GRUPO solitium

EUROPA · INTELIGENCIA ARTIFICIAL · EMPRESA

REGLAMENTO EUROPEO DE INTELIGENCIA ARTIFICIAL

TEXTO LEGAL ÍNTEGRO + ANÁLISIS PRÁCTICO

Un marco de referencia para las empresas que innovan.



IA · LEGISLACIÓN · ERP

GUÍA DE CONSULTA

REGLAMENTO (UE) 2024/1689

13 CAPÍTULOS / 14 ANEXOS / TEXTO CONSOLIDADO A 27.07.2026

SOLITIUM

Guía de lectura

Este documento reúne los resúmenes elaborados durante el estudio del Reglamento (UE) 2024/1689. Conserva los textos, ejemplos, tablas y conclusiones de las respuestas trabajadas, adaptando a Word la presentación de tarjetas, esquemas y otros elementos visuales de la conversación. El índice jurídico reproduce la numeración y las páginas del PDF de referencia.

Documento de trabajo. Esta recopilación es un material explicativo, no sustituye el texto normativo ni una evaluación jurídica individualizada de un sistema de IA.

Índice del Reglamento Europeo de Inteligencia Artificial (AI Act)

Reglamento (UE) 2024/1689, de 13 de junio de 2024.

Texto consolidado a 27 de julio de 2026, con las modificaciones del Reglamento (UE) 2026/1744. Documento de 151 páginas. La numeración corresponde a las páginas del PDF adjunto.

Capítulo I. Disposiciones generales

Páginas 2–12

- Artículo 1. Objeto — p. 2
- Artículo 2. Ámbito de aplicación — p. 2
- Artículo 3. Definiciones — p. 5
- Artículo 4. Alfabetización en materia de IA — p. 11
- Artículo 4 bis. Tratamiento de categorías especiales de datos personales para la detección y corrección de sesgos — p. 12

Capítulo II. Prácticas de IA prohibidas

Páginas 13–17

- Artículo 5. Prácticas de IA prohibidas — p. 13

Capítulo III. Sistemas de IA de alto riesgo

Páginas 17–58

Sección 1. Clasificación de los sistemas de IA como sistemas de alto riesgo

- Artículo 6. Reglas de clasificación de los sistemas de IA de alto riesgo — p. 17
- Artículo 7. Modificaciones del anexo III — p. 19

Sección 2. Requisitos de los sistemas de IA de alto riesgo

- Artículo 8. Cumplimiento de los requisitos — p. 20
- Artículo 9. Sistema de gestión de riesgos — p. 21
- Artículo 10. Datos y gobernanza de datos — p. 22
- Artículo 11. Documentación técnica — p. 24
- Artículo 12. Conservación de registros — p. 24
- Artículo 13. Transparencia y comunicación de información a los responsables del despliegue — p. 25

- Artículo 14. Supervisión humana — p. 26
- Artículo 15. Precisión, solidez y ciberseguridad — p. 27

Sección 3. Obligaciones de los proveedores y responsables del despliegue de sistemas de IA de alto riesgo y de otras partes

- Artículo 16. Obligaciones de los proveedores — p. 28
- Artículo 17. Sistema de gestión de la calidad — p. 29
- Artículo 18. Conservación de la documentación — p. 30
- Artículo 19. Archivos de registro generados automáticamente — p. 31
- Artículo 20. Medidas correctoras y obligación de información — p. 31
- Artículo 21. Cooperación con las autoridades competentes — p. 32
- Artículo 22. Representantes autorizados de los proveedores — p. 32
- Artículo 23. Obligaciones de los importadores — p. 33
- Artículo 24. Obligaciones de los distribuidores — p. 34
- Artículo 25. Responsabilidades a lo largo de la cadena de valor de la IA — p. 35
- Artículo 26. Obligaciones de los responsables del despliegue — p. 37
- Artículo 27. Evaluación de impacto relativa a los derechos fundamentales — p. 39

Sección 4. Autoridades notificantes y organismos notificados

- Artículo 28. Autoridades notificantes — p. 40
- Artículo 29. Solicitud de notificación de organismos de evaluación — p. 42
- Artículo 30. Procedimiento de notificación — p. 42
- Artículo 31. Requisitos relativos a los organismos notificados — p. 43
- Artículo 32. Presunción de conformidad — p. 45
- Artículo 33. Filiales y subcontratación — p. 45
- Artículo 34. Obligaciones operativas — p. 45
- Artículo 35. Números de identificación y listas — p. 46
- Artículo 36. Cambios en las notificaciones — p. 46
- Artículo 37. Cuestionamiento de la competencia — p. 48
- Artículo 38. Coordinación de los organismos notificados — p. 49
- Artículo 39. Organismos de evaluación de terceros países — p. 49

Sección 5. Normas, evaluación de la conformidad, certificados y registro

- Artículo 40. Normas armonizadas y documentos de normalización — p. 49
- Artículo 41. Especificaciones comunes — p. 50
- Artículo 42. Presunción de conformidad — p. 52
- Artículo 43. Evaluación de la conformidad — p. 52
- Artículo 44. Certificados — p. 54
- Artículo 45. Obligaciones de información de organismos notificados — p. 55
- Artículo 46. Exención del procedimiento de evaluación — p. 56
- Artículo 47. Declaración UE de conformidad — p. 57
- Artículo 48. Marcado CE — p. 57
- Artículo 49. Registro — p. 58

Capítulo IV. Obligaciones de transparencia

Páginas 59–60

- Artículo 50. Obligaciones de transparencia de los proveedores y responsables del despliegue de determinados sistemas de IA — p. 59

Capítulo V. Modelos de IA de uso general

Páginas 60–66

Sección 1. Reglas de clasificación

- Artículo 51. Clasificación de los modelos de IA de uso general con riesgo sistémico — p. 60
- Artículo 52. Procedimiento — p. 61

Sección 2. Obligaciones de los proveedores de modelos de IA de uso general

- Artículo 53. Obligaciones de los proveedores — p. 62
- Artículo 54. Representantes autorizados — p. 63

Sección 3. Obligaciones de los proveedores de modelos con riesgo sistémico

- Artículo 55. Obligaciones de los proveedores de modelos de IA de uso general con riesgo sistémico — p. 64

Sección 4. Códigos de buenas prácticas

- Artículo 56. Códigos de buenas prácticas — p. 65

Capítulo VI. Medidas de apoyo a la innovación

Páginas 67–79

- Artículo 57. Espacios controlados de pruebas para la IA — p. 67
- Artículo 58. Disposiciones detalladas sobre los espacios controlados — p. 70
- Artículo 59. Tratamiento ulterior de datos personales para desarrollar determinados sistemas de IA de interés público — p. 72
- Artículo 60. Pruebas de sistemas de IA de alto riesgo en condiciones reales — p. 74
- Artículo 60 bis. Pruebas en condiciones reales de sistemas de alto riesgo regulados por legislación sectorial del anexo I, sección B — p. 76
- Artículo 61. Consentimiento informado para participar en pruebas — p. 77
- Artículo 62. Medidas dirigidas a proveedores y responsables del despliegue, especialmente pymes y empresas emergentes — p. 78
- Artículo 63. Excepciones para operadores específicos — p. 79

Capítulo VII. Gobernanza

Páginas 79–86

Sección 1. Gobernanza a escala de la Unión

- Artículo 64. Oficina de IA — p. 79
- Artículo 65. Creación y estructura del Consejo Europeo de Inteligencia Artificial — p. 80
- Artículo 66. Funciones del Consejo de IA — p. 81
- Artículo 67. Foro consultivo — p. 83
- Artículo 68. Grupo de expertos científicos independientes — p. 83
- Artículo 69. Acceso a expertos por parte de los Estados miembros — p. 85

Sección 2. Autoridades nacionales competentes

- Artículo 70. Designación de las autoridades nacionales competentes y de los puntos de contacto único — p. 85

Capítulo VIII. Base de datos de la UE para sistemas de IA de alto riesgo

Páginas 86–87

- Artículo 71. Base de datos de la UE para los sistemas de IA de alto riesgo enumerados en el anexo III — p. 86

Capítulo IX. Vigilancia poscomercialización, intercambio de información y vigilancia del mercado

Páginas 87–112

Sección 1. Vigilancia poscomercialización

- Artículo 72. Vigilancia poscomercialización por parte de los proveedores y plan de vigilancia — p. 87

