determinadas tareas u obligaciones. Actúa como interlocutor ante las autoridades competentes, conserva la documentación técnica y colabora en inspecciones y auditorías oficiales.
Operador económico	Conjunto de figuras que intervienen en la puesta en el mercado, la puesta en servicio o la utilización de un sistema de inteligencia artificial. Incluye al fabricante, al proveedor, al representante autorizado, al importador, al distribuidor y al responsable del despliegue, conforme a los artículos 3.3 a 3.9 del Reglamento (UE) 2024/1689.

Organismo notificado	Entidad de evaluación de la conformidad designada por un Estado miembro de la Unión Europea para realizar las tareas de evaluación de la conformidad previstas en el Reglamento (UE) 2024/1689. Estos organismos son supervisados por las autoridades nacionales competentes y deben cumplir los criterios de independencia, competencia técnica e imparcialidad establecidos en la normativa de la Unión.
Modelo de inteligencia artificial de propósito general (GPAI)	Modelo de inteligencia artificial que presenta una generalidad significativa y es capaz de ejecutar de manera competente una amplia gama de tareas distintas, independientemente de su forma de comercialización o distribución, y que puede integrarse o adaptarse en diversos sistemas de inteligencia artificial. Conforme al artículo 3, apartado 63, del Reglamento (UE) 2024/1689.
Modelo de inteligencia artificial de propósito general con riesgo sistémico (GPAI sistémico)	Modelo de inteligencia artificial de propósito general cuya escala, capacidad funcional o potencia de cómputo puede generar impactos significativos sobre la seguridad, la salud pública, los derechos fundamentales o la estabilidad social o económica de la Unión. Se consideran tales los modelos cuyo entrenamiento haya requerido un cómputo total superior a diez elevado a veinticinco operaciones de coma flotante o que hayan sido designados por la Comisión Europea conforme al artículo 55 del Reglamento (UE) 2024/1689.
Sistema de inteligencia artificial de alto riesgo	Sistema de inteligencia artificial que cumple los criterios del artículo 6 y figura en el Anexo III del Reglamento (UE) 2024/1689 y que, por su finalidad o ámbito de aplicación, puede afectar de manera significativa a la salud, la seguridad o los derechos fundamentales de las personas. Está sujeto a los requisitos del Título III, Capítulo II, del Reglamento.
Sistema de inteligencia artificial de riesgo inaceptable o prohibido	Sistema cuyo uso está prohibido por el artículo 5 del Reglamento (UE) 2024/1689 por contravenir derechos fundamentales o la dignidad humana. Incluye, entre otros supuestos, la manipulación cognitiva subliminal, la puntuación social generalizada y el reconocimiento biométrico en tiempo real en espacios públicos con fines de aplicación de la ley, salvo excepciones expresamente previstas.
Sistema de inteligencia artificial de riesgo limitado	Sistema que no se clasifica como de alto riesgo ni prohibido y que está sujeto a obligaciones de transparencia específicas en virtud del artículo 52 del Reglamento (UE) 2024/1689, como la obligación de informar a las personas de que interactúan con un sistema de inteligencia artificial o con contenido generado artificialmente.
Sistema de inteligencia artificial de riesgo mínimo	Sistema cuyo uso presenta un riesgo bajo o nulo para la seguridad o los derechos fundamentales y que no está sujeto a obligaciones regulatorias específicas más allá de las buenas prácticas de gobernanza y supervisión responsable.

Marcado CE	Marcado mediante el cual el fabricante o el proveedor declara que un producto cumple todos los requisitos aplicables establecidos en la legislación de armonización de la Unión Europea. El marcado CE acredita que el producto ha superado los procedimientos de evaluación de conformidad requeridos y puede ser comercializado dentro del mercado de la Unión.
Evaluación de conformidad	Procedimiento formal mediante el cual se verifica y documenta que un sistema de inteligencia artificial cumple los requisitos esenciales del Reglamento (UE) 2024/1689 y, cuando corresponda, los de la normativa sectorial aplicable. Su resultado es la declaración de conformidad y la colocación del marcado CE.
Vigilancia del mercado	Conjunto de actividades y medidas realizadas por las autoridades competentes de los Estados miembros de la Unión Europea con el fin de garantizar que los sistemas de inteligencia artificial puestos en el mercado o en servicio cumplen las disposiciones del Reglamento (UE) 2024/1689 y no representan riesgos para la salud, la seguridad o los derechos fundamentales.
FLOPs	Operaciones de coma flotante. Unidad de medida que indica el número total de operaciones matemáticas realizadas, por ejemplo, durante el entrenamiento de un modelo de inteligencia artificial. Refleja la magnitud del cálculo utilizado, no la velocidad de procesamiento.
FLOPS	Operaciones de coma flotante por segundo. Unidad de medida de la velocidad de cálculo de un hardware o sistema informático que cuantifica su capacidad de procesamiento durante el entrenamiento y la ejecución de modelos de inteligencia artificial.
SSF (Marco de Seguridad y Protección)	Conjunto documentado de políticas, procedimientos y controles técnicos y organizativos que deben elaborar los proveedores de modelos de inteligencia artificial de propósito general con riesgo sistémico. Este marco describe la evaluación, mitigación y supervisión de riesgos asociados a la seguridad, la ciberresiliencia y los posibles impactos sistémicos del modelo, conforme al artículo 55 del Reglamento (UE) 2024/1689.
MDR	Reglamento (UE) 2017/745 del Parlamento Europeo y del Consejo, de 5 de abril de 2017, relativo a los productos sanitarios. Establece los requisitos para la comercialización, seguridad, desempeño, evaluación clínica y vigilancia de los productos sanitarios en la Unión Europea.

IVDR	Reglamento (UE) 2017/746 del Parlamento Europeo y del Consejo, de 5 de abril de 2017, relativo a los productos sanitarios para diagnóstico in vitro. Regula los requisitos de seguridad, desempeño y evaluación de conformidad de los productos de diagnóstico in vitro dentro del mercado de la Unión.
RGPD	Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de dichos datos. Constituye el marco jurídico general de la Unión en materia de protección de datos personales.
CRA	Reglamento (UE) 2023/2854 del Parlamento Europeo y del Consejo, de 13 de diciembre de 2023, relativo a los requisitos de ciberresiliencia aplicables a los productos con elementos digitales. Establece las normas esenciales de ciberseguridad para el diseño, desarrollo y mantenimiento de productos y sistemas digitales, en coherencia con el Reglamento (UE) 2024/1689.
Directiva 2006/42/CE (Directiva de Maquinaria)	Directiva 2006/42/CE del Parlamento Europeo y del Consejo, de 17 de mayo de 2006, relativa a las máquinas y por la que se modifica la Directiva 95/16/CE. Regula los requisitos esenciales de seguridad y salud en el diseño y la construcción de maquinaria comercializada o puesta en servicio en el mercado de la Unión.
Directiva 2012/19/UE (Directiva RAEE)	Directiva 2012/19/UE del Parlamento Europeo y del Consejo, de 4 de julio de 2012, sobre residuos de aparatos eléctricos y electrónicos. Establece medidas para la recogida, tratamiento, reciclado y eliminación ambientalmente correcta de los residuos de aparatos eléctricos y electrónicos en la Unión Europea.
ISO e IEC	Organización Internacional de Normalización (ISO) y Comisión Electrotécnica Internacional (IEC). Organismos internacionales de normalización que elaboran normas técnicas reconocidas globalmente, incluidas las relativas a la gestión, seguridad y gobernanza de la inteligencia artificial.
NIST	National Institute of Standards and Technology. Instituto Nacional de Estándares y Tecnología de los Estados Unidos encargado de desarrollar marcos de gestión de riesgos y estándares técnicos, incluido el Marco de Gestión de Riesgos de Inteligencia Artificial.

TABLA 1: DEFINICIONES EMPLEADAS.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PUBLICA SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

4. Identificación y descripción de roles en base al RIA

El Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas sobre la inteligencia artificial (Reglamento de Inteligencia Artificial), establece un marco jurídico basado en el riesgo que define de forma precisa los roles que intervienen en el ciclo de vida de los sistemas de inteligencia artificial.

Cada uno de estos roles está vinculado a un grado distinto de participación y control sobre el sistema, y constituye la base sobre la que se asignan las obligaciones regulatorias correspondientes. La identificación correcta de estos roles es el primer paso para determinar las responsabilidades que cada entidad debe asumir conforme al Reglamento.

El artículo 3 del RIA define formalmente seis figuras principales: proveedor, responsable del despliegue, fabricante, importador, distribuidor y representante autorizado. Cada una de ellas desempeña una función específica en la cadena de valor de la inteligencia artificial, desde el desarrollo inicial del sistema hasta su utilización práctica o retirada.

A continuación, se describen los roles reconocidos por el Reglamento, indicando su alcance jurídico y su aplicación general en los entornos de Salud y Smart Cities.

4.1. Roles definidos por el Reglamento de IA

A continuación, se describen los roles reconocidos oficialmente por el RIA, conforme a sus artículos 3.3 a 3.9, y su aplicación práctica en los sectores de Salud y Smart Cities.

4.1.1. Proveedor:

Con arreglo al artículo 3, apartado 3, del RIA, se considera proveedor a toda persona física o jurídica, autoridad pública, agencia u otro organismo que desarrolle un sistema de inteligencia artificial o encargue su desarrollo y lo ponga en el mercado o lo ponga en servicio bajo su nombre o marca, con independencia de que el sistema se ofrezca a título oneroso o gratuito.

El proveedor es el sujeto jurídico principal del marco regulatorio y asume la responsabilidad directa sobre la conformidad técnica y documental del sistema con los requisitos establecidos en los artículos 8 a 15 del Reglamento. Entre estos se incluyen la gestión del riesgo, la gobernanza de los datos, la documentación técnica, la trazabilidad de registros, la transparencia, la supervisión humana, la robustez y la ciberseguridad. Esta figura abarca tanto a quienes desarrollan el sistema de IA por medios propios como a las entidades que subcontratan su desarrollo y lo comercializan bajo su denominación.

En el ámbito sanitario, el proveedor suele coincidir con los desarrolladores de software médico, laboratorios tecnológicos o centros de investigación que crean modelos de diagnóstico, predicción clínica o apoyo terapéutico.

En las Smart Cities, el rol corresponde habitualmente a empresas tecnológicas o integradores que diseñan soluciones de análisis predictivo, control del tráfico, eficiencia energética o gestión automatizada de servicios urbanos.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PUBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

El proveedor es el titular de las obligaciones de conformidad previa al mercado y del mantenimiento de dicha conformidad durante todo el ciclo de vida del sistema.

4.1.2. Responsable del despliegue

El artículo 3, apartado 4, del RIA define como responsable del despliegue a toda persona física o jurídica, autoridad pública, agencia u otro organismo que utilice un sistema de inteligencia artificial bajo su autoridad, salvo cuando el sistema se emplee en el marco de una actividad personal no profesional.

Esta figura representa al operador efectivo del sistema en el entorno en que se aplica y tiene la obligación de garantizar que la utilización del sistema se ajusta a la finalidad prevista y a las condiciones definidas por el proveedor. Su intervención marca la transición entre la fase de desarrollo y la de operación práctica.

El responsable del despliegue no es el titular de la conformidad técnica del sistema, pero debe asegurar su utilización conforme, segura y verificable, así como mantener la supervisión humana efectiva y la capacitación del personal que interactúa con la inteligencia artificial.

En el ámbito de la salud, este rol corresponde, por regla general, a centros hospitalarios, servicios clínicos o administraciones sanitarias que integran IA en sus procesos asistenciales o de gestión. En las Smart Cities, lo desempeñan ayuntamientos, empresas públicas o concesionarias que operan sistemas de control urbano, movilidad, energía o seguridad ciudadana.

El responsable del despliegue actúa, por tanto, como garante del uso legítimo y proporcional del sistema, dentro del marco técnico y jurídico definido por el Reglamento.

4.1.3. Fabricante

Según el artículo 3, apartado 6, del RIA, se entiende por fabricante a toda persona física o jurídica que fabrica o manda fabricar un producto que incorpora un sistema de inteligencia artificial o que utiliza dicho sistema como componente del producto, con vistas a su puesta en el mercado o en servicio bajo su nombre o marca.

Este rol se aplica cuando la inteligencia artificial forma parte de un producto físico regulado por otra normativa sectorial europea, como el Reglamento (UE) 2017/745 sobre productos sanitarios (MDR), el Reglamento (UE) 2017/746 sobre diagnóstico in vitro (IVDR) o el Reglamento (UE) 2023/2854 relativo a la ciberresiliencia de productos con elementos digitales (CRA).

En tales casos, el fabricante debe garantizar que la integración del sistema de IA no altera la conformidad global del producto ni compromete su seguridad. Esta figura puede corresponder, por ejemplo, a fabricantes de dispositivos médicos inteligentes, sistemas de monitorización, sensores urbanos o infraestructuras IoT que incorporan módulos de inteligencia artificial en su funcionamiento interno.

El fabricante se distingue del proveedor en que su responsabilidad deriva del producto final que contiene el sistema de IA, no necesariamente del desarrollo del algoritmo o modelo en sí.

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

4.1.4. Importador

El artículo 3, apartado 7, del RIA define como importador a toda persona física o jurídica establecida en la Unión que introduzca en el mercado de la Unión un sistema de inteligencia artificial procedente de un tercer país.

El importador desempeña una función de control previo a la comercialización, asegurando que los sistemas procedentes de fuera del territorio de la Unión cumplen todas las exigencias del Reglamento. Debe verificar la existencia de una evaluación de conformidad válida, el marcado CE, la declaración UE de conformidad y la documentación técnica en una lengua oficial de la Unión, así como conservar dicha documentación y colaborar con las autoridades competentes.

En los sectores de Salud y Smart Cities, el importador resulta especialmente relevante cuando se introducen en el mercado europeo plataformas, algoritmos o sistemas desarrollados en terceros países, cuya conformidad debe garantizarse antes de su despliegue operativo.

4.1.5. Distribuidor

Conforme al artículo 3, apartado 8, del RIA, se considera distribuidor a toda persona física o jurídica de la cadena de suministro, distinta del proveedor o del importador, que pone a disposición en el mercado un sistema de inteligencia artificial sin ser su proveedor ni su importador.

El distribuidor actúa en la fase intermedia de la cadena comercial y su función principal es verificar la integridad documental y la trazabilidad del sistema antes de su distribución. Está obligado a comprobar la presencia del marcado CE, la existencia de la documentación de conformidad y la ausencia de alteraciones que puedan afectar a la validez del sistema.

Aunque su papel no implica participación técnica en el diseño o uso del sistema, el distribuidor responde administrativamente en caso de comercializar sistemas no conformes. En la práctica, esta figura suele corresponder a integradores tecnológicos, empresas de reventa o entidades intermediarias que canalizan soluciones de IA hacia los usuarios finales

4.1.6. Representante autorizado

Por último, el artículo 3, apartado 9, del RIA define como representante autorizado a toda persona física o jurídica establecida en la Unión que haya recibido un mandato escrito de un proveedor para actuar en su nombre con respecto a determinadas tareas.

El representante autorizado es el interlocutor legal del proveedor ante las autoridades competentes y la Oficina Europea de Inteligencia Artificial, y resulta indispensable cuando el proveedor está establecido fuera de la Unión. Entre sus funciones figuran la custodia de la documentación técnica y de la declaración UE de conformidad, la cooperación en inspecciones o auditorías y la gestión de notificaciones relativas a incidentes o medidas correctoras.

En el sector sanitario, este rol guarda equivalencia funcional con el representante autorizado previsto en los Reglamentos MDR e IVDR, contribuyendo a la coherencia intersectorial del sistema regulatorio europeo.

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

4.2. Roles del reglamento en el ciclo de vida del sistema IA

El Reglamento (UE) 2024/1689 se articula sobre un enfoque basado en el ciclo de vida del sistema de inteligencia artificial, comprendido como la secuencia estructurada de fases que permiten gestionar su diseño, desarrollo, despliegue, supervisión y eventual retirada, con garantía de conformidad, seguridad y transparencia en todo momento.

Este enfoque se alinea con los marcos internacionales ISO/IEC 42001:2023 (Artificial Intelligence Management System), ISO/IEC 23894:2023 (Gestión de riesgos en IA) y el NIST AI Risk Management Framework (RMF 1.0).

Cada rol definido por el RIA, proveedor, responsable del despliegue, importador, distribuidor y representante autorizado, interviene en distintas fases de este ciclo, según el grado de autoridad técnica, control operativo o responsabilidad jurídica que ejerza sobre el sistema.

En algunos casos, la figura del fabricante mantiene un papel complementario, cuando la inteligencia artificial forma parte de un producto físico sometido a una regulación sectorial específica, pero no constituye un rol autónomo dentro del RIA.

Con el fin de facilitar la identificación de responsabilidades, se exponen a continuación **las fases en las que participan los roles identificados dentro del ciclo de vida** de un sistema de inteligencia artificial, junto con los roles que participan en cada una según el Reglamento (UE) 2024/1689:

I. Fase de diseño y desarrollo

Esta etapa constituye el origen del sistema de inteligencia artificial. Comprende el proceso completo de conceptualización, modelado, entrenamiento, validación técnica interna y documentación inicial del sistema, y abarca las decisiones sobre la finalidad del sistema, los criterios de funcionamiento, la selección de conjuntos de datos y los mecanismos de control de calidad y ciberseguridad aplicables durante el desarrollo.

La validación técnica interna tiene por objeto comprobar que el sistema funciona de acuerdo con sus especificaciones y cumple los requisitos técnicos y de rendimiento definidos por el proveedor antes de cualquier evaluación regulatoria o de conformidad. Incluye las pruebas internas de robustez, precisión y coherencia funcional del modelo, así como la verificación de los procesos de entrenamiento y del control de los datos empleados.

Rol principal:

El **proveedor** es el actor central de esta fase, al ejercer control directo sobre la concepción y validación del sistema y establecer las políticas de gestión del riesgo, gobernanza de datos, ciberseguridad y supervisión humana exigidas por los artículos 8 a 15 del RIA.

Entornos específicos:

- En **salud**, esta fase comprende la definición de la arquitectura del modelo, la validación técnica y la trazabilidad de los datos sanitarios, asegurando el cumplimiento del Reglamento (UE) 2016/679 (RGPD) y, cuando proceda, del Reglamento (UE) 2017/745 (MDR).

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

- En **Smart Cities**, abarca el diseño de sistemas de predicción de tráfico, eficiencia energética o gestión urbana basados en datos ciudadanos, respetando los principios de minimización y proporcionalidad en el tratamiento de datos personales.

II. Fase de evaluación y preparación para la puesta en el mercado

Una vez concluido el desarrollo, el sistema debe someterse a una evaluación de conformidad que verifique que cumple los requisitos esenciales establecidos por el RIA según su clasificación de riesgo (Título III, Capítulos 2 y 3).

Rol principal:

El **proveedor** conserva la responsabilidad principal en esta fase, debiendo realizar la evaluación directamente o a través de un organismo notificado (en el caso de encontrase fuera de la unión europea), y emitir la declaración UE de conformidad y el marcado CE cuando corresponda.

Roles cooperantes:

- El **representante autorizado**, en caso de que el proveedor esté fuera de la Unión Europea, asume la comunicación con las autoridades y la conservación de la documentación técnica.
- El **importador** puede participar verificando que los documentos de conformidad estén disponibles y actualizados.
- En productos mixtos, el **fabricante** coordina la compatibilidad del sistema con la legislación sectorial aplicable (MDR, IVDR, CRA).

Entornos específicos:

- En **salud**, la validación en esta fase corresponde a la evaluación externa de fiabilidad clínica, la verificación de la seguridad del paciente y la interoperabilidad con dispositivos o sistemas hospitalarios, complementando la validación técnica interna realizada durante la fase de desarrollo.
- En **Smart Cities**, la evaluación debe considerar el impacto sobre la seguridad pública, la privacidad y los derechos fundamentales de la ciudadanía, así como la integridad de las infraestructuras urbanas conectadas

III. Fase de comercialización e introducción en el mercado

Esta fase abarca todas las actividades de puesta a disposición del sistema de IA en el mercado de la Unión Europea, tanto por el proveedor como por los agentes intermedios. Se comienza cuando el sistema se pone a disposición en el mercado de la Unión Europea y se extiende hasta su distribución al usuario final. Es el momento en que el sistema deja de ser un prototipo o modelo interno y pasa a formar parte del circuito económico.

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

Rol principal:

El **proveedor** continúa siendo responsable de la conformidad regulatoria y de la exactitud de la documentación entregada con el sistema.

Roles cooperantes:

- **El importador** (cuando el sistema procede de un tercer país) debe comprobar que el sistema posee marcado CE, declaración de conformidad y documentación técnica completa, y conservar copia de dichos documentos.
- **El distribuidor** actúa como garante de la integridad documental, asegurando que no se han producido modificaciones que afecten a la validez de la conformidad.
- El **representante autorizado** se mantiene como interlocutor ante autoridades y supervisores europeos, especialmente ante la Oficina de Inteligencia Artificial de la UE (AI Office).

Entornos específicos:

- En sistemas de IA aplicados a salud pública o ciudades inteligentes, los intermediarios deben prestar especial atención a la cadena de custodia de software y a la verificación de actualizaciones, para evitar alteraciones que puedan comprometer la seguridad o la fiabilidad del sistema.

IV. Fase de despliegue y uso operativo

Esta fase corresponde al momento en que el sistema se utiliza efectivamente bajo la autoridad de una organización, generando resultados o decisiones que afectan a personas, infraestructuras o procesos. Es la etapa en que se materializan los riesgos y beneficios del sistema.

Rol principal:

El **responsable del despliegue** asume la autoridad funcional y la responsabilidad sobre el uso del sistema. Debe garantizar que se utiliza según la finalidad prevista, que existe supervisión humana adecuada, y que los usuarios internos cuentan con capacitación técnica suficiente.

Roles cooperantes:

- El **proveedor** presta soporte técnico y actualizaciones necesarias para mantener la conformidad y resolver incidencias.
- Cuando el sistema está embebido en un producto físico, el fabricante puede intervenir en mantenimiento o revisión de componentes.

Entornos específicos:

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

- En salud, el despliegue puede consistir en el uso de un sistema de apoyo al diagnóstico o triaje automatizado; el centro sanitario (responsable del despliegue) debe controlar su funcionamiento y registrar resultados.
- En Smart Cities, puede implicar el uso de algoritmos de predicción de tráfico o análisis de videovigilancia, cuya operación exige protocolos de control humano, limitación de uso y documentación de decisiones.