Sección 2. Intercambio de información sobre incidentes graves

- Artículo 73. Notificación de incidentes graves — p. 88

Sección 3. Garantía del cumplimiento

- Artículo 74. Vigilancia del mercado y control de los sistemas de IA — p. 90
- Artículo 75. Vigilancia del mercado y control de los sistemas de IA y asistencia mutua — p. 92
- Artículo 75 bis. Competencias de supervisión y de garantía del cumplimiento de la Oficina de IA — p. 95
- Artículo 75 ter. Compromisos — p. 97
- Artículo 75 quater. Incumplimiento, multas sancionadoras y multas coercitivas — p. 98
- Artículo 75 quinquies. Salvaguardias y especificaciones adicionales — p. 99
- Artículo 76. Supervisión de las pruebas en condiciones reales — p. 100
- Artículo 77. Poderes de las autoridades encargadas de proteger los derechos fundamentales y cooperación con las autoridades de vigilancia del mercado — p. 101
- Artículo 78. Confidencialidad — p. 102
- Artículo 79. Procedimiento nacional para sistemas que presentan riesgos — p. 103
- Artículo 80. Procedimiento para sistemas clasificados como no de alto riesgo — p. 105
- Artículo 81. Procedimiento de salvaguardia de la Unión — p. 106
- Artículo 82. Sistemas de IA conformes que presentan riesgos — p. 107
- Artículo 83. Incumplimiento formal — p. 107
- Artículo 84. Estructuras de apoyo a los ensayos de IA de la Unión — p. 108

Sección 4. Vías de recurso

- Artículo 85. Derecho a presentar reclamaciones — p. 108
- Artículo 86. Derecho a explicación de decisiones tomadas individualmente — p. 108
- Artículo 87. Denuncia de infracciones y protección de denunciantes — p. 109

Sección 5. Supervisión, investigación, cumplimiento y seguimiento de proveedores de modelos de IA de uso general

- Artículo 88. Cumplimiento de las obligaciones de los proveedores — p. 109
- Artículo 89. Medidas de seguimiento — p. 109
- Artículo 90. Alertas del grupo de expertos científicos sobre riesgos sistémicos — p. 110
- Artículo 91. Poderes para solicitar documentación e información — p. 110
- Artículo 92. Poderes para realizar evaluaciones — p. 111
- Artículo 93. Poderes para solicitar la adopción de medidas — p. 112
- Artículo 94. Garantías procesales de los operadores económicos — p. 112

Capítulo X. Códigos de conducta y directrices

Páginas 112–114

- Artículo 95. Códigos de conducta para la aplicación voluntaria de requisitos específicos — p. 112
- Artículo 96. Directrices de la Comisión sobre la aplicación del Reglamento — p. 113

Capítulo XI. Delegación de poderes y procedimiento de comité

Páginas 114–115

- Artículo 97. Ejercicio de la delegación — p. 114
- Artículo 98. Procedimiento de comité — p. 115

Capítulo XII. Sanciones

Páginas 115–120

- Artículo 99. Sanciones — p. 115
- Artículo 100. Multas administrativas a instituciones, órganos y organismos de la Unión — p. 118
- Artículo 101. Multas a proveedores de modelos de IA de uso general — p. 119

Capítulo XIII. Disposiciones finales

Páginas 120–127

- Artículo 102. Modificación del Reglamento (CE) 300/2008 — p. 120
- Artículo 103. Modificación del Reglamento (UE) 167/2013 — p. 120
- Artículo 104. Modificación del Reglamento (UE) 168/2013 — p. 121
- Artículo 105. Modificación de la Directiva 2014/90/UE — p. 121
- Artículo 106. Modificación de la Directiva (UE) 2016/797 — p. 122
- Artículo 107. Modificación del Reglamento (UE) 2018/858 — p. 122
- Artículo 108. Modificación del Reglamento (UE) 2018/1139 — p. 122
- Artículo 109. Modificación del Reglamento (UE) 2019/2144 — p. 123
- Artículo 110. Modificación de la Directiva (UE) 2020/1828 — p. 124
- Artículo 111. Sistemas de IA y modelos de uso general ya introducidos en el mercado o puestos en servicio — p. 124
- Artículo 112. Evaluación y revisión — p. 125
- Artículo 113. Entrada en vigor y aplicación — p. 127

Anexos

Anexo	Contenido	Página
I	Lista de actos legislativos de armonización de la Unión	128
II	Lista de delitos contemplados en el artículo 5	130
III	Sistemas de IA de alto riesgo	131
IV	Documentación técnica de los sistemas de IA	134
V	Declaración UE de conformidad	136
VI	Procedimiento de evaluación de conformidad mediante control interno	137
VII	Evaluación del sistema de gestión de calidad y documentación técnica	138
VIII	Información para el registro de sistemas de alto riesgo	141

Anexo	Contenido	Página
IX	Información registral de las pruebas en condiciones reales	143
X	Legislación sobre sistemas informáticos de gran magnitud en el espacio de libertad, seguridad y justicia	144
XI	Documentación técnica de los modelos de IA de uso general	146
XII	Información de transparencia para proveedores posteriores que integran modelos de IA	148
XIII	Criterios de clasificación de modelos de IA de uso general con riesgo sistémico	149
XIV	Códigos y categorías de sistemas de IA para la designación de organismos notificados	150

Índice elaborado sobre el texto consolidado que has facilitado. Los títulos extensos se han abreviado en algunos casos para facilitar la consulta, manteniendo la numeración y las páginas de referencia originales.

TEXTO OFICIAL · CAPÍTULO I

CAPÍTULO I
DISPOSICIONES GENERALES

ARTÍCULO 1
OBJETO

1. El objetivo del presente Reglamento es mejorar el funcionamiento del mercado interior y promover la adopción de una inteligencia artificial (IA) centrada en el ser humano y fiable, garantizando al mismo tiempo un elevado nivel de protección de la salud, la seguridad y los derechos fundamentales consagrados en la Carta, incluidos la democracia, el Estado de Derecho y la protección del medio ambiente, frente a los efectos perjudiciales de los sistemas de IA (en lo sucesivo, «sistemas de IA») en la Unión así como prestar apoyo a la innovación.
2. El presente Reglamento establece:
   a) normas armonizadas para la introducción en el mercado, la puesta en servicio y la utilización de sistemas de IA en la Unión;
   b) prohibiciones de determinadas prácticas de IA;
   c) requisitos específicos para los sistemas de IA de alto riesgo y obligaciones para los operadores de dichos sistemas;
   d) normas armonizadas de transparencia aplicables a determinados sistemas de IA;
   e) normas armonizadas para la introducción en el mercado de modelos de IA de uso general;
   f) normas sobre el seguimiento del mercado, la vigilancia del mercado, la gobernanza y la garantía del cumplimiento;
   g) medidas en apoyo de la innovación, prestando especial atención a las pequeñas empresas de mediana capitalización y a las pequeñas y medianas empresas (pymes), incluidas las empresas emergentes.

ARTÍCULO 2
ÁMBITO DE APLICACIÓN

1. El presente Reglamento se aplicará a:
   a) los proveedores que introduzcan en el mercado o pongan en servicio sistemas de IA o que introduzcan en el mercado modelos de IA de uso general en la Unión, con independencia de si dichos proveedores están establecidos o ubicados en la Unión o en un tercer país;
   b) los responsables del despliegue de sistemas de IA que estén establecidos o ubicados en la Unión;
   c) los proveedores y responsables del despliegue de sistemas de IA que estén establecidos o ubicados en un tercer país, cuando los resultados de salida generados por el sistema de IA se utilicen en la Unión;
   d) los importadores y distribuidores de sistemas de IA;
   e) los fabricantes de productos que introduzcan en el mercado o pongan en servicio un sistema de IA junto con su producto y con su propio nombre o marca;
   f) los representantes autorizados de los proveedores que no estén establecidos en la Unión;
   g) las personas afectadas que estén ubicadas en la Unión.
2. A los sistemas de IA clasificados como sistemas de IA de alto riesgo de conformidad con el artículo 6, apartado 1, y relativos a productos regulados por los actos legislativos de armonización de la Unión enumerados en el anexo I, sección B, únicamente se les aplicarán el artículo 6, apartado 1, el artículo 60 bis y los artículos 102 a 112. Los artículos 57, 58 y 59 se aplicarán únicamente en la medida en que los requisitos para los sistemas de IA de alto riesgo en virtud del presente Reglamento se hayan integrado en dichos actos legislativos de armonización de la Unión.
3. El presente Reglamento no se aplicará a los ámbitos que queden fuera del ámbito de aplicación del Derecho de la Unión y, en cualquier caso, no afectará a las competencias de los Estados miembros en materia de seguridad nacional, independientemente del tipo de entidad a la que los Estados miembros hayan encomendado el desempeño de tareas en relación con dichas competencias.

El presente Reglamento no se aplicará a los sistemas de IA que, y en la medida en que, se introduzcan en el mercado, se pongan en servicio o se utilicen, con o sin modificaciones, exclusivamente con fines militares, de defensa o de seguridad nacional, independientemente del tipo de entidad que lleve a cabo estas actividades.

El presente Reglamento no se aplicará a los sistemas de IA que no se introduzcan en el mercado o no se pongan en servicio en la Unión en los casos en que sus resultados de salida se utilicen en la Unión exclusivamente con fines militares, de defensa o de seguridad nacional, independientemente del tipo de entidad que lleve a cabo estas actividades.