V. Fase de supervisión y seguimiento posterior al mercado

Esta fase comprende el periodo posterior a la puesta en el mercado o en servicio del sistema de inteligencia artificial, durante el cual debe mantenerse una vigilancia activa sobre su funcionamiento, rendimiento y posibles riesgos. Su finalidad es garantizar la conformidad continua, la seguridad y la protección de los derechos fundamentales a lo largo de toda la vida útil del sistema.

Roles principales:

- El **proveedor** es responsable de establecer y mantener el sistema formal de vigilancia posterior al mercado, de conformidad con el artículo 72 del RIA, recopilando y analizando la información recibida, evaluando los incidentes y adoptando medidas de correctoras o de notificación cuando proceda.
- El **responsable del despliegue** es responsable de ejercer el liderazgo operativo de la supervisión en el entorno real. Debe monitorizar el uso del sistema, registrar incidencias, comunicar los hallazgos al proveedor y aplicar medidas inmediatas de mitigación. Esta cooperación constituye la base práctica del sistema de vigilancia continua.

Roles cooperantes:

- El **representante autorizado**, cuando se considere necesario, canaliza la comunicación entre el proveedor y las autoridades y mantiene la documentación técnica actualizada.
- El **importador** y el **distribuidor** colaboran en la entrega de información y en la trazabilidad documental que las autoridades competentes puedan requerir.
- Cuando la IA esté integrada en un producto físico o dispositivo, el **fabricante** puede intervenir en las operaciones de mantenimiento, actualización o revisión de componentes para asegurar la conformidad continua del conjunto

Entornos específicos:

- En **salud,** esta fase incluye el seguimiento continuo del rendimiento clínico, el registro y análisis de incidentes y falsas alarmas, así como la comunicación de resultados al proveedor para la actualización del sistema o la adopción de medidas correctoras.
- En **Smart Cities**, comprende la monitorización del comportamiento del sistema en condiciones reales, la detección de desviaciones, vulnerabilidades o sesgos, y la actualización coordinada de medidas de seguridad y gobernanza con el proveedor y las autoridades competentes.

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

La vigilancia posterior a la puesta en el mercado debe integrarse en los sistemas internos de gestión de riesgos, calidad y cumplimiento normativo de la organización, documentarse de manera trazable y servir de base para las auditorías y la mejora continua del sistema de inteligencia artificial.

VI. Fase de retirada, desactivación o sustitución

Esta fase constituye la etapa final del ciclo de vida del sistema de inteligencia artificial y tiene por objeto garantizar su retirada o desactivación segura, la protección de los datos y registros generados durante su uso, y la conservación de la documentación técnica y de conformidad conforme a lo establecido en el RIA. Su correcta ejecución asegura que el cierre del ciclo de vida se lleve a cabo sin generar riesgos residuales para la salud, la seguridad o los derechos fundamentales, y que la información obtenida durante la operación y la vigilancia posterior al mercado se utilice para la mejora continua de futuros desarrollos.

Rol principal:

El **proveedor** conserva la responsabilidad principal en esta fase y debe cumplir las siguientes obligaciones específicas:

a) Planificación y ejecución de la retirada o desactivación.

Debe elaborar un procedimiento documentado que establezca las condiciones técnicas, jurídicas y de seguridad necesarias para poner fin a la operación del sistema. En caso de sustitución por una nueva versión, el proveedor verificará que la transición mantiene la conformidad regulatoria y la continuidad de las obligaciones de seguridad y supervisión.

b) Conservación y custodia de la documentación.

Conforme al artículo 72 del RIA, el proveedor garantizará la conservación de la documentación técnica, los registros de vigilancia posterior al mercado y los informes de conformidad durante el periodo mínimo exigido por la normativa aplicable. Esta obligación incluye la trazabilidad completa de las versiones y configuraciones retiradas.

c) Comunicación y cierre regulatorio.

Antes de la retirada definitiva, deberá notificar a las autoridades competentes cualquier incidente pendiente, medida correctora no resuelta o información relevante derivada del seguimiento posterior al mercado. Asimismo, coordinará con el responsable del despliegue las acciones necesarias para asegurar que el sistema quede efectivamente desactivado y libre de riesgo residual.

Roles cooperantes:

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PUBLICA SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

- El **responsable del despliegue** ejecuta la retirada o desactivación en el entorno operativo bajo su autoridad, garantizando la eliminación o anonimización segura de los datos tratados, la revocación de accesos y la desconexión de interfaces, verificando que el sistema no permanezca activo en ningún subsistema o servicio auxiliar.
- El **representante autorizado**, cuando es necesario, actúa como enlace entre el proveedor y las autoridades competentes, garantizando la custodia y entrega de la documentación final relativa a la conformidad y a la retirada.
- El **importador** y el **distribuidor** colaboran en la trazabilidad del sistema y en la entrega de la información que las autoridades soliciten, especialmente respecto de los lotes, versiones o configuraciones que deban retirarse del mercado.
- Cuando la inteligencia artificial esté integrada en un producto físico o dispositivo regulado por otra normativa europea, el **fabricante** coordina el proceso de sustitución o eliminación conforme a los requisitos específicos aplicables, incluidos, en su caso, los previstos en el Reglamento (UE) 2017/745 (MDR), el Reglamento (UE) 2023/2854 (CRA) y la Directiva 2012/19/UE (RAEE).

Entornos específicos:

- En salud, esta fase comprende la desactivación controlada de sistemas de apoyo clínico o diagnóstico, la conservación segura de historiales y registros generados durante su funcionamiento y la comunicación a las autoridades sanitarias competentes de los resultados obtenidos en el seguimiento final, conforme a los requisitos de trazabilidad y protección de datos del Reglamento (UE) 2016/679 (RGPD).
- En Smart Cities, incluye la planificación y ejecución de la retirada o sustitución de sistemas de análisis predictivo, control del tráfico, videovigilancia o gestión energética, garantizando la continuidad de los servicios públicos esenciales.

La fase de retirada, desactivación o sustitución debe integrarse en el sistema de gestión de calidad y de riesgos del operador económico, documentarse de forma trazable y conservarse junto con el resto de los registros del ciclo de vida del sistema de IA. Los resultados obtenidos, incluidos los informes finales de rendimiento, incidentes y lecciones aprendidas, constituirán la base para la mejora continua, la transparencia y el desarrollo responsable de nuevas soluciones de inteligencia artificial.

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

5. Determinación del rol aplicable a la organización

Este apartado establece el procedimiento mediante el cual las organizaciones pueden identificar su rol o combinación de roles dentro del marco regulatorio del Reglamento de Inteligencia Artificial (RIA), en función de su grado de intervención, responsabilidad y autoridad sobre el sistema de IA.

El objetivo es permitir que cada entidad determine con precisión las obligaciones que le corresponden, asegurando coherencia con los principios de rendición de cuentas y trazabilidad del Reglamento.

5.1. Formulario de autoevaluación

Cada organización deberá aplicar un procedimiento interno de autoevaluación para cada sistema de inteligencia artificial que desarrolle, adquiera o utilice, con el fin de determinar su rol conforme al artículo 3 del RIA.

La autoevaluación se realizará mediante un cuestionario estructurado que aborde los siguientes aspectos:

- Actividades de desarrollo o entrenamiento de modelos.
- Introducción del sistema en el mercado o puesta en servicio.
- Uso operativo o supervisión bajo autoridad propia.
- Importación, distribución o intermediación en la cadena de suministro.
- Representación de terceros ante autoridades competentes.

El cuestionario se completará de forma independiente para cada sistema de IA identificado en el inventario de la organización y deberá conservarse como parte integrante de su documentación regulatoria.

Pregunta	Respuesta	Resultado
¿El sistema de inteligencia artificial es puesto en el mercado o puesto en servicio dentro del territorio de la Unión Europea, o sus resultados se utilizan en la UE?	☐ Si ☐ No	**Sí:** El sistema entra en el ámbito de aplicación del RIA (art. 2). Continúe con la siguiente pregunta. **No:** El sistema está fuera del ámbito territorial del RIA. No aplica.
¿La organización realiza actividades relacionadas con el sistema de IA (desarrollo, distribución o uso) en el marco de una actividad profesional o comercial, y no únicamente persona?	☐ Sí ☐ No	**Sí:** El sistema está sujeto al RIA. Continúe con la siguiente pregunta. **No:** El uso es doméstico y está exento (art. 2.5).

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

¿Desarrolla su organización el sistema de inteligencia artificial, total o parcialmente, por medios propios?	☐ Si ☐ No	**Sí:** Es Proveedor (art. 3.3). *Anótelo y continúe*. Podría también asumir otros roles (p. ej. responsable del despliegue o importador). **No:** Pase a la siguiente pregunta.
¿Encarga su organización a un tercero el desarrollo del sistema de IA bajo su propio nombre o marca comercial?	☐ Si ☐ No	**Sí:** Es Proveedor (art. 3.3). Continúe con la siguiente pregunta (posible rol combinado). **No:** Continúe a la siguiente pregunta.
¿Pone su organización por primera vez el sistema de IA en el mercado o lo pone en servicio dentro de la Unión Europea, bajo su nombre o marca, con o sin ánimo de lucro?	☐ Si ☐ No	**Sí:** Es Proveedor (art. 3.3). Si además lo utiliza internamente: también es Responsable del despliegue (art. 3.4). Continúe con la siguiente pregunta. **No:** Continúe a la siguiente pregunta.
¿Ha modificado su organización de manera sustancial un sistema de IA existente o cambiado su finalidad prevista?	☐ Si ☐ No	**Sí:** Se convierte en el nuevo proveedor del sistema (art. 3.23). Continúe con la siguiente pregunta. **No:** Continúe a la siguiente pregunta.
¿Integra su organización el sistema de IA como componente de seguridad o funcionalidad esencial en un producto físico que comercializa bajo su marca (por ejemplo, dispositivo médico, vehículo, sensor o infraestructura)?	☐ Si ☐ No	**Sí:** Es Fabricante/Proveedor conforme al RIA y la legislación sectorial (MDR, IVDR, CRA). Continúe a la siguiente pregunta para comprobar si tiene rol combinado de Proveedor y responsable de despliegue. **No**: Continúe a la siguiente pregunta.

Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia
Junta de Andalucía
Agencia Digital de Andalucía

¿Utiliza su organización el sistema de IA bajo su propia autoridad para tomar decisiones o generar resultados que afectan a personas, bienes, servicios o procesos?	☐ Si ☐ No	**Sí:** Es Responsable del despliegue (art. 3.4). Si además desarrolla, encarga o modifica el sistema, rol combinado: Proveedor y responsable del despliegue. Continúe con la siguiente pregunta (posible importación o distribución). **No:** Continúe a la siguiente pregunta.
¿Importa su organización un sistema de IA o un producto que incorpora IA desde un país tercero para su puesta en el mercado o en servicio dentro de la Unión Europea?	☐ Si ☐ No	**Sí:** Es Importador (art. 3.7). Continúe con la pregunta 11. Si además lo usa directamente: también es Responsable del despliegue (art. 3.4). Si además lo comercializa dentro de la UE: también es Distribuidor (art. 3.8). **No:** Continúe con la pregunta 11.
¿Distribuye o revende su organización un sistema de IA dentro del mercado de la Unión sin ser su proveedor ni su importador (por ejemplo, como revendedor o integrador)?	☐ Si ☐ No	**Sí:** Es Distribuidor (art. 3.8). Si además importa: Importador y Distribuidor. Si además utiliza el sistema internamente: Distribuidor y responsable del despliegue. **No:** Continúe con la siguiente pregunta.
¿Ha sido su organización designada mediante mandato escrito por un proveedor establecido fuera de la UE para actuar en su nombre ante autoridades competentes o conservar documentación técnica?	☐ Si ☐ No	**Sí:** Es Representante autorizado (art. 3.9). Continúe con la siguiente pregunta. **No:** Continúe con la siguiente pregunta.
¿Realiza su organización tareas de mantenimiento, actualización o modificación sobre un sistema de IA ya desplegado por terceros que puedan alterar su rendimiento o finalidad? (p. ej. “fine-tuning”, adaptación de modelo, o integración de nuevas fuentes de datos)	☐ Si ☐ No	**Sí:** Podría convertirse en nuevo Proveedor si la modificación es sustancial (art. 3.23). Debe reevaluar la conformidad del sistema y registrar el cambio de rol. **No:** Continúe con la siguiente pregunta.

¿Ha determinado que su organización asume uno o varios roles según el sistema de IA concreto?	☐ Si ☐ No	**Sí:** Registre los roles identificados (Proveedor, responsable del despliegue, Importador, Distribuidor, Representante autorizado o combinación). Conserve esta información en sus registros internos. **No:** La organización no desempeña ningún rol operativo dentro del ámbito del RIA, sin perjuicio de futuras revisiones si cambia su grado de intervención.

TABLA 2: FORMULARIO DE AUTOEVALUACIÓN DEL ROL

5.2. Resultados y trazabilidad

El resultado del proceso de autoevaluación permitirá vincular el rol determinado con las obligaciones regulatorias correspondientes, garantizando la coherencia con la clasificación de riesgos establecida en la guía anterior.

La información obtenida deberá conservarse en registros internos que aseguren la trazabilidad del proceso y la rendición de cuentas. El resultado del proceso de autoevaluación permitirá asignar uno o varios roles a la organización en relación con cada sistema de inteligencia artificial.

Dicha asignación constituirá la referencia oficial interna para determinar las obligaciones regulatorias aplicables y las medidas de cumplimiento asociadas.

Los resultados deberán:

- Registrarse formalmente en los sistemas internos de gestión de cumplimiento o de calidad.
- Vincularse al inventario de sistemas de IA definido en el apartado 6.2.
- Mantenerse actualizados ante cualquier cambio en la finalidad, titularidad o modo de operación del sistema.
- Servir como trazabilidad documental en auditorías, inspecciones o revisiones de conformidad.

Cada registro de autoevaluación deberá incluir, al menos:

- ✓ Identificación del sistema de IA.
- ✓ Fecha de evaluación y responsable interno.
- ✓ Roles identificados según el artículo 3 del RIA.
- ✓ Nivel de riesgo asignado (según la guía de clasificación).
- ✓ Observaciones y justificación de la decisión cuando se aplica.

La trazabilidad del proceso de determinación del rol es esencial para garantizar la **rendición de cuentas** y demostrar el cumplimiento del RIA ante las autoridades competentes o ante la Oficina Europea de Inteligencia Artificial.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PUBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

5.3. Casos de rol único y rol combinado

Dependiendo de la naturaleza de sus actividades, una organización puede desempeñar un único rol o una combinación de varios dentro del ciclo de vida del sistema de inteligencia artificial.

Estos roles corresponden a las figuras descritas en la sección anterior, que abarcan desde el desarrollo inicial hasta el uso operativo y la retirada del sistema.

I. Rol único

Se produce cuando la entidad interviene exclusivamente en una fase del ciclo de vida del sistema, sin asumir responsabilidades adicionales.

Ejemplos:

- Un hospital que utiliza un sistema de IA desarrollado por un tercero actúa únicamente como responsable del despliegue.
- Una empresa tecnológica que desarrolla y comercializa una plataforma de IA sin utilizarla internamente actúa únicamente como proveedor.

II. Rol combinado

Existen situaciones en las que una misma entidad asume múltiples funciones, de forma simultánea o secuencial, dentro del ciclo de vida del sistema.

Ejemplos habituales incluyen:

- Una empresa que desarrolla un sistema de IA y lo utiliza internamente: Proveedor y responsable del despliegue.
- Una entidad que importa adapta y revende un sistema de IA en la UE: Importador y distribuidor.
- Una compañía que desarrolla un modelo de IA y lo integra en un dispositivo físico: Proveedor y fabricante.

Cuando una entidad desempeñe más de un rol, deberá aplicar el principio de mayor responsabilidad, cumpliendo el conjunto de obligaciones más estricto entre los que correspondan a sus funciones.

Además, la identificación de roles debe interpretarse en continuidad con las fases del ciclo de vida descritas previamente, garantizando que la responsabilidad regulatoria de cada figura se mantiene desde el diseño del sistema hasta su retirada.

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

6. Obligaciones generales

El Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, establece una serie de obligaciones generales que resultan de aplicación a todas las entidades que desarrollen, desplieguen o utilicen sistemas de inteligencia artificial (IA) en el territorio de la Unión Europea, independientemente del nivel de riesgo del sistema.

Estas obligaciones, recogidas en los artículos 4, 5 y 6 del RIA, se aplican principalmente a los proveedores y responsables del despliegue, y constituyen los pilares del marco de cumplimiento horizontal sobre el que se construyen las obligaciones específicas por nivel de riesgo desarrolladas en el apartado siguiente.

A continuación, se detallan las obligaciones generales aplicables a todas las organizaciones comprendidas en el ámbito del Reglamento.

✓ Alfabetización en inteligencia artificial

Las organizaciones deberán adoptar medidas adecuadas para garantizar que el personal y las personas que actúen en su nombre en el desarrollo, operación, supervisión o uso de sistemas de IA dispongan de un nivel suficiente de alfabetización en materia de inteligencia artificial.

Dicha alfabetización debe ser proporcional a las funciones desempeñadas e incluir:

- Comprensión básica del funcionamiento de los sistemas de IA y sus limitaciones.
- Conocimiento de los riesgos potenciales y de las medidas de mitigación aplicables.
- Capacitación en materia de supervisión humana, seguridad, sesgos y protección de datos.
- Formación continuada para mantener la competencia técnica frente a la evolución tecnológica.

El nivel de formación exigible deberá tener en cuenta:

- Los conocimientos técnicos, la experiencia y el perfil del personal.
- El contexto de uso del sistema.
- Los colectivos o personas potencialmente afectados por sus resultados.

Las entidades deberán conservar evidencia documental del cumplimiento de esta obligación (planes formativos, registros de asistencia, materiales, certificaciones o evaluaciones).

✓ Inventario de sistemas de inteligencia artificial

Todas las entidades deberán elaborar y mantener actualizado un inventario completo de los sistemas de inteligencia artificial que desarrollen, adquieran, desplieguen o utilicen.

El inventario deberá:

- Incluir todos los sistemas de IA utilizados de forma profesional o comercial, propios o de terceros.
- Recoger información mínima sobre: finalidad, proveedor, tecnología base (modelo, versión, proveedor), nivel de riesgo, contexto de uso, fecha de introducción y responsable interno.
- Estar disponible para las autoridades competentes cuando sea requerido.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PUBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

- Ser revisado y actualizado periódicamente, especialmente tras la modificación o sustitución de sistemas.

El inventario constituye el punto de partida para la aplicación del Reglamento, ya que permite identificar los sistemas sometidos al RIA y facilita la posterior clasificación de riesgos y asignación de obligaciones específicas.

✓ **Clasificación y análisis de impacto**

A partir del inventario de sistemas, las organizaciones deberán realizar una clasificación de cada sistema de IA conforme a las categorías de riesgo establecidas en el Reglamento.

La clasificación deberá fundamentarse en los criterios establecidos en los artículos 5 y 6 y, en su caso, en los anexos de la guía "Clasificación de sistemas de IA en entornos de Salud y Smart Cities".

Asimismo, las organizaciones deberán realizar un análisis de impacto que valore:

- Los posibles efectos del sistema sobre los derechos fundamentales, la seguridad y la salud.
- La proporcionalidad de su uso respecto a los fines perseguidos.
- La necesidad de aplicar medidas adicionales de mitigación, supervisión o transparencia.

El resultado del análisis deberá conservarse en la documentación interna y vincularse al expediente de cada sistema.

✓ **Gobernanza y responsabilidad interna**

Las organizaciones deberán establecer una estructura organizativa y de gobernanza que asegure el cumplimiento de las obligaciones del RIA, incluyendo:

- Designación de un responsable interno de cumplimiento del RIA o equipo equivalente.
- Integración de las funciones de IA dentro del sistema general de gestión de riesgos y cumplimiento.
- Conservación de registros documentales sobre los procesos de toma de decisiones relativos a la IA.

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

7. Obligaciones regulatorias según nivel de riesgo

El presente apartado establece las obligaciones regulatorias que las organizaciones deben cumplir en función del nivel de riesgo de sus sistemas de inteligencia artificial, conforme al Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, relativo a la Inteligencia Artificial (RIA).

La clasificación de riesgos utilizada se corresponde con la definida en la Guía de clasificación de sistemas de IA en entornos de salud y Smart Cities, de forma que cada nivel de riesgo determina las medidas, responsabilidades y controles aplicables a los distintos actores: proveedor, responsable del despliegue, importador, distribuidor, representante autorizado u operador.

El objetivo es proporcionar una referencia práctica que permita a las entidades conocer con precisión qué obligaciones deben cumplir según el nivel de riesgo del sistema y el rol de la organización sobre este sistema en la cadena de valor, promoviendo así la coherencia regulatoria y la trazabilidad del cumplimiento.

7.1. Niveles de Riesgo

7.1.1. Riesgo prohibido

Los sistemas de IA de riesgo inaceptable o prohibido son aquellos que constituyen una amenaza manifiesta para los derechos fundamentales de las personas, su dignidad o la seguridad pública.

Conforme al artículo 5 del RIA, estos sistemas están estrictamente prohibidos en la Unión Europea, al considerarse incompatibles con los valores democráticos y con el acervo jurídico de la Unión. El incumplimiento de estas disposiciones puede dar lugar a sanciones administrativas grave.

Ejemplos de sistemas prohibidos:

- Tecnologías de **puntuación social** desarrolladas o utilizadas por empresas o entidades privadas para evaluar o clasificar a personas físicas.
- Sistemas de IA que utilicen **técnicas subliminales o de manipulación** del comportamiento humano de manera que puedan causar daños físicos o psicológicos
- **Reconocimiento facial y biométrico en tiempo real** en espacios públicos con fines de aplicación de la ley, salvo excepciones limitadas y autorizadas conforme al artículo 5.1, letra d).
- Sistemas que **exploten vulnerabilidades de grupos vulnerables** (menores, personas con discapacidad o dependencia) para influir indebidamente en su comportamiento.

Obligaciones por rol:

- **Proveedor:** debe identificar, bloquear y abstenerse de poner en el mercado o en servicio sistemas incluidos en esta categoría. Está obligado a notificar inmediatamente a las autoridades competentes cualquier indicio de incumplimiento o uso no autorizado.