4. El presente Reglamento no se aplicará a las autoridades públicas de terceros países ni a las organizaciones internacionales que entren dentro del ámbito de aplicación de este Reglamento conforme al apartado 1 cuando dichas autoridades u organizaciones utilicen sistemas de IA en el marco de acuerdos o de la cooperación internacionales con fines de garantía del cumplimiento del Derecho y cooperación judicial con la Unión o con uno o varios Estados miembros, siempre que tal tercer país u organización internacional ofrezca garantías suficientes con respecto a la protección de los derechos y libertades fundamentales de las personas.
5. El presente Reglamento no afectará a la aplicación de las disposiciones relativas a la responsabilidad de los prestadores de servicios intermediarios que figuran en el capítulo II del Reglamento (UE) 2022/2065.
6. El presente Reglamento no se aplicará a los sistemas o modelos de IA, incluidos sus resultados de salida, desarrollados y puestos en servicio específicamente con la investigación y el desarrollo científicos como única finalidad.
7. El Derecho de la Unión en materia de protección de los datos personales, la intimidad y la confidencialidad de las comunicaciones se aplicará a los datos personales tratados en relación con los derechos y obligaciones establecidos en el presente Reglamento. Sin perjuicio de sus artículos 4 bis y 59, el presente Reglamento no afectará a los Reglamentos (UE) 2016/679 o (UE) 2018/1725 ni a las Directivas 2002/58/CE o (UE) 2016/680.
8. El presente Reglamento no se aplicará a ninguna actividad de investigación, prueba o desarrollo relativa a sistemas de IA o modelos de IA antes de su introducción en el mercado o puesta en servicio. Estas actividades se llevarán a cabo de conformidad con el Derecho de la Unión aplicable. Las pruebas en condiciones reales no estarán cubiertas por esa exclusión.

9. El presente Reglamento se entenderá sin perjuicio de las normas establecidas por otros actos jurídicos de la Unión relativos a la protección de los consumidores y a la seguridad de los productos.
10. El presente Reglamento no se aplicará a las obligaciones de los responsables del despliegue que sean personas físicas que utilicen sistemas de IA en el ejercicio de una actividad puramente personal de carácter no profesional.
11. El presente Reglamento no impedirá que la Unión o los Estados miembros mantengan o introduzcan disposiciones legales, reglamentarias o administrativas que sean más favorables a los trabajadores en lo que atañe a la protección de sus derechos respecto al uso de sistemas de IA por parte de los empleadores ni que fomenten o permitan la aplicación de convenios colectivos que sean más favorables a los trabajadores.
12. El presente Reglamento no se aplicará a los sistemas de IA divulgados con arreglo a licencias libres y de código abierto, a menos que se introduzcan en el mercado o se pongan en servicio como sistemas de IA de alto riesgo o como sistemas de IA que entren en el ámbito de aplicación del artículo 5 o del artículo 50.
13. En el caso de los sistemas de IA de alto riesgo a que se refiere el artículo 6, apartado 1, la aplicación de los requisitos u obligaciones específicos establecidos en los artículos 9 a 15 y 17 a 25 podrá limitarse cuando y en la medida en que:
    a) los actos legislativos de armonización de la Unión enumerados en el anexo I, sección A, establezcan requisitos u obligaciones que proporcionen un nivel de protección de la salud, la seguridad o los derechos fundamentales equivalente o superior al del requisito u obligación de que se trate, y
    b) dicha limitación no reduzca el nivel global de protección previsto en el presente Reglamento.

A más tardar el 2 de agosto de 2027, la Comisión adoptará actos delegados con arreglo al artículo 97 a fin de completar el presente Reglamento especificando los sistemas de IA de alto riesgo afectados, los requisitos u obligaciones que pueden limitarse, las condiciones en las que se aplica dicha limitación y el alcance de la limitación.

ARTÍCULO 3
DEFINICIONES

A los efectos del presente Reglamento, se entenderá por:

1) «sistema de IA»: un sistema basado en una máquina que está diseñado para funcionar con distintos niveles de autonomía y que pueda mostrar capacidad de adaptación tras el despliegue, y que, para objetivos explícitos o implícitos, infiere de la información de entrada que recibe la manera de generar resultados de salida, como predicciones, contenidos, recomendaciones o decisiones, que pueden influir en entornos físicos o virtuales;

2) «riesgo»: la combinación de la probabilidad de que se produzca un perjuicio y la gravedad de dicho perjuicio;

3) «proveedor»: una persona física o jurídica, autoridad pública, órgano u organismo que desarrolle un sistema de IA o un modelo de IA de uso general o para el que se desarrolle un sistema de IA o un modelo de IA de uso general y lo introduzca en el mercado o ponga en servicio el sistema de IA con su propio nombre o marca, previo pago o gratuitamente;

4) «responsable del despliegue»: una persona física o jurídica, o autoridad pública, órgano u organismo que utilice un sistema de IA bajo su propia autoridad, salvo cuando su uso se enmarque en una actividad personal de carácter no profesional;

5) «representante autorizado»: una persona física o jurídica ubicada o establecida en la Unión que haya recibido y aceptado el mandato por escrito de un proveedor de un sistema de IA o de un modelo de IA de uso general para cumplir las obligaciones y llevar a cabo los procedimientos establecidos en el presente Reglamento en representación de dicho proveedor;

6) «importador»: una persona física o jurídica ubicada o establecida en la Unión que introduzca en el mercado un sistema de IA que lleve el nombre o la marca de una persona física o jurídica establecida en un tercer país;

7) «distribuidor»: una persona física o jurídica que forme parte de la cadena de suministro, distinta del proveedor o el importador, que comercialice un sistema de IA en el mercado de la Unión;

8) «operador»: un proveedor, fabricante del producto, responsable del despliegue, representante autorizado, importador o distribuidor;

9) «introducción en el mercado»: la primera comercialización en el mercado de la Unión de un sistema de IA o de un modelo de IA de uso general;

10) «comercialización»: el suministro de un sistema de IA o de un modelo de IA de uso general para su distribución o utilización en el mercado de la Unión en el transcurso de una actividad comercial, previo pago o gratuitamente;

11) «puesta en servicio»: el suministro de un sistema de IA para su primer uso directamente al responsable del despliegue o para uso propio en la Unión para su finalidad prevista;

12) «finalidad prevista»: el uso para el que un proveedor concibe un sistema de IA, incluidos el contexto y las condiciones de uso concretos, según la información facilitada por el proveedor en las instrucciones de uso, los materiales y las declaraciones de promoción y venta, y la documentación técnica;

13) «uso indebido razonablemente previsible»: la utilización de un sistema de IA de un modo que no corresponde a su finalidad prevista, pero que puede derivarse de un comportamiento humano o una interacción con otros sistemas, incluidos otros sistemas de IA, razonablemente previsible;

14) «componente de seguridad»: un componente de un producto o un sistema de IA que cumple una función de seguridad para dicho producto o sistema de IA, o cuyo fallo o defecto de funcionamiento pone en peligro la salud y la seguridad de las personas o los bienes; a efectos de la presente definición, un componente cumple una función de seguridad cuando su finalidad prevista es prevenir o mitigar los riesgos para la salud y la seguridad de las personas o los bienes;

14 bis) «microempresa, pequeña o mediana empresa» o «pyme»: una microempresa, o una pequeña o mediana empresa, tal como se definen en el artículo 2 del anexo de la Recomendación 2003/361/CE;

14 ter) «pequeña empresa de mediana capitalización»: una empresa pequeña de mediana capitalización, tal como se define en el punto 2 del anexo de la Recomendación (UE) 2025/1099;

15) «instrucciones de uso»: la información facilitada por el proveedor para informar al responsable del despliegue, en particular, de la finalidad prevista y de la correcta utilización de un sistema de IA;

16) «recuperación de un sistema de IA»: toda medida encaminada a conseguir la devolución al proveedor de un sistema de IA puesto a disposición de los responsables del despliegue, a inutilizarlo o a desactivar su uso;

17) «retirada de un sistema de IA»: toda medida destinada a impedir la comercialización de un sistema de IA que se encuentra en la cadena de suministro;

18) «funcionamiento de un sistema de IA»: la capacidad de un sistema de IA para alcanzar su finalidad prevista;

19) «autoridad notificante»: la autoridad nacional responsable de establecer y llevar a cabo los procedimientos necesarios para la evaluación, designación y notificación de los organismos de evaluación de la conformidad, así como de su supervisión;

20) «evaluación de la conformidad»: el proceso por el que se demuestra si se han cumplido los requisitos establecidos en el capítulo III, sección 2, en relación con un sistema de IA de alto riesgo;

21) «organismo de evaluación de la conformidad»: un organismo que desempeña actividades de evaluación de la conformidad de terceros, como el ensayo, la certificación y la inspección;