- **Responsable del despliegue**: debe garantizar que no se utilicen sistemas de IA prohibidos en sus operaciones. En caso de detección, deberá suspender su uso y activar procedimientos internos de retirada y comunicación a las autoridades.

- **Importador y distribuidor:** deben verificar, antes de la puesta en el mercado, que los sistemas que comercializan no pertenecen a esta categoría. Deberán mantener trazabilidad documental y adoptar medidas correctoras ante cualquier incumplimiento.

7.1.2. Riesgo alto

Los sistemas de IA de alto riesgo son aquellos que, por su naturaleza, finalidad o ámbito de aplicación, pueden tener un impacto significativo sobre la seguridad, la salud o los derechos fundamentales de las personas. Se encuentran recogidos en el Anexo III del Reglamento e incluyen, entre otros, los sistemas utilizados en la práctica médica para diagnóstico asistido, planificación quirúrgica o monitorización de pacientes, los empleados en la evaluación de personas físicas como procesos de selección de personal o admisión educativa, los que determinan el acceso a servicios esenciales como el suministro energético, el agua o el transporte, y los utilizados para la gestión de infraestructuras críticas y servicios urbanos automatizados dentro de las denominadas ciudades inteligentes.

En estos ámbitos, un fallo de funcionamiento puede comprometer la vida o la salud de las personas, afectar a la continuidad de servicios esenciales o vulnerar derechos fundamentales. Por ello, el Reglamento impone un conjunto reforzado de obligaciones de cumplimiento, supervisión, trazabilidad y gobernanza a todos los operadores económicos que intervienen en el ciclo de vida del sistema.

Obligaciones de sistema de alto riesgo según el rol:

- **Proveedor:**

  El proveedor del sistema de IA de alto riesgo es el responsable de garantizar que el producto cumple plenamente con los requisitos aplicables, incluyendo:

  - ✓ **Cumplimiento normativo:** Cumplir con todas las obligaciones regulatorias aplicables, incluyendo la implementación de un sistema documentado de gestión de calidad, la elaboración de la documentación técnica, la realización de evaluaciones de conformidad, el marcado CE y el registro en la base de datos de la UE. El proveedor debe poder justificar que ha desarrollado y conservado toda la evidencia técnica necesaria para demostrar su conformidad, garantizando además que no existan duplicidades con otras normativas sectoriales como la de productos sanitarios o dispositivos eléctricos.

  - ✓ **Gestión de riesgos:** Debe establecer, documentar y mantener un sistema de gestión de riesgos que cubra todo el ciclo de vida del sistema. Este sistema debe identificar los riesgos razonablemente previsibles, analizarlos, evaluarlos y mitigarlos mediante controles técnicos y organizativos. En salud, se integrará con los mecanismos de gestión de riesgos clínicos y seguridad del paciente; en Smart Cities, debe abarcar

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

interdependencias entre sistemas urbanos interconectados, como semáforos inteligentes, redes eléctricas y transporte autónomo.

- ✓ **Gobernanza y gestión de datos:** Los conjuntos de datos empleados para el entrenamiento, validación y prueba deben ser pertinentes, representativos, libres de errores y completos. Se debe garantizar la trazabilidad del origen de los datos, su tratamiento ético y la protección de los datos personales conforme al RGPD. En salud, los datos deberán ser clínicamente validados y anonimizarse adecuadamente; en ciudades inteligentes, deberán eliminarse los identificadores personales procedentes de sensores, cámaras u otros dispositivos urbanos.

- ✓ **Documentación técnica y trazabilidad**: Desarrollar y mantener una documentación técnica completa que demuestre el cumplimiento del sistema con los requisitos regulatorios. Esta debe incluir la arquitectura, el diseño, los algoritmos, los procesos de entrenamiento y validación, las métricas de rendimiento y los resultados de las evaluaciones de conformidad. Además, el sistema debe contar con la capacidad de registrar automáticamente los eventos y operaciones significativas que permitan la trazabilidad completa de su funcionamiento y de las modificaciones introducidas a lo largo del tiempo.

- ✓ **Transparencia y supervisión humana:** El sistema debe diseñarse de modo que sus resultados sean comprensibles e interpretables para los responsables del despliegue. Deben proporcionarse instrucciones de uso claras, concisas y accesibles, que describan su finalidad, requisitos, limitaciones, riesgos residuales y mecanismos de control humano. Debe garantizarse que el operador humano pueda intervenir, ajustar o detener el sistema cuando sea necesario, asegurando una supervisión eficaz.

- ✓ **Precisión, robustez y ciberseguridad:** El sistema de IA debe alcanzar y mantener niveles adecuados de precisión, solidez y ciberseguridad. El proveedor debe definir métricas cuantificables, realizar pruebas de estrés y establecer medidas de protección frente a errores, fallos y ataques adversariales. En el ámbito sanitario, los márgenes de error deben ser clínicamente aceptables; en ciudades inteligentes, debe asegurarse la resiliencia operativa ante caídas de red o interferencias.

- ✓ **Conservación de documentación y registros:** El proveedor debe conservar toda la documentación técnica, la relativa al sistema de gestión de calidad, las decisiones de los organismos notificados y la declaración UE de conformidad durante al menos diez años desde su puesta en el mercado o en servicio. Esta documentación debe mantenerse en formato electrónico y estar disponible para las autoridades competentes.

- ✓ **Medidas correctoras y cooperación:** Cuando un sistema no cumpla los requisitos del Reglamento, el proveedor debe adoptar de inmediato medidas correctoras, como su modificación, retirada o inutilización, notificando las acciones al resto de operadores y

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

a las autoridades. Debe también cooperar plenamente en las investigaciones, facilitando la documentación necesaria.

- ✓ **Representación en la UE:** Los proveedores establecidos fuera de la Unión deben designar un representante autorizado mediante mandato escrito. Este actuará como interlocutor con las autoridades, custodiará la documentación técnica y conservará la declaración UE de conformidad durante diez años.

- ✓ **Vigilancia poscomercialización:** Debe establecerse un sistema de vigilancia proporcional al nivel de riesgo del sistema, que recopile y analice datos sobre su rendimiento y los posibles incidentes. Cualquier incidente grave deberá notificarse a las autoridades competentes en un plazo máximo de quince días desde su detección o de dos días si implica un riesgo inminente para la salud o seguridad pública.

- ✓ **Registro en la base de datos de la UE:** Antes de la comercialización o puesta en servicio, el proveedor debe registrar el sistema de IA de alto riesgo en la base de datos oficial de la Unión Europea, incluyendo la información técnica y administrativa necesaria para su trazabilidad y supervisión.

- **Responsable de despliegue:**

  - ✓ **Cumplimiento normativo**: El responsable del despliegue debe garantizar que cada sistema de IA de alto riesgo se utilice únicamente conforme a la finalidad prevista por el proveedor y en condiciones controladas y seguras. Debe adoptar las medidas técnicas y organizativas necesarias para evitar usos indebidos, alteraciones o desviaciones que puedan comprometer la seguridad, la salud o los derechos fundamentales. Cuando el despliegue se produzca en entornos críticos, como hospitales o infraestructuras urbanas, el responsable deberá disponer de procedimientos específicos de verificación antes de la puesta en servicio y durante toda la operación.

  - ✓ **Supervisión humana y control operativo:** Se requiere asegurar una supervisión humana efectiva a lo largo de toda la vida operativa del sistema. El responsable debe definir los límites de autonomía, los protocolos de intervención y los mecanismos para la detección de comportamientos anómalos. En el ámbito sanitario, la supervisión humana implica que un profesional médico conserve la capacidad de validar o anular cualquier decisión automatizada; en entornos urbanos inteligentes, la autoridad local o el operador debe poder suspender de inmediato decisiones automatizadas que afecten al tráfico, la energía o la seguridad ciudadana.

  - ✓ **Formación y alfabetización en IA:** El personal que intervenga en el uso, mantenimiento o supervisión del sistema debe contar con la formación y competencia técnica necesarias para comprender sus capacidades, limitaciones y riesgos. La empresa

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

responsable debe desarrollar planes formativos documentados que abarquen la detección de fallos, la gestión de incidentes y los procedimientos de parada segura.

- ✓ **Evaluación de impacto sobre derechos fundamentales y protección de datos**: Antes del despliegue, el responsable debe realizar una evaluación de impacto relativa a los derechos fundamentales, la salud, la seguridad y la protección de datos, conforme a los artículos 26 y 27 del Reglamento y al RGPD. La evaluación debe incluir el propósito del uso, las categorías de personas afectadas, los riesgos específicos y las medidas de mitigación previstas. Sus resultados deben notificarse a la autoridad competente y conservarse como parte de la documentación del sistema.

- ✓ **Transparencia y comunicación**: Las personas afectadas por el uso del sistema deben ser informadas de forma clara sobre su funcionamiento, finalidad, posibles impactos y uso de datos personales. En el lugar de trabajo, los representantes de los trabajadores deberán ser notificados antes de la implementación de sistemas que evalúen o monitoricen el desempeño laboral.

- ✓ **Registro y conservación de datos:** El responsable del despliegue debe garantizar la conservación de los registros generados automáticamente por el sistema durante un periodo mínimo de seis meses, salvo que otra normativa sectorial exija un plazo mayor. Estos registros deben mantenerse seguros y disponibles para las autoridades en caso de auditoría o incidente.

- ✓ **Medidas técnicas y organizativas:** Se deberán establecer procedimientos internos de calibración, mantenimiento y revisión periódica del sistema, así como protocolos para su desactivación segura en caso de fallo. El responsable debe garantizar la coherencia entre las instrucciones del proveedor y las prácticas de uso internas.

- ✓ **Notificación de incidentes y retroalimentación:** Cualquier incidente grave o desviación significativa del comportamiento previsto del sistema deberá notificarse al proveedor y a las autoridades competentes sin dilación. El responsable debe mantener un registro documentado de incidentes, acciones correctoras y medidas preventivas, garantizando la retroalimentación continua hacia el proveedor para la mejora del sistema.

- **Importador:**

  - ✓ **Verificación de conformidad:** Antes de introducir un sistema de IA de alto riesgo en el mercado de la Unión, el importador debe verificar que el proveedor ha completado correctamente el procedimiento de evaluación de conformidad ha elaborado la documentación técnica, ha emitido la declaración UE de conformidad y ha colocado el marcado CE.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PUBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

- ✓ **Trazabilidad y cooperación**: El importador debe conservar la documentación relevante durante al menos diez años y garantizar la trazabilidad del sistema desde su origen hasta su comercialización. Está obligado a cooperar con las autoridades competentes, proporcionando cualquier información o registro que se le requiera.

- ✓ **Medidas correctoras y suspensión de comercialización:** Si detecta que un sistema no cumple los requisitos, presenta falsificaciones o riesgos graves, el importador debe abstenerse de introducirlo en el mercado y comunicarlo inmediatamente al proveedor, al representante autorizado y a las autoridades de vigilancia del mercado. También deberá adoptar medidas correctoras para retirar el producto cuando proceda

- **Distribuidor:**

  - ✓ **Control previo a la distribución**: El distribuidor debe asegurarse, antes de comercializar un sistema de IA de alto riesgo, de que este lleva el marcado CE, dispone de declaración UE de conformidad y de instrucciones de uso completas. Asimismo, debe verificar que el proveedor e importador han cumplido todas las obligaciones reglamentarias.