22) «organismo notificado»: un organismo de evaluación de la conformidad notificado con arreglo al presente Reglamento y a otros actos pertinentes de la legislación de armonización de la Unión;

23) «modificación sustancial»: un cambio en un sistema de IA tras su introducción en el mercado o puesta en servicio que no haya sido previsto o proyectado en la evaluación de la conformidad inicial realizada por el proveedor y a consecuencia del cual se vea afectado el cumplimiento por parte del sistema de IA de los requisitos establecidos en el capítulo III, sección 2, o que dé lugar a una modificación de la finalidad prevista para la que se haya evaluado el sistema de IA de que se trate;

24) «marcado CE»: un marcado con el que un proveedor indica que un sistema de IA es conforme con los requisitos establecidos en el capítulo III, sección 2, y con otros actos aplicables de la legislación de armonización de la Unión que prevén su colocación;

25) «sistema de vigilancia poscomercialización»: todas las actividades realizadas por los proveedores de sistemas de IA destinadas a recoger y examinar la experiencia obtenida con el uso de sistemas de IA que introducen en el mercado o ponen en servicio, con objeto de detectar la posible necesidad de aplicar inmediatamente cualquier tipo de medida correctora o preventiva que resulte necesaria;

26) «autoridad de vigilancia del mercado»: la autoridad nacional que lleva a cabo las actividades y adopta las medidas previstas en el Reglamento (UE) 2019/1020;

27) «norma armonizada»: una norma armonizada tal como se define en el artículo 2, punto 1, letra c), del Reglamento (UE) n. o 1025/2012;

28) «especificación común»: un conjunto de especificaciones técnicas tal como se definen en el artículo 2, punto 4, del Reglamento (UE) n. o 1025/2012 que proporciona medios para cumplir determinados requisitos establecidos en virtud del presente Reglamento;

29) «datos de entrenamiento»: los datos usados para entrenar un sistema de IA mediante el ajuste de sus parámetros entrenables;

30) «datos de validación»: los datos usados para proporcionar una evaluación del sistema de IA entrenado y adaptar sus parámetros no entrenables y su proceso de aprendizaje para, entre otras cosas, evitar el subajuste o el sobreajuste;

31) «conjunto de datos de validación»: un conjunto de datos independiente o una parte del conjunto de datos de entrenamiento, obtenida mediante una división fija o variable;

32) «datos de prueba»: los datos usados para proporcionar una evaluación independiente del sistema de IA, con el fin de confirmar el funcionamiento previsto de dicho sistema antes de su introducción en el mercado o su puesta en servicio;

33) «datos de entrada»: los datos proporcionados a un sistema de IA u obtenidos directamente por él a partir de los cuales produce un resultado de salida;

34) «datos biométricos»: los datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física, como imágenes faciales o datos dactiloscópicos;

35) «identificación biométrica»: el reconocimiento automatizado de características humanas de tipo físico, fisiológico, conductual o psicológico para determinar la identidad de una persona física comparando sus datos biométricos con los datos biométricos de personas almacenados en una base de datos;

36) «verificación biométrica»: la verificación automatizada y uno-a- uno, incluida la autenticación, de la identidad de las personas físicas mediante la comparación de sus datos biométricos con los datos biométricos facilitados previamente;

37) «categorías especiales de datos personales»: las categorías de datos personales a que se refieren el artículo 9, apartado 1, del Reglamento (UE) 2016/679, el artículo 10 de la Directiva (UE) 2016/680 y el artículo 10, apartado 1, del Reglamento (UE) 2018/1725;

38) «datos operativos sensibles»: los datos operativos relacionados con actividades de prevención, detección, investigación o enjuiciamiento de delitos cuya divulgación podría poner en peligro la integridad de las causas penales;

39) «sistema de reconocimiento de emociones»: un sistema de IA destinado a distinguir o inferir las emociones o las intenciones de las personas físicas a partir de sus datos biométricos;

40) «sistema de categorización biométrica»: un sistema de IA destinado a incluir a las personas físicas en categorías específicas en función de sus datos biométricos, a menos que sea accesorio a otro servicio comercial y estrictamente necesario por razones técnicas objetivas;

41) «sistema de identificación biométrica remota»: un sistema de IA destinado a identificar a las personas físicas sin su participación activa y generalmente a distancia comparando sus datos biométricos con los que figuran en una base de datos de referencia;

42) «sistema de identificación biométrica remota en tiempo real»: un sistema de identificación biométrica remota, en el que la recogida de los datos biométricos, la comparación y la identificación se producen sin una demora significativa; engloba no solo la identificación instantánea, sino también, a fin de evitar la elusión, demoras mínimas limitadas;

43) «sistema de identificación biométrica remota en diferido»: cualquier sistema de identificación biométrica remota que no sea un sistema de identificación biométrica remota en tiempo real;

44) «espacio de acceso público»: cualquier lugar físico, de propiedad privada o pública, al que pueda acceder un número indeterminado de personas físicas, con independencia de que deban cumplirse determinadas condiciones de acceso y con independencia de las posibles restricciones de capacidad;

45) «autoridad garante del cumplimiento del Derecho»:

a) toda autoridad pública competente para la prevención, la investigación, la detección o el enjuiciamiento de delitos o la ejecución de sanciones penales, incluidas la protección frente a amenazas para la seguridad pública y la prevención de dichas amenazas, o

b) cualquier otro organismo o entidad a quien el Derecho del Estado miembro haya confiado el ejercicio de la autoridad pública y las competencias públicas a efectos de prevención, investigación, detección o enjuiciamiento de delitos o ejecución de sanciones penales, incluidas la protección frente a amenazas para la seguridad pública y la prevención de dichas amenazas;

46) «garantía del cumplimiento del Derecho»: las actividades realizadas por las autoridades garantes del cumplimiento del Derecho, o en su nombre, para la prevención, la investigación, la detección o el enjuiciamiento de delitos o la ejecución de sanciones penales, incluidas la protección frente a amenazas para la seguridad pública y la prevención de dichas amenazas;

47) «Oficina de IA»: la función de la Comisión consistente en contribuir a la implantación, el seguimiento y la supervisión de los sistemas de IA y modelos de IA de uso general, y a la gobernanza de la IA prevista por la Decisión de la Comisión de 24 de enero de 2024; las referencias hechas en el presente Reglamento a la Oficina de IA se entenderán hechas a la Comisión;

48) «autoridad nacional competente»: una autoridad notificante o una autoridad de vigilancia del mercado; en lo que respecta a sistemas de IA puestos en servicio o utilizados por instituciones, órganos y organismos de la Unión, las referencias hechas en el presente Reglamento a autoridades nacionales competentes o a autoridades de vigilancia del mercado se interpretarán como referencias al Supervisor Europeo de Protección de Datos;

49) «incidente grave»: un incidente o defecto de funcionamiento de un sistema de IA que, directa o indirectamente, tenga alguna de las siguientes consecuencias:

a) el fallecimiento de una persona o un perjuicio grave para su salud;

b) una alteración grave e irreversible de la gestión o el funcionamiento de infraestructuras críticas;

c) el incumplimiento de obligaciones en virtud del Derecho de la Unión destinadas a proteger los derechos fundamentales;

d) daños graves a la propiedad o al medio ambiente;

50) «datos personales»: los datos personales tal como se definen en el artículo 4, punto 1, del Reglamento (UE) 2016/679;

51) «datos no personales»: los datos que no sean datos personales tal como se definen en el artículo 4, punto 1, del Reglamento (UE) 2016/679;

52) «elaboración de perfiles»: la elaboración de perfiles tal como se define en el artículo 4, punto 4, del Reglamento (UE) 2016/679;

53) «plan de la prueba en condiciones reales»: un documento que describe los objetivos, la metodología, el ámbito geográfico, poblacional y temporal, el seguimiento, la organización y la realización de la prueba en condiciones reales;

54) «plan del espacio controlado de pruebas»: un documento acordado entre el proveedor participante y la autoridad competente en el que se describen los objetivos, las condiciones, el calendario, la metodología y los requisitos para las actividades realizadas en el espacio controlado de pruebas;

55) «espacio controlado de pruebas para la IA»: un marco controlado establecido por una autoridad competente que ofrece a los proveedores y proveedores potenciales de sistemas de IA la posibilidad de desarrollar, entrenar, validar y probar, en condiciones reales cuando proceda, un sistema de IA innovador, con arreglo a un plan del espacio controlado de pruebas y durante un tiempo limitado, bajo supervisión regulatoria;

56) «alfabetización en materia de IA»: las capacidades, los conocimientos y la comprensión que permiten a los proveedores, responsables del despliegue y demás personas afectadas, teniendo en cuenta sus respectivos derechos y obligaciones en el contexto del presente Reglamento, llevar a cabo un despliegue informado de los sistemas de IA y tomar conciencia de las oportunidades y los riesgos que plantea la IA, así como de los perjuicios que puede causar;

57) «prueba en condiciones reales»: la prueba temporal de un sistema de IA para su finalidad prevista en condiciones reales, fuera de un laboratorio u otro entorno de simulación, con el fin de recabar datos sólidos y fiables y evaluar y comprobar la conformidad del sistema de IA con los requisitos del presente Reglamento; si se cumplen todas las condiciones establecidas en el artículo 57 o 60, no se considerará una introducción en el mercado o una puesta en servicio del sistema de IA en el sentido de lo dispuesto en el presente Reglamento;

58) «sujeto»: a los efectos de la prueba en condiciones reales, una persona física que participa en la prueba en condiciones reales;

59) «consentimiento informado»: la expresión libre, específica, inequívoca y voluntaria por parte de un sujeto de su voluntad de participar en una determinada prueba en condiciones reales tras haber sido informado de todos los aspectos de la prueba que sean pertinentes para su decisión de participar;

60) «ultrafalsificación»: un contenido de imagen, audio o vídeo generado o manipulado por una IA que se asemeja a personas, objetos, lugares, entidades o sucesos reales y que puede inducir a una persona a pensar erróneamente que son auténticos o verídicos;

61) «infracción generalizada»: todo acto u omisión contrario al Derecho de la Unión por el que se protegen los intereses de las personas y que:

a) haya perjudicado o pueda perjudicar los intereses colectivos de personas que residen en al menos dos Estados miembros distintos de aquel en el que:

i) se originó o tuvo lugar el acto u omisión,

ii) esté ubicado o establecido el proveedor de que se trate o, en su caso, su representante autorizado, o

iii) esté establecido el responsable del despliegue en el momento de cometer la infracción;

b) haya perjudicado, perjudique o pueda perjudicar los intereses colectivos de las personas y tenga características comunes —incluidas la misma práctica ilícita o la vulneración del mismo interés— y sea

cometido simultáneamente por el mismo operador en al menos tres Estados miembros;

62) «infraestructura crítica»: una infraestructura crítica tal como se define en el artículo 2, punto 4, de la Directiva (UE) 2022/2557;

63) «modelo de IA de uso general»: un modelo de IA, también uno entrenado con un gran volumen de datos utilizando autosupervisión a gran escala, que presenta un grado considerable de generalidad y es capaz de realizar de manera competente una gran variedad de tareas distintas, independientemente de la manera en que el modelo se introduzca en el mercado, y que puede integrarse en diversos sistemas o aplicaciones posteriores, excepto los modelos de IA que se utilizan para actividades de investigación, desarrollo o creación de prototipos antes de su introducción en el mercado;

64) «capacidades de gran impacto»: capacidades que igualan o superan las capacidades mostradas por los modelos de IA de uso general más avanzados;

65) «riesgo sistémico»: un riesgo específico de las capacidades de gran impacto de los modelos de IA de uso general, que tienen unas repercusiones considerables en el mercado de la Unión debido a su alcance o a los efectos negativos reales o razonablemente previsibles en la salud pública, la seguridad, la seguridad pública, los derechos fundamentales o la sociedad en su conjunto, que puede propagarse a gran escala a lo largo de toda la cadena de valor;

66) «sistema de IA de uso general»: un sistema de IA basado en un modelo de IA de uso general y que puede servir para diversos fines, tanto para su uso directo como para su integración en otros sistemas de IA;

67) «operación de coma flotante»: cualquier operación o tarea matemática que implique números de coma flotante, que son un subconjunto de los números reales normalmente representados en los ordenadores mediante un número entero de precisión fija elevado por el exponente entero de una base fija;

68) «proveedor posterior»: un proveedor de un sistema de IA, también de un sistema de IA de uso general, que integra un modelo de IA, con independencia de que el modelo de IA lo proporcione él mismo y esté integrado verticalmente o lo proporcione otra entidad en virtud de relaciones contractuales.

ARTÍCULO 4
ALFABETIZACIÓN EN MATERIA DE IA

1. Los proveedores y responsables del despliegue de sistemas de IA adoptarán medidas para apoyar la promoción de la alfabetización en materia de IA de su personal y demás personas que se encarguen en su nombre del funcionamiento y la utilización de sistemas de IA, teniendo en cuenta sus conocimientos técnicos, su experiencia, su educación y su formación, así como el contexto previsto de uso de los sistemas de IA y las personas o los colectivos de personas en que se van a utilizar dichos sistemas. Esta obligación no exige que los proveedores o los responsables del despliegue garanticen un nivel específico de alfabetización en materia de IA de ninguna persona en particular.
2. La Comisión y los Estados miembros apoyarán y facilitarán los esfuerzos de los proveedores y responsables del despliegue de sistemas de IA, en particular de las pymes, en el cumplimiento de su obligación en virtud del apartado 1 del presente artículo. A tal fin, la Comisión publicará ejemplos prácticos de cómo cumplir dicha obligación en la plataforma única de información a que se refiere el artículo 62, apartado 3, letra b).
3. El Consejo de IA adoptará recomendaciones, teniendo en cuenta los marcos europeos de competencias, con vistas a apoyar a la Comisión y a los Estados miembros en la promoción de la alfabetización en materia de IA exigida en virtud del apartado 1, incluido mediante el establecimiento de objetivos comunes.

ARTÍCULO 4 BIS
TRATAMIENTO DE CATEGORÍAS ESPECIALES DE DATOS PERSONALES PARA LA DETECCIÓN Y CORRECCIÓN DE SESGOS

1. En la medida en que sea estrictamente necesario para garantizar la detección y corrección de los sesgos asociados a los sistemas de IA de alto riesgo de conformidad con lo dispuesto en el artículo 10, apartado 2, letras f) y g), del presente Reglamento, los proveedores de dichos sistemas podrán tratar excepcionalmente las categorías especiales de datos personales siempre que ofrezcan las garantías adecuadas en relación con los derechos y las libertades fundamentales de las personas físicas. Además de las disposiciones establecidas en los Reglamentos (UE) 2016/679 y (UE) 2018/1725 y la Directiva (UE) 2016/680, según proceda, para que se produzca dicho tratamiento deberán cumplirse todas las condiciones siguientes:
   a) que el tratamiento de otros datos, como los sintéticos o los anonimizados, no permita efectuar de forma efectiva la detección y corrección de sesgos;
   b) que las categorías especiales de datos personales estén sujetas a limitaciones técnicas relativas a la reutilización de los datos personales y a medidas punteras en materia de seguridad y protección de la intimidad, incluida la pseudonimización;
   c) que las categorías especiales de datos personales estén sujetas a medidas para garantizar que los datos personales tratados estén asegurados, protegidos y sujetos a garantías adecuadas, incluidos controles estrictos y documentación del acceso, a fin de evitar el uso indebido y garantizar que solo las personas autorizadas tengan acceso a dichos datos personales con obligaciones de confidencialidad adecuadas;
   d) que las categorías especiales de datos personales no se transmitan ni transfieran a terceros y que estos no puedan acceder de ningún otro modo a ellos;
   e) que las categorías especiales de datos personales se eliminen una vez que se haya corregido el sesgo o los datos personales hayan llegado al final de su período de conservación, si esta fecha es anterior, y
   f) que los registros de las actividades de tratamiento en virtud de los Reglamentos (UE) 2016/679 y (UE) 2018/1725 y la Directiva (UE) 2016/680 incluyan las razones por las que el tratamiento de categorías especiales de datos personales era estrictamente necesario para detectar y corregir sesgos, y por las que ese objetivo no podía alcanzarse mediante el tratamiento de otros datos.
2. Los proveedores y responsables del despliegue de otros sistemas y modelos de IA y los responsables del despliegue de sistemas de IA de alto riesgo podrán excepcionalmente tratar categorías especiales de datos personales en la medida en que:

a) dicho tratamiento sea estrictamente necesario para garantizar la detección y corrección de sesgos atendiendo a posibles sesgos que afecten probablemente a la salud y la seguridad de las personas, tengan consecuencias negativas para los derechos fundamentales o den lugar a una discriminación prohibida por el Derecho de la Unión, especialmente cuando las salidas de datos influyan en las informaciones de entrada de futuras operaciones, y

b) se apliquen todas las condiciones y garantías previstas en el apartado 1.

El presente apartado no crea obligación alguna de llevar a cabo dicha detección y corrección de sesgos.

Fuente: Reglamento (UE) 2024/1689, texto consolidado a 27 de julio de 2026. Transcripción del PDF aportado; se han omitido las marcas editoriales de consolidación y las cabeceras de página.

Resumen del Capítulo I — Disposiciones generales

Reglamento (UE) 2024/1689 de Inteligencia Artificial · Texto consolidado a 27/07/2026 · Páginas 2–12

Este capítulo establece las bases del Reglamento Europeo de Inteligencia Artificial: **qué pretende conseguir, a quién afecta, qué conceptos utiliza y cuáles son las primeras obligaciones para las empresas**.