  - ✓ **Garantía de integridad y almacenamiento seguro**: Durante el almacenamiento y transporte, el distribuidor debe adoptar medidas que impidan el deterioro o modificación del sistema que pueda comprometer su conformidad.

  - ✓ **Detección de riesgos y comunicación:** Si sospecha que un sistema no es conforme, el distribuidor debe abstenerse de comercializarlo y comunicarlo al proveedor o importador, así como a las autoridades si persisten los riesgos. Debe conservar los registros de las acciones correctoras adoptadas y cooperar en las inspecciones.

- **Representante autorizado:**

  - ✓ **Mandato y funciones:** El representante autorizado actúa en nombre del proveedor y como interlocutor ante las autoridades competentes y la Oficina Europea de IA. Su mandato debe establecerse por escrito antes de la comercialización.

  - ✓ **Custodia de documentación y cooperación institucional:** Debe custodiar la documentación técnica y la declaración UE de conformidad durante un mínimo de diez años, y ponerlas a disposición de las autoridades cuando se le solicite. También debe cooperar plenamente en inspecciones y auditorías, notificando al proveedor cualquier incumplimiento detectado.

  - ✓ **Finalización del mandato**: El representante está obligado a poner fin a su mandato si el proveedor incumple gravemente sus obligaciones regulatorias, informando a las autoridades competentes de esta circunstancia.

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

7.1.3. Riesgo limitado

Esta categoría comprende los sistemas de IA cuyo uso implica interacción directa con personas, sin generar riesgos significativos para su seguridad o sus derechos, pero que requieren transparencia reforzada conforme al artículo 52 del Reglamento.

Entre estos sistemas se incluyen los agentes conversacionales o chatbots, las herramientas de generación de contenido sintético en texto, imagen, audio o vídeo, y las aplicaciones de reconocimiento de emociones o categorización biométrica.

Aunque su impacto potencial es menor, su uso indebido puede afectar la confianza del público, la privacidad o la percepción de veracidad de la información. Por ello, se exige informar de manera clara cuando las personas interactúan con una máquina o con contenidos generados artificialmente, y aplicar medidas adecuadas de supervisión y responsabilidad.

Obligaciones de sistema de riesgo limitado según el rol:

- **Proveedor:**

  ✓ **Transparencia y comunicación clara:** El proveedor debe garantizar que las personas sepan en todo momento que están interactuando con un sistema de inteligencia artificial. Esta información debe proporcionarse antes o durante la interacción, mediante avisos visibles, mensajes automáticos o etiquetas que indiquen claramente "interacción automatizada" o "contenido generado por IA". En entornos sensibles, como los servicios médicos o las comunicaciones institucionales, estos avisos deben ser comprensibles para usuarios con distintos niveles de alfabetización digital.

  ✓ **Supervisión humana:** El proveedor debe diseñar el sistema de modo que las personas encargadas de su operación puedan supervisar, interrumpir o corregir su funcionamiento en cualquier momento. La supervisión humana efectiva incluye la capacidad de detener procesos automáticos, revisar decisiones generadas y garantizar que los resultados no se apliquen de forma ciega o irreversible.

  ✓ **Identificación de contenido sintético**: Si el sistema genera o manipula contenido (texto, imagen, vídeo o audio), debe marcarlo con metadatos o etiquetas visibles que lo identifiquen como generado o alterado artificialmente. Esto garantiza la trazabilidad y evita usos fraudulentos o desinformativos.

- **Responsable del despliegue**

  ✓ **Obligación de transparencia:** Debe garantizar la transparencia hacia las personas afectadas, informándoles del funcionamiento y finalidad del sistema y obteniendo su consentimiento cuando se traten datos personales. Si se utilizan sistemas de reconocimiento emocional o categorización biométrica, el responsable debe notificar su uso y cumplir con la normativa de protección de datos. En el caso de deepfakes o textos

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

generados para informar al público, deberá divulgarse que el contenido ha sido producido o modificado mediante IA.

- ✓ **Evaluación del nivel técnico y experiencia del personal:** Antes del uso, el responsable debe evaluar la capacitación del personal que interactuará con el sistema. Esto incluye verificar su conocimiento sobre el funcionamiento, limitaciones y posibles impactos del sistema en los usuarios.

- ✓ **Aviso sobre contenidos generados o manipulados artificialmente:** Si el sistema produce o modifica contenido audiovisual que pueda inducir a error, el responsable debe advertirlo explícitamente al público, especificando que el material ha sido creado o alterado mediante IA. Esta obligación se aplica especialmente en entornos donde la veracidad del contenido sea relevante para la seguridad, la salud o la reputación de personas físicas o jurídicas.

7.1.4. Riesgo mínimo

Los sistemas de IA de riesgo mínimo presentan un impacto limitado sobre los derechos y la seguridad de las personas, y no están sujetos a obligaciones regulatorias obligatorias. Se incluyen en esta categoría los filtros de spam, los sistemas de recomendación internos, los asistentes de productividad y los videojuegos basados en IA.

Aunque no están regulados con carácter obligatorio, se recomienda adoptar buenas prácticas de gobernanza que refuercen la confianza, la seguridad y la ética tecnológica.

- **Buenas prácticas recomendadas:**

  - ✓ **Documentación básica del sistema:** Aunque no sea obligatorio, las organizaciones deberían documentar de forma sencilla las funciones principales del sistema, sus limitaciones y su ámbito de uso previsto. Esta documentación permite mantener el control sobre la evolución del sistema y facilita auditorías internas en caso de incidencias.

  - ✓ **Supervisión periódica y revisión técnica:** Los responsables deben revisar periódicamente el rendimiento del sistema para detectar posibles sesgos, desviaciones o resultados inesperados. En entornos urbanos, por ejemplo, un sistema de recomendación de rutas o un chatbot de atención ciudadana debe evaluarse para evitar comportamientos discriminatorios o errores persistentes.

  - ✓ **Aplicación de códigos de conducta:** Se recomienda que las organizaciones adopten estándares y códigos de conducta éticos, como la norma ISO/IEC 42001 sobre gestión responsable de la IA. Estos marcos promueven la transparencia, la rendición de cuentas y la mejora continua del desempeño tecnológico.

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

7.1.5. Modelos de inteligencia artificial de propósito general (GPAI)

Los modelos de Inteligencia Artificial de Propósito General (GPAI) son aquellos que presentan una generalidad significativa y son capaces de ejecutar de forma competente una amplia gama de tareas, independientemente de la forma en que se comercialicen o distribuyan. Estos modelos pueden integrarse en diversos sistemas de IA o aplicaciones posteriores, incluidos los de alto riesgo, y su comportamiento puede influir en múltiples sectores simultáneamente.

El Reglamento (UE) 2024/1689 relativo a la Inteligencia Artificial (RIA) establece un conjunto de obligaciones específicas para los modelos GPAI, dirigidas a reforzar la transparencia, la trazabilidad y la gobernanza responsable. Estas medidas buscan prevenir riesgos derivados del uso indebido, promover la seguridad técnica y garantizar el cumplimiento del Derecho de la Unión, en particular en materia de protección de datos, derechos de autor y propiedad intelectual.

En el contexto de Salud, los GPAI pueden utilizarse como base para sistemas de apoyo diagnóstico, análisis predictivos o asistentes clínicos automatizados. En Smart Cities, su uso se orienta hacia sistemas de predicción de tráfico, gestión energética inteligente o generación de contenido automatizado para servicios urbanos.

Los modelos GPAI deben disponer de documentación que describa sus capacidades, limitaciones, arquitectura, procesos de entrenamiento, tipo de datos empleados, consumo de recursos y medidas de ciberseguridad implementadas. Asimismo, deben establecer políticas claras de uso aceptable, mecanismos de supervisión y procedimientos de revisión periódica.

Antes de detallar las obligaciones por rol, conviene señalar que, en el caso de los Modelos de Inteligencia Artificial de Propósito General (GPAI), el Reglamento (UE) 2024/1689 centra las obligaciones específicas en los roles de proveedor y responsable del despliegue. Los demás operadores económicos, como el importador, el distribuidor, el representante autorizado o el fabricante, no asumen obligaciones adicionales específicas en este contexto, salvo cuando actúen efectivamente como proveedores o desplieguen el sistema bajo su propia autoridad.

Obligaciones de modelos de IA de propósito general según el rol:

- **Proveedor:**

El Reglamento establece que el proveedor de un modelo GPAI debe garantizar la fiabilidad, seguridad y trazabilidad del modelo durante todo su ciclo de vida. Para ello, debe cumplir los siguientes principios:

- ✓ **Transparencia y documentación técnica:** El modelo debe estar acompañado de información clara sobre su funcionamiento, finalidad y limitaciones, así como sobre los métodos de entrenamiento, validación y prueba. Esta documentación debe permitir a terceros comprender las capacidades del modelo y los posibles riesgos asociados.

- ✓ **Gobernanza de datos y cumplimiento normativo:** Los datos utilizados deben obtenerse de forma legítima, respetando la legislación de la Unión en materia de derechos de autor y protección de datos personales. Deben implementarse políticas

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

internas para evitar el uso de contenido protegido sin autorización y asegurar que los procesos de minería de datos se ajustan al marco jurídico europeo.

- ✓ **Política de derechos de autor y transparencia:** Los proveedores deben contar con políticas específicas que garanticen el cumplimiento de la Directiva (UE) 2019/790 y las disposiciones sobre minería de texto y datos. Además, deben ofrecer información pública, accesible y comprensible sobre las fuentes de datos utilizadas y las medidas adoptadas para prevenir infracciones de derechos de autor.

- ✓ **Evaluación y mitigación de riesgos:** Debe disponerse de un proceso estructurado para identificar, analizar y mitigar los riesgos asociados con el modelo, en particular los relacionados con sesgos, falta de representatividad de datos, errores de interpretación o usos indebidos.

- ✓ **Seguridad y ciberresiliencia**: Los modelos GPAI deben incorporar medidas de protección frente a ataques adversariales, accesos no autorizados o manipulación de parámetros. Estas medidas deben actualizarse conforme a las mejores prácticas de ciberseguridad y a la evolución tecnológica.

- ✓ **Buenas prácticas y estándares internacionales:** Se recomienda la adopción de marcos de gestión responsable de IA, como la norma ISO/IEC 42001:2023, y la participación en códigos de conducta europeos que refuercen la confianza, la ética y la interoperabilidad.

- **Responsable del despliegue:**

  Las entidades que utilicen modelos GPAI en sus operaciones deben asegurarse de que su aplicación sea compatible con la finalidad prevista y no genere riesgos nuevos o no evaluados.

  - ✓ **Verificación de compatibilidad**: Antes de la integración del modelo, debe verificarse su adecuación técnica y su impacto en el entorno operativo. En el ámbito sanitario, ello implica una validación clínica previa; en Smart Cities, una evaluación de impacto sobre la seguridad y la privacidad urbana.

  - ✓ **Gestión de riesgos y trazabilidad:** El responsable debe documentar el proceso de integración, los resultados de pruebas internas y las acciones de mitigación adoptadas.

  - ✓ **Formación y competencias:** Debe garantizarse que el personal implicado en la supervisión del modelo dispone de la formación necesaria sobre sus capacidades, limitaciones y posibles sesgos.