Artículo 1. Objeto

El objetivo es impulsar una inteligencia artificial fiable, segura y centrada en las personas, sin frenar la innovación.

El Reglamento establece normas sobre la comercialización y utilización de IA, las prácticas prohibidas, los sistemas de alto riesgo, la transparencia, los modelos de uso general y los mecanismos de supervisión y cumplimiento.

Idea principal: Europa no prohíbe utilizar la IA, sino que establece reglas para que se desarrolle y utilice respetando la seguridad y los derechos fundamentales.

CELEX_02024R1689-20260727_ES_TXT.pdf

Artículo 2. Ámbito de aplicación

Determina a quién afecta el Reglamento.

- **Proveedores:** empresas que desarrollan o comercializan sistemas o modelos de IA.
- **Responsables del despliegue:** empresas y organizaciones que utilizan sistemas de IA bajo su responsabilidad.
- **Importadores y distribuidores:** quienes comercializan sistemas de IA en el mercado europeo.
- **Empresas de terceros países:** también pueden estar sujetas cuando los resultados de sus sistemas se utilizan en la UE.
- **Personas afectadas:** personas ubicadas en la UE cuyos derechos puedan verse afectados.

Existen exclusiones, entre ellas determinados usos exclusivamente militares, de defensa, seguridad nacional, investigación científica y actividades estrictamente personales no profesionales.

Además, se mantiene la aplicación de las normas de protección de datos, como el RGPD.

Aplicación empresarial: una empresa que utiliza IA integrada en un ERP puede estar sujeta al Reglamento aunque no haya desarrollado la tecnología. Sin embargo, las obligaciones concretas dependen del sistema y de su utilización.

CELEX_02024R1689-20260727_ES_TXT.pdf

Artículo 3. Definiciones

Establece los conceptos jurídicos fundamentales que se utilizan en todo el Reglamento.

Entre los más importantes:

Concepto	Significado práctico
Sistema de IA	Sistema automatizado que infiere resultados como predicciones, recomendaciones, contenidos o decisiones.
Proveedor	Quien desarrolla o comercializa una solución de IA bajo su nombre o marca.
Responsable del despliegue	Quien utiliza el sistema de IA bajo su autoridad.

Concepto	Significado práctico
Riesgo	Combinación de la probabilidad de un perjuicio y su gravedad.
Supervisión y conformidad	Conceptos relacionados con el control y la evaluación del cumplimiento.
Modelo de IA de uso general	Modelo capaz de desempeñar distintas tareas y utilizarse en diversas aplicaciones.
Alfabetización en IA	Conocimientos necesarios para utilizar la IA de manera informada, comprendiendo sus posibilidades y riesgos.

Aplicación empresarial: resulta especialmente importante distinguir entre el fabricante del sistema, la empresa que lo integra y el cliente que lo utiliza, porque sus responsabilidades pueden ser diferentes.

Artículo 4. Alfabetización en materia de IA

Especialmente relevante para las empresas

Los proveedores y responsables del despliegue deben adoptar medidas para fomentar los conocimientos sobre IA de sus trabajadores y de quienes utilicen estos sistemas en su nombre.

Esas medidas deben considerar la experiencia, formación y conocimientos técnicos de los usuarios, el contexto de utilización y las personas que puedan verse afectadas.

La redacción consolidada de 2026 aclara que **no es obligatorio garantizar un nivel específico de conocimientos para cada persona**, aunque sí adoptar medidas para promover la alfabetización.

Aplicación empresarial: formar adecuadamente al personal en las herramientas de IA que utiliza, sus limitaciones, los riesgos de introducir información confidencial y la necesidad de comprobar los resultados.

CELEX_02024R1689-20260727_ES_TXT.pdf

Artículo 4 bis. Tratamiento de datos sensibles para detectar sesgos

Incorporado en la modificación de 2026

Regula cuándo se pueden tratar excepcionalmente categorías especiales de datos personales para detectar y corregir sesgos en sistemas de IA.

El tratamiento debe ser estrictamente necesario y estar sometido a garantías específicas, como medidas de seguridad, limitación de accesos, protección de la privacidad y eliminación de los datos cuando corresponda.

Se contempla tanto para determinados proveedores de sistemas de alto riesgo como, bajo condiciones específicas, para otros proveedores y responsables del despliegue.

Aplicación empresarial: si una herramienta de IA toma decisiones sobre candidatos, empleados o clientes, pueden existir riesgos de discriminación. Este artículo permite, en determinadas circunstancias, analizar datos especialmente protegidos para detectar esos sesgos, pero no autoriza su utilización indiscriminada.

Conclusión: ¿qué supone este capítulo para una empresa?

El capítulo I establece tres ideas fundamentales:

La empresa que utiliza IA también tiene responsabilidades, aunque compre la tecnología a un proveedor externo.

Los trabajadores deben disponer de conocimientos adecuados para utilizar los sistemas de IA de forma informada.

La protección de datos y los derechos fundamentales siguen siendo esenciales, especialmente cuando la IA interviene en decisiones sobre personas.

En el contexto de un ERP como Sage 200, este capítulo significa que incorporar funcionalidades de IA no es únicamente una cuestión tecnológica: también exige comprender quién responde por cada sistema, preparar a los usuarios y utilizar correctamente la información empresarial.

TEXTO OFICIAL · CAPÍTULO II

CAPÍTULO II
PRÁCTICAS DE IA PROHIBIDAS

ARTÍCULO 5
PRÁCTICAS DE IA PROHIBIDAS

1. Quedan prohibidas las siguientes prácticas de IA:

a) la introducción en el mercado, la puesta en servicio o la utilización de un sistema de IA que se sirva de técnicas subliminales que trasciendan la conciencia de una persona o de técnicas deliberadamente manipuladoras o engañosas con el objetivo o el efecto de alterar de manera sustancial el comportamiento de una persona o un colectivo de personas, mermando de manera apreciable su capacidad para tomar una decisión informada y haciendo que tomen una decisión que de otro modo no habrían tomado, de un modo que provoque, o sea razonablemente probable que provoque, perjuicios considerables a esa persona, a otra persona o a un colectivo de personas;

b) la introducción en el mercado, la puesta en servicio o la utilización de un sistema de IA que explote alguna de las vulnerabilidades de una persona física o un determinado colectivo de personas derivadas de su edad o discapacidad, o de una situación social o económica específica, con la finalidad o el efecto de alterar de manera sustancial el comportamiento de dicha persona o de una persona que pertenezca a dicho colectivo de un modo que provoque, o sea razonablemente probable que provoque, perjuicios considerables a esa persona o a otra;

b bis) la introducción en el mercado, la puesta en servicio o la utilización de un sistema de IA que genere o manipule imágenes, vídeos o audios realistas o material similar de las partes íntimas de una persona física identificable, o de una persona física identificable que participe en actividades sexualmente explícitas, sin el consentimiento libre, específico, informado e inequívoco y explícito de dicha persona para tal generación o manipulación;

b ter) la introducción en el mercado, la puesta en servicio o la utilización de un sistema de IA que genere o manipule material o espectáculos en el sentido del artículo 2, letras c) y e), de la Directiva 2011/93/UE, excepto cuando se aplique una defensa de «forma ilícita» en virtud del Derecho nacional;

c) la introducción en el mercado, la puesta en servicio o la utilización de sistemas de IA para evaluar o clasificar a personas físicas o a colectivos de personas durante un período determinado de tiempo atendiendo a su comportamiento social o a características personales o de su personalidad conocidas, inferidas o predichas, de forma que la puntuación ciudadana resultante provoque una o varias de las situaciones siguientes:

i) un trato perjudicial o desfavorable hacia determinadas personas físicas o colectivos de personas en contextos sociales que no guarden relación con los contextos donde se generaron o recabaron los datos originalmente,

ii) un trato perjudicial o desfavorable hacia determinadas personas físicas o colectivos de personas que sea injustificado o desproporcionado con respecto a su comportamiento social o la gravedad de este;

d) la introducción en el mercado, la puesta en servicio para este fin específico o el uso de un sistema de IA para realizar evaluaciones de riesgos de personas físicas con el fin de valorar o predecir el riesgo de que una persona física cometa un delito basándose únicamente en la elaboración del perfil de una persona física o en la evaluación de los rasgos y características de su personalidad; esta prohibición no se aplicará a los sistemas de IA utilizados para apoyar la valoración humana de la implicación de una persona en una actividad delictiva que ya se base en hechos objetivos y verificables directamente relacionados con una actividad delictiva;

e) la introducción en el mercado, la puesta en servicio para este fin específico o el uso de sistemas de IA que creen o amplíen bases de datos de reconocimiento facial mediante la extracción no selectiva de imágenes faciales de internet o de circuitos cerrados de televisión;

f) la introducción en el mercado, la puesta en servicio para este fin específico o el uso de sistemas de IA para inferir las emociones de una persona física en los lugares de trabajo y en los centros educativos, excepto cuando el sistema de IA esté destinado a ser instalado o introducido en el mercado por motivos médicos o de seguridad;

g) la introducción en el mercado, la puesta en servicio para este fin específico o el uso de sistemas de categorización biométrica que clasifiquen individualmente a las personas físicas sobre la base de sus datos biométricos para deducir o inferir su raza, opiniones políticas, afiliación sindical, convicciones religiosas o filosóficas, vida sexual u orientación sexual; esta prohibición no incluye el etiquetado o filtrado de conjuntos de datos biométricos adquiridos lícitamente, como imágenes, basado en datos biométricos ni la categorización de datos biométricos en el ámbito de la garantía del cumplimiento del Derecho;

h) el uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de garantía del cumplimiento del Derecho, salvo y en la medida en que dicho uso sea estrictamente necesario para alcanzar uno o varios de los objetivos siguientes:

i) la búsqueda selectiva de víctimas concretas de secuestro, trata de seres humanos o explotación sexual de seres humanos, así como la búsqueda de personas desaparecidas,

ii) la prevención de una amenaza específica, importante e inminente para la vida o la seguridad física de las personas físicas o de una amenaza real y actual o real y previsible de un atentado terrorista,

iii) la localización o identificación de una persona sospechosa de haber cometido un delito a fin de llevar a cabo una investigación o un enjuiciamiento penales o de ejecutar una sanción penal por alguno de los delitos mencionados en el anexo II que en el Estado miembro de que se trate se castigue con una pena o una medida de seguridad privativas de libertad cuya duración máxima sea de al menos cuatro años.

El párrafo primero, letra h), se entiende sin perjuicio de lo dispuesto en el artículo 9 del Reglamento (UE) 2016/679 en lo que respecta al tratamiento de datos biométricos con fines distintos de la garantía del cumplimiento del Derecho.

1 bis. A efectos del apartado 1, párrafo primero, letras b bis) y b ter):

a) la introducción en el mercado o la puesta en servicio de un sistema de IA que genere o manipule el material o los espectáculos a que se refiere el apartado 1, párrafo primero, letras b bis) o b ter), solo estará prohibida cuando:

i) dicha generación o manipulación sea la finalidad prevista del sistema de IA, o

ii) el diseño, el entrenamiento, la arquitectura, las capacidades o las funcionalidades orientadas al usuario del sistema hagan que esa generación o manipulación sea un resultado razonablemente previsible y reproducible, sin requerir modificaciones técnicas sustanciales, y el sistema no disponga de medidas técnicas de seguridad razonables y adecuadas y de otras salvaguardias para evitar de forma fiable dicha generación o manipulación, tomando en consideración un uso indebido razonablemente previsible, ni para corregir el uso indebido observado o notificado;

b) la utilización de un sistema de IA que genere o manipule el material o los espectáculos a que se refiere el apartado 1, párrafo primero, letras b bis) y b ter), solo está prohibida cuando el responsable del despliegue utilice el sistema con el fin de generar o manipular dicho material o espectáculos.

1 ter. A efectos del apartado 1, párrafo primero, letra b bis), no constituirán manipulación los sistemas de IA que manipulen el material en un modo que no aumente la exposición de ninguna parte íntima representada ni altere la naturaleza de ninguna actividad sexualmente explícita representada.

2. El uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de garantía del cumplimiento del Derecho para cualquiera de los objetivos mencionados en el apartado 1, párrafo primero, letra h), debe desplegarse para los fines establecidos en dicha letra, únicamente para confirmar la identidad de la persona que constituya el objetivo específico y tendrá en cuenta los siguientes aspectos:

a) la naturaleza de la situación que dé lugar al posible uso, y en particular la gravedad, probabilidad y magnitud del perjuicio que se produciría de no utilizarse el sistema;

b) las consecuencias que tendría el uso del sistema en los derechos y las libertades de las personas implicadas, y en particular la gravedad, probabilidad y magnitud de dichas consecuencias.

Además, el uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de garantía del cumplimiento del Derecho para cualquiera de los objetivos mencionados en el apartado 1, párrafo primero, letra h), del presente artículo deberá cumplir garantías y condiciones necesarias y proporcionadas en relación con el uso de conformidad con el Derecho nacional que autorice dicho uso, en particular en lo que respecta a las limitaciones temporales, geográficas y personales. El uso del sistema de identificación biométrica remota «en tiempo real» en espacios de acceso público solo se autorizará si la autoridad garante del cumplimiento del Derecho ha completado una evaluación de impacto relativa a los derechos fundamentales según lo dispuesto en el artículo 27 y ha registrado el sistema en la base de datos de la UE de conformidad con el artículo 49. No obstante, en casos de urgencia debidamente justificados, se podrá empezar a utilizar tales sistemas sin el registro en la base de datos de la UE, siempre que dicho registro se complete sin demora indebida.

3. A los efectos del apartado 1, párrafo primero, letra h), y el apartado 2, todo uso de un sistema de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de garantía del cumplimiento del Derecho estará supeditado a la concesión de una autorización previa por parte de una autoridad judicial o una autoridad administrativa independiente cuya decisión sea vinculante del Estado miembro en el que vaya a utilizarse dicho sistema, que se expedirá previa solicitud motivada y de conformidad con las normas detalladas del Derecho nacional mencionadas en el apartado 5. No obstante, en una situación de urgencia debidamente justificada, se podrá empezar a utilizar tal sistema sin autorización siempre que se solicite dicha autorización sin demora indebida, a más tardar en un plazo de veinticuatro horas. Si se rechaza dicha autorización, el uso se interrumpirá con efecto inmediato y todos los datos, así como los resultados y la información de salida generados por dicho uso, se desecharán y suprimirán inmediatamente.

La autoridad judicial competente o una autoridad administrativa independiente cuya decisión sea vinculante únicamente concederá la autorización cuando tenga constancia, sobre la base de pruebas objetivas o de indicios claros que se le aporten, de que el uso del sistema de identificación biométrica remota «en tiempo real» es necesario y proporcionado para alcanzar alguno de los objetivos especificados en el apartado 1, párrafo primero, letra h), el cual se indicará en la solicitud, y, en particular, se limita a lo estrictamente necesario en lo que se refiere al período de tiempo, así como al ámbito geográfico y personal. Al pronunciarse al respecto, esa autoridad tendrá en cuenta los aspectos mencionados en el apartado 2. Dicha autoridad no podrá adoptar ninguna decisión que produzca efectos jurídicos adversos para una persona exclusivamente sobre la base de los resultados de salida del sistema de identificación biométrica remota «en tiempo real».

4. Sin perjuicio de lo dispuesto en el apartado 3, todo uso de un sistema de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de garantía del cumplimiento del Derecho se notificará a la autoridad de vigilancia del mercado pertinente y a la autoridad nacional de protección de datos de conformidad con las normas nacionales a que se refiere el apartado 5. La notificación contendrá, como mínimo, la información especificada en el apartado 6 y no incluirá datos operativos sensibles.

5. Los Estados miembros podrán decidir contemplar la posibilidad de autorizar, ya sea total o parcialmente, el uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de garantía del cumplimiento del Derecho dentro de los límites y en las condiciones que se indican en el apartado 1, párrafo primero, letra h), y los apartados 2 y 3. Los Estados miembros de que se trate deberán establecer en sus respectivos Derechos nacionales las normas detalladas necesarias aplicables a la solicitud, la concesión y el ejercicio de las autorizaciones a que se refiere el apartado 3, así como a la supervisión y la presentación de informes relacionadas con estas. Dichas normas especificarán también para qué objetivos de los enumerados en el apartado 1, párrafo primero, letra h), y en su caso en relación con qué delitos de los indicados en la letra h),

inciso iii), se podrá autorizar a las autoridades competentes para que utilicen esos sistemas con fines de garantía del cumplimiento del Derecho. Los Estados miembros notificarán dichas normas a la Comisión a más tardar treinta días después de su adopción. Los Estados miembros podrán adoptar, de conformidad con el Derecho de la Unión, leyes más restrictivas sobre el uso de sistemas de identificación biométrica remota.

6. Las autoridades nacionales de vigilancia del mercado y las autoridades nacionales de protección de datos de los Estados miembros a las que se haya notificado el uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de garantía del cumplimiento del Derecho con arreglo al apartado 4 presentarán a la Comisión informes anuales sobre dicho uso. A tal fin, la Comisión facilitará a los Estados miembros y a las autoridades nacionales de vigilancia del mercado y de protección de datos un modelo que incluya información sobre el número de decisiones adoptadas por las autoridades judiciales competentes o una autoridad administrativa independiente cuya decisión sea vinculante en relación con las solicitudes de autorización de conformidad con el apartado 3, así como su resultado.
7. La Comisión publicará informes anuales sobre el uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de garantía del cumplimiento del Derecho elaborados basados en datos agregados relativos a los Estados miembros sobre la base de los informes anuales a que se refiere el apartado 6. Dichos informes anuales no incluirán datos operativos sensibles de las actividades de garantía del cumplimiento del Derecho conexas.
8. El presente artículo no afectará a las prohibiciones aplicables cuando una práctica de IA infrinja otras disposiciones de Derecho de la Unión.