  - ✓ **Transparencia hacia los usuarios:** Cuando el modelo interactúe con personas físicas o genere contenido automatizado, los usuarios deben ser informados de manera clara de la naturaleza artificial del sistema y de su intervención en los procesos decisionales.

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

7.1.6. Modelos de Inteligencia Artificial de Propósito General (GPAI) con riesgo sistémico

Los Modelos de Inteligencia Artificial de Propósito General (GPAI) con riesgo sistémico constituyen una categoría especial dentro del Reglamento (UE) 2024/1689, que se aplica a aquellos modelos cuya escala, potencia de cómputo o capacidad funcional puede generar impactos amplios y significativos sobre la seguridad, la salud pública, los derechos fundamentales o la estabilidad social y económica de la Unión Europea.

De acuerdo con el artículo 55 del RIA, se consideran modelos con riesgo sistémico aquellos que:

- Han requerido un volumen de cálculo superior a 10^{25} operaciones de coma flotante (FLOPs) durante su entrenamiento, indicador del total de operaciones computacionales realizadas y no de la velocidad de procesamiento por segundo (FLOPS), o
- Han sido designados formalmente por la Comisión Europea como modelos de alto impacto debido a su potencial de propagación de riesgos a través de la cadena de valor de la IA.

Esta categoría incluye tanto modelos cerrados (comerciales o de uso restringido) como modelos abiertos que, por su escala o capacidad técnica, puedan facilitar conductas ilícitas, desinformación masiva, pérdida de control operacional o riesgos de uso dual (p. ej., en ámbitos cibernéticos, químicos o biológicos). En los sectores de **Salud y Smart Cities**, los GPAI con riesgo sistémico pueden tener un efecto multiplicador: en sanidad, por su integración en sistemas clínicos o diagnósticos; y en entornos urbanos, por su potencial para alterar infraestructuras críticas o sistemas automatizados de decisión pública.

En el caso de los GPAI con riesgo sistémico, el Reglamento (UE) 2024/1689 centra las obligaciones específicas en los roles de **proveedor y responsable del despliegue.** Los demás operadores, como el importador, el distribuidor y el representante autorizado, mantienen sus obligaciones generales previstas en el RIA, sin que ello implique nuevas obligaciones por tratarse de GPAI con riesgo sistémico. Por otro lado, el fabricante solo adquiere responsabilidades directas cuando integra un modelo de inteligencia artificial en un producto físico que está regulado por otra normativa sectorial de la Unión (como el Reglamento (UE) 2017/745 sobre productos sanitarios o la Directiva 2006/42/CE sobre maquinaria). En tal caso, sus obligaciones se rigen principalmente por esa normativa específica, aunque también por el RIA en la medida en que el **fabricante actúe como proveedor** del sistema de IA integrado.

- **Proveedor:**

Los proveedores de GPAI con riesgo sistémico están sujetos a un régimen reforzado de seguridad, gobernanza, transparencia y supervisión, que busca prevenir los efectos adversos de los modelos a gran escala.

Estas obligaciones se materializan principalmente a través de la elaboración de un Marco de Seguridad y Protección (Safety and Security Framework, SSF), complementado por la documentación técnica, las evaluaciones periódicas, los mecanismos de vigilancia y la cooperación con las autoridades competentes y actores posteriores.

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

- ✓ **Desarrollo e implementación del Marco de Seguridad y Protección (SSF):** Debe elaborar un SSF documentado que describa los procedimientos de evaluación, mitigación y supervisión de riesgos sistémicos. Este marco debe contemplar los riesgos técnicos (por ejemplo, cibernéticos, químicos o biológicos), los de gobernanza (pérdida de control, manipulación, desinformación o discriminación masiva) y los éticos o sociales derivados de la escala del modelo.

- ✓ **Identificación y análisis de riesgos:** El proveedor debe identificar de forma continua los riesgos sistémicos asociados al modelo, evaluando su severidad, probabilidad y vías de propagación. Esto incluye análisis técnicos de capacidades peligrosas, sesgos estructurales, vulnerabilidades de seguridad y escenarios de impacto transversal en distintos sectores.

- ✓ **Mitigación técnica y organizativa:** Debe establecer controles proporcionales al nivel de riesgo, que incluyan salvaguardias de acceso, medidas de ciberseguridad avanzadas, pruebas adversariales periódicas y mecanismos de monitorización automática del comportamiento del modelo en entornos operativos.

- ✓ **Evaluaciones y auditorías independientes:** El proveedor debe someter su modelo a evaluaciones externas o auditorías de seguridad realizadas por expertos cualificados o instituciones reconocidas, garantizando la independencia del proceso y la validez científica de los resultados.

- ✓ **Gestión de incidentes y notificación:** Cualquier incidente grave que afecte a la salud, seguridad o derechos fundamentales de las personas debe ser documentado y comunicado sin dilación a las autoridades competentes, conforme al artículo 80 del RIA.

- ✓ **Gobernanza corporativa y responsabilidad ejecutiva**: La dirección y los órganos de gobierno de la entidad proveedora deben asignar responsabilidades explícitas sobre el riesgo sistémico, asegurando que existan recursos humanos, técnicos y financieros suficientes para su gestión.

- ✓ **Transparencia y publicación de resultados:** El proveedor debe garantizar una transparencia adecuada sobre las capacidades, limitaciones y medidas de seguridad aplicadas al modelo, publicando información resumida sobre las evaluaciones, el consumo energético, las fuentes de datos y las medidas de mitigación adoptadas, de forma que pueda ser comprendida por el público sin comprometer la seguridad o la confidencialidad industrial.

- ✓ **Cumplimiento con el Derecho de la Unión:** Debe asegurar la observancia del Derecho de la Unión en materia de protección de datos, derechos de autor y ciberseguridad, evitando el uso de material protegido o contenido pirateado en la fase de entrenamiento y validación del modelo.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PUBLICA SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

- ✓ **Código de buenas prácticas:** Se recomienda adherirse voluntariamente al Código de Buenas Prácticas para modelos de inteligencia artificial de uso general, adoptado por la Comisión Europea conforme al artículo 56 del Reglamento (UE) 2024/1689, así como a sus actualizaciones o desarrollos complementarios que puedan adoptarse en el marco europeo. Dicho código establece pautas armonizadas para la gestión responsable, la supervisión posterior al despliegue y la mitigación de riesgos transfronterizos asociados.

- **Responsable del despliegue:**

Las entidades que utilicen modelos GPAI con riesgo sistémico en sus operaciones, ya sea en el ámbito sanitario, urbano o industrial, deben garantizar que su uso se desarrolla bajo condiciones de seguridad, trazabilidad y control humano efectivo. Las principales obligaciones del responsable del despliegue son:

- ✓ **Verificación de conformidad y seguridad:** Antes de la integración del modelo, el responsable debe verificar que el proveedor ha implementado un SSF adecuado y que el modelo cumple las condiciones de seguridad y gobernanza establecidas en el RIA.

- ✓ **Supervisión operativa y control humano:** Durante su uso, debe garantizarse una supervisión continua, con mecanismos técnicos y organizativos que permitan detectar comportamientos anómalos, suspender procesos automatizados y revertir decisiones potencialmente dañinas.

- ✓ **Evaluación de impacto y documentación:** En el caso de aplicaciones que puedan afectar a la salud, la seguridad o los derechos fundamentales, el responsable debe realizar una evaluación de impacto previa que documente los riesgos asociados, las medidas de mitigación adoptadas y las condiciones de uso.

- ✓ **Cooperación con el proveedor y autoridades:** El responsable debe establecer canales de comunicación y cooperación con el proveedor, notificando cualquier incidente relevante o desviación del comportamiento esperado del modelo.

- ✓ **Formación y capacitación del personal:** Las personas encargadas del manejo o supervisión del modelo deben recibir formación especializada sobre su funcionamiento, límites técnicos y medidas de seguridad, garantizando una comprensión adecuada de los riesgos sistémicos.

- ✓ **Trazabilidad y registro:** El responsable debe mantener registros automáticos del funcionamiento del modelo, incluyendo logs de interacción, cambios de configuración y revisiones periódicas, asegurando la trazabilidad y la posibilidad de auditoría posterior.

- **Importador y distribuidor:**

Estos actores, cuando participen en la introducción o comercialización de modelos GPAI con riesgo sistémico en el mercado europeo, deben:

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PUBLICA SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

- ✓ Verificar que el modelo cuenta con documentación técnica completa, información sobre el SSF y evidencia de cumplimiento de los requisitos del RIA.
- ✓ Garantizar la integridad del modelo durante el almacenamiento y transporte, evitando cualquier modificación que altere su comportamiento o aumente su riesgo.
- ✓ Abstenerse de comercializar el modelo si se detectan deficiencias graves o incumplimientos, informando de inmediato a las autoridades competentes.
- ✓ Colaborar con las autoridades y el proveedor en la trazabilidad y vigilancia poscomercialización.

- **Representante autorizado:**

Cuando el proveedor esté establecido fuera de la Unión Europea, debe designarse un representante autorizado en el territorio de la Unión, quien asumirá funciones de enlace y custodia documental. Sus responsabilidades incluyen:

- ✓ **Conservación de documentación técnica y SSF**: Custodiar la documentación técnica, el Marco de Seguridad y Protección y la declaración de conformidad durante un periodo mínimo de diez años.

- ✓ **Cooperación institucional**: Actuar como punto de contacto con las autoridades competentes y la Oficina Europea de Inteligencia Artificial para facilitar la supervisión y el acceso a información técnica.

- ✓ **Verificación de cumplimiento:** Comprobar que el proveedor cumple con las obligaciones del RIA y comunicar a las autoridades cualquier incumplimiento grave detectado.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

8. Documentación, trazabilidad y supervisión del cumplimiento

El Reglamento (UE) 2024/1689 establece que los operadores de sistemas de inteligencia artificial deberán mantener una documentación técnica completa, garantizar la trazabilidad de las operaciones y aplicar mecanismos de seguimiento posterior al mercado que permitan demostrar la conformidad continua del sistema con los requisitos legales y técnicos establecidos.

Las obligaciones descritas en este apartado se aplican **exclusivamente a los sistemas de inteligencia artificial clasificados como de alto riesgo**, conforme a los artículos 8 a 72 del Reglamento (UE) 2024/1689 sobre Inteligencia Artificial (RIA). Los sistemas de riesgo limitado solo deben cumplir con las exigencias de transparencia del artículo 52 y los de riesgo mínimo pueden aplicar buenas prácticas voluntarias. Los sistemas de riesgo prohibido, definidos en el artículo 5, no pueden desarrollarse, comercializarse ni utilizarse.

8.1. Documentación técnica

Según los artículos 16 y 17 del RIA, el proveedor de un sistema de IA de alto riesgo debe elaborar y conservar una documentación técnica que demuestre el cumplimiento de los requisitos esenciales del Reglamento (arts. 8 a 15), incluidos los relativos a:

- Gestión del riesgo
- Gobernanza de datos
- Transparencia
- Supervisión humana
- Robustez y ciberseguridad

Esta documentación constituye la base de la evaluación de conformidad previa al marcado CE y deberá estar disponible para las autoridades competentes.

Debe incluir, como mínimo:

- Descripción del sistema, finalidad prevista, arquitectura y versiones.
- Información sobre los algoritmos, modelos y procesos de entrenamiento.
- Datos utilizados en entrenamiento, validación y prueba, con su origen y calidad.
- Resultados del sistema de gestión de riesgos y medidas de mitigación adoptadas.
- Descripción del sistema de gestión de calidad (artículo 17 RIA).
- Evidencias del cumplimiento de los requisitos de los artículos 8 a 15 (RIA).
- Instrucciones de uso, mantenimiento y supervisión humana.

El proveedor conservará esta documentación durante diez años desde la puesta en el mercado o en servicio (artículo 71).

Si el proveedor está establecido fuera de la Unión, su **representante autorizado** asumirá la obligación de conservación y de facilitarla a las autoridades competentes cuando se requiera.

Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia
Junta de Andalucía
Agencia Digital de Andalucía

8.2. Registros y trazabilidad

Los sistemas de IA de alto riesgo deben estar diseñados de modo que registren automáticamente los eventos relevantes que se produzcan durante su funcionamiento.

Estos registros o logs permiten:

- Reconstruir la secuencia de decisiones y operaciones del sistema;
- Detectar errores o anomalías;
- Verificar el cumplimiento normativo;
- Y facilitar la supervisión humana.

El **proveedor** garantizará que el sistema disponga de la capacidad técnica necesaria para generar y conservar los registros de forma íntegra y accesible.

El **responsable del despliegue** conservará los registros generados durante la operación del sistema durante el tiempo necesario para cumplir con el Reglamento o con la normativa sectorial aplicable.

Los registros deben protegerse frente a accesos no autorizados o manipulaciones y estar disponibles para las autoridades competentes cuando se soliciten.

8.3. Sistema de gestión de calidad

El artículo 17 del RIA establece la obligación **del proveedor** de un sistema de alto riesgo de establecer, aplicar y mantener un sistema de gestión de calidad que garantice el cumplimiento del Reglamento.

Este sistema debe incluir procedimientos que abarquen:

- Control del diseño, desarrollo, verificación y validación;
- Gestión y actualización de la documentación técnica;
- Vigilancia posterior al mercado y aplicación de medidas correctoras;
- Comunicación con las autoridades competentes;
- Gestión de incidencias o no conformidades.

El sistema de gestión de calidad debe permitir demostrar la trazabilidad de todas las fases del ciclo de vida del sistema y la existencia de controles internos adecuados.

8.4. Notificación de incidentes graves

Según el articulo 80 del RIA, cuando un sistema de IA de alto riesgo cause o pueda causar un incidente grave que afecte a la salud, la seguridad o los derechos fundamentales, el proveedor deberá notificarlo a la autoridad competente en un plazo máximo de **15 días** desde que tenga conocimiento del hecho, o en **2 días** si existe riesgo inminente.

El **responsable del despliegue** informará de inmediato al proveedor cuando detecte un incidente de esta naturaleza.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PUBLICA SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

La notificación deberá incluir:

- La descripción del incidente
- Su causa probable
- Las medidas adoptadas
- Y, en su caso, las acciones preventivas implementadas

Las autoridades pueden solicitar información adicional o llevar a cabo inspecciones y auditorías.

8.5. Actualización y modificaciones sustanciales

Cualquier modificación sustancial del sistema obliga a actualizar la documentación técnica y, cuando corresponda, a realizar una nueva evaluación de conformidad.

El proveedor mantendrá la documentación, registros y resultados de vigilancia siempre actualizados y a disposición de las autoridades competentes.

Se considera **modificación sustancial** cualquier cambio que pueda alterar la seguridad, la precisión o la finalidad prevista del sistema, entre ellos:

- La modificación del modelo de inteligencia artificial, sus parámetros o su arquitectura;
- La sustitución o ampliación de los conjuntos de datos utilizados para el entrenamiento o la validación;
- La incorporación de nuevas funcionalidades o modos de uso no previstos originalmente;
- La integración del sistema en un producto o servicio distinto del declarado en la evaluación inicial;
- La modificación de las condiciones de despliegue o de los contextos operativos que puedan afectar al rendimiento o a los derechos de las personas.

Ante una modificación sustancial**, el proveedor** deberá:

- Revisar la evaluación de conformidad para determinar si el sistema sigue cumpliendo los requisitos del reglamento o si requiere una nueva evaluación formal;
- Actualizar la documentación técnica con una descripción detallada de los cambios realizados, su justificación técnica y el análisis de impacto correspondiente;
- Ajustar la gestión de riesgos, documentando los nuevos riesgos identificados, su probabilidad, severidad y las medidas de mitigación aplicadas;
- Actualizar las instrucciones de uso y mantenimiento, asegurando que el responsable del despliegue y los usuarios conozcan las nuevas condiciones de operación o limitaciones;
- Notificar, cuando proceda, las modificaciones a las autoridades competentes o al organismo notificado que participó en la evaluación inicial.

El **responsable del despliegue**, por su parte, deberá:

- Verificar si los cambios introducidos afectan a la finalidad o condiciones de uso del sistema en su entorno operativo;
- Ajustar sus protocolos de supervisión, mantenimiento y formación del personal en función de las actualizaciones;

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

- Y mantener la trazabilidad de todas las versiones utilizadas, incluyendo fechas, número de versión, proveedor y configuración aplicada.

Toda actualización deberá registrarse en los expedientes técnicos internos, manteniendo la trazabilidad entre versiones y la correspondencia con los informes de vigilancia posterior al mercado.

La documentación revisada deberá conservarse durante el mismo periodo mínimo de diez años desde la última puesta en el mercado o en servicio del sistema actualizado.

8.6. Plantillas y formularios oficiales de la comisión europea

La Comisión Europea y la Oficina Europea de Inteligencia Artificial han publicado y anunciado varios instrumentos de apoyo para la aplicación práctica del Reglamento, que deberán ser utilizados por los operadores cuando se encuentren disponibles.

Actualmente, el estado es el siguiente:

- **Plantilla de transparencia para modelos de propósito general,** publicada el 24 de julio de 2025, que define cómo resumir los datos de entrenamiento y la información sobre derechos de autor.
- **Guía y plantilla para la notificación de incidentes graves**, actualmente en borrador y en fase de consulta pública desde el tercer trimestre de 2025.
- **Plantilla del plan de vigilancia posterior al mercado**, pendiente de adopción; la Comisión debe aprobarla mediante acto de ejecución antes del 2 de febrero de 2026.
- **Formulario y base de datos de registro de sistemas de alto riesgo**, **en desarrollo** por la Comisión, obligatorios antes de la puesta en el mercado o en servicio; con campos públicos y otros reservados por motivos de seguridad o aplicación de la ley.

Los operadores deberán adaptar sus procedimientos internos y utilizar estas plantillas y formularios en cuanto sean adoptados oficialmente por la Comisión Europea.

9. Referencias

1. Unión Europea. (2024). 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 (Ley de Inteligencia Artificial).
https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=OJ:L_202401689

2. Unión Europea. (2017). Reglamento (UE) 2017/745 del Parlamento Europeo y del Consejo, de 5 de abril de 2017, sobre los productos sanitarios (MDR).
https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32017R0745

3. Unión Europea. (2017). Reglamento (UE) 2017/746 del Parlamento Europeo y del Consejo, de 5 de abril de 2017, sobre los productos sanitarios para diagnóstico in vitro (IVDR).
https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32017R0746

4. Unión Europea. (2016). Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de dichos datos (Reglamento General de Protección de Datos – RGPD).
https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016R0679

5. Comisión Europea. (2024). Oficina Europea de Inteligencia Artificial (AI Office) – Estructura de gobernanza y funciones.
https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=OJ:C_202401459

6. Unión Europea. (2023). Reglamento (UE) 2023/2854 del Parlamento Europeo y del Consejo, de 13 de diciembre de 2023, relativo a los requisitos de ciberresiliencia aplicables a los productos con elementos digitales (Ley de Ciberresiliencia – CRA).
https://www.boe.es/doue/2024/2847/L00001-00081.pdf

7. Unión Europea. (2006). Directiva 2006/42/CE del Parlamento Europeo y del Consejo, de 17 de mayo de 2006, relativa a las máquinas y por la que se modifica la Directiva 95/16/CE (Directiva de Maquinaria).
https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32006L0042

8. Unión Europea. (2012). Directiva 2012/19/UE del Parlamento Europeo y del Consejo, de 4 de julio de 2012, sobre residuos de aparatos eléctricos y electrónicos (Directiva RAEE).
https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32012L0019

9. Organización Internacional de Normalización. (2023). Norma ISO/IEC 42001:2023, Tecnologías de la información – Inteligencia artificial – Sistema de gestión.
https://www.iso.org/standard/81230.html

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

10. Organización Internacional de Normalización. (2023). Norma ISO/IEC 23894:2023, Inteligencia artificial – Directrices para la gestión del riesgo. https://www.iso.org/standard/77608.html

11. Instituto Nacional de Estándares y Tecnología (NIST). (2023). Marco de gestión de riesgos de inteligencia artificial (AI Risk Management Framework 1.0). https://www.nist.gov/itl/ai-risk-management-framework

12. Comisión Europea. (2025). Plantilla de transparencia para modelos de IA de propósito general (publicada el 24 de julio de 2025). https://digital-strategy.ec.europa.eu/es/library/explanatory-notice-and-template-public-summary-training-content-general-purpose-ai-models

13. Comisión Europea. (2025). Guía y plantilla para la notificación de incidentes graves en sistemas de IA de alto riesgo (borrador en consulta pública desde el T3 2025). https://digital-strategy.ec.europa.eu/es/consultations/ai-act-commission-issues-draft-guidance-and-reporting-template-serious-ai-incidents-and-seeks

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

10. Otras referencias de interés

El presente apartado recoge un resumen de los principales temas abordados en la guía, así como la relación de productos y servicios mencionados en ella. Su finalidad es ofrecer una visión global de los ámbitos tratados y facilitar la identificación de posibles referencias o elementos relevantes para futuras consultas o ampliaciones documentales.

10.1. Lista de materias tratadas en la guía

- Aplicación y cumplimiento del Reglamento (UE) 2024/1689 sobre inteligencia artificial.
- Integración de la inteligencia artificial en entornos de salud y Smart Cities.
- Clasificación de los sistemas de inteligencia artificial según niveles de riesgo, de acuerdo con la *Guía de clasificación de sistemas de IA en base al RIA en entornos de Salud y Smart Cities* (2025).
- Evaluación de conformidad y marcado CE.
- Transparencia, supervisión humana y gobernanza responsable.
- Documentación técnica, trazabilidad y vigilancia posterior al mercado.
- Gestión de riesgos, ciberresiliencia y seguridad digital en sistemas de inteligencia artificial.
- Protección de datos personales y derechos fundamentales.
- Integración sectorial con el MDR, el IVDR, el CRA y la Directiva de Maquinaria.
- Aplicación de normas y estándares internacionales (ISO, IEC, NIST).
- Interoperabilidad y coordinación institucional entre autoridades competentes.
- Mejora continua, auditoría y supervisión de los sistemas de inteligencia artificial.

10.2. Lista de productos mencionados en la guía

No se mencionan productos específicos en la guía.

10.3. Lista de servicios mencionados en la guía

No se mencionan servicios específicos en la guía.

Roles y obligaciones regulatorias del RIA para sistemas de IA en entornos de Salud y Smart Cities

Octubre de 2025

Versión 1.0

Junta de Andalucía

Financiado por la Unión Europea NextGenerationEU