Fuente: Reglamento (UE) 2024/1689, texto consolidado a 27 de julio de 2026. Transcripción del PDF aportado; se han omitido las marcas editoriales de consolidación y las cabeceras de página.

Resumen del Capítulo II — Prácticas de inteligencia artificial prohibidas

Reglamento (UE) 2024/1689 · Texto consolidado a 27/07/2026 · Páginas 13–17

Este capítulo establece **qué usos de la inteligencia artificial están prohibidos en la Unión Europea** por considerarse incompatibles con la protección de las personas, sus derechos fundamentales o su seguridad.

A diferencia de los sistemas de alto riesgo, que pueden utilizarse cumpliendo determinados requisitos, las prácticas aquí contempladas no están permitidas, salvo las excepciones expresamente previstas.

El capítulo contiene un único artículo: el **artículo 5, Prácticas de IA prohibidas**.

1. Prácticas de IA prohibidas

El artículo 5 identifica las siguientes prácticas:

1. Manipulación del comportamiento humano

Prohibición de sistemas que utilizan técnicas subliminales, manipuladoras o engañosas para alterar sustancialmente las decisiones de las personas, reduciendo su capacidad de decidir de manera informada y provocando, o pudiendo provocar, perjuicios considerables.

Ejemplo: una IA diseñada para manipular psicológicamente a clientes y conseguir decisiones de compra perjudiciales que de otro modo no tomarían.

2. Explotación de personas vulnerables

Prohibición de sistemas que aprovechan vulnerabilidades derivadas de la edad, discapacidad o situación social o económica para alterar sustancialmente el comportamiento, causando o pudiendo causar perjuicios considerables.

Ejemplo: una herramienta comercial que explota deliberadamente las dificultades económicas de personas vulnerables para inducirlas a contratar productos perjudiciales.

3. Generación de contenido íntimo sin consentimiento

La modificación de 2026 introduce prohibiciones relativas a la creación o manipulación de imágenes, vídeos o audios realistas de contenido íntimo o sexualmente explícito de personas identificables sin el consentimiento exigido, así como de determinado material de abuso sexual infantil.

Ejemplo: generar imágenes íntimas falsas de un trabajador o una persona conocida sin su consentimiento. El texto establece condiciones específicas sobre cuándo se prohíbe comercializar el sistema y cuándo se prohíbe su utilización.

4. Puntuación social de las personas (social scoring)

Prohibición de utilizar IA para clasificar a las personas por su comportamiento social o características personales cuando la puntuación produce un trato perjudicial injustificado, desproporcionado o en contextos no relacionados.

Ejemplo: una puntuación general de «buen ciudadano» que condiciona el acceso a servicios o beneficios sin justificación adecuada.

5. Predicción de delitos basada únicamente en perfiles personales

Prohibición de sistemas que evalúan o predicen la probabilidad de que una persona cometa un delito basándose exclusivamente en su perfil o rasgos de personalidad.

Ejemplo: un programa policial que predice quién puede delinquir únicamente por sus características personales, sin hechos objetivos y verificables relacionados con actividades delictivas.

6. Captura masiva de rostros

Prohibición de crear o ampliar bases de datos de reconocimiento facial mediante la extracción indiscriminada de imágenes de internet o de cámaras de vigilancia.

Ejemplo: recopilar automáticamente millones de fotografías de redes sociales para construir una base de identificación facial.

7. Reconocimiento de emociones en el trabajo y la educación

Prohibición de utilizar sistemas de IA que infieran emociones a partir de datos biométricos en centros de trabajo y educativos, salvo los usos previstos por motivos médicos o de seguridad.

Ejemplo: cámaras con IA que analizan los rostros de los empleados para determinar si están contentos, frustrados o motivados.

8. Clasificación biométrica por características sensibles

Prohibición de determinados sistemas que utilizan datos biométricos para inferir raza, opiniones políticas, afiliación sindical, creencias religiosas, vida sexual u orientación sexual.

Ejemplo: una IA que analiza rostros para inferir la orientación sexual o las creencias religiosas de las personas.

9. Identificación biométrica remota en tiempo real en espacios públicos

Se prohíbe su utilización con fines policiales como regla general, aunque existen excepciones muy restringidas para determinadas situaciones de especial gravedad.

Ejemplo: identificar automáticamente a los peatones mediante reconocimiento facial en directo con fines policiales sin cumplir las excepciones y garantías legales.

Los apartados relativos a las prácticas prohibidas están recogidos en las páginas 13–15 del documento.

CELEX_02024R1689-20260727_ES_TXT.pdf

2. Excepciones al reconocimiento facial en tiempo real

El artículo 5 permite excepcionalmente la identificación biométrica remota en espacios públicos con fines policiales cuando sea estrictamente necesaria para:

- Buscar víctimas de secuestro, trata o explotación sexual, o personas desaparecidas.
- Prevenir amenazas graves e inminentes para la vida o seguridad de las personas y determinadas amenazas terroristas.
- Identificar o localizar sospechosos de determinados delitos graves recogidos en el anexo II.

Su uso debe cumplir garantías como autorización judicial o administrativa independiente vinculante, necesidad, proporcionalidad, limitaciones temporales y geográficas, evaluación del impacto en derechos fundamentales y supervisión.

En situaciones de urgencia debidamente justificadas se permite solicitar la autorización posteriormente, dentro de un máximo de 24 horas, con las condiciones establecidas por el Reglamento.

CELEX_02024R1689-20260727_ES_TXT.pdf

3. ¿Cómo afecta este capítulo a las empresas?

Estas son algunas situaciones empresariales que conviene distinguir:

Utilización de IA	¿Qué establece el capítulo II?
IA que analiza facturas, gastos o documentos	No está prohibida por estas funciones.
IA que ayuda a decidir a quién conceder financiación	No está prohibida de forma general; puede estar sometida a requisitos de alto riesgo.
IA que puntúa el rendimiento laboral	No está prohibida automáticamente; depende de su funcionamiento y puede ser de alto riesgo.
IA que detecta emociones de empleados mediante biometría	Prohibida, salvo excepciones médicas o de seguridad.
IA comercial que manipula de forma perjudicial decisiones personales	Prohibida cuando concurren las condiciones del artículo 5.
IA que infiere afiliación sindical mediante datos biométricos	Prohibida en los supuestos recogidos por el artículo 5.
IA que automatiza tareas administrativas en un ERP	No está prohibida por la mera automatización.

Los ejemplos de aplicación empresarial son interpretaciones prácticas del artículo, no una clasificación jurídica individual de cada producto.

4. ¿Qué ocurre si una empresa utiliza IA prohibida?

El incumplimiento puede dar lugar a medidas de las autoridades competentes, como el cese de la utilización, medidas correctoras y sanciones.

El régimen sancionador se desarrolla en el capítulo XII. Para las infracciones de prácticas prohibidas, el artículo 99 contempla multas de hasta **35 millones de euros o el 7 % del volumen de negocios mundial anual del ejercicio anterior**, si esta última cifra es superior, con reglas específicas y límites diferenciados para pymes y otros supuestos.

5. Conclusión del capítulo II

La idea fundamental es que no todo uso arriesgado de IA está prohibido, pero existen determinados límites que las empresas no pueden superar.

En entornos empresariales y ERP, los principales puntos de atención son la utilización de IA para manipular decisiones, explotar vulnerabilidades, analizar emociones de trabajadores, elaborar perfiles discriminatorios o tratar indebidamente información biométrica.

Para una empresa que utiliza Sage 200, por ejemplo, integrar IA para automatizar contabilidad, analizar ventas o consultar información del negocio no constituye por sí mismo una práctica prohibida.

La cuestión es **cómo se utiliza la tecnología, qué información procesa y qué efectos produce sobre las personas**.

El capítulo III, que viene a continuación, es especialmente importante para las empresas porque establece cuáles son los sistemas de IA de alto riesgo que sí pueden utilizarse, pero bajo obligaciones y controles específicos.

Lo importante: el capítulo I no clasifica por sí mismo todas las herramientas empresariales como sistemas de alto riesgo. Esa cuestión se desarrolla principalmente en el capítulo III.

TEXTO OFICIAL · CAPÍTULO III

CAPÍTULO III
SISTEMAS DE IA DE ALTO RIESGO

SECCIÓN 1
CLASIFICACIÓN DE LOS SISTEMAS DE IA COMO SISTEMAS DE ALTO RIESGO

ARTÍCULO 6
REGLAS DE CLASIFICACIÓN DE LOS SISTEMAS DE IA DE ALTO RIESGO

1. Con independencia de si se ha introducido en el mercado o se ha puesto en servicio sin estar integrado en los productos que se mencionan en las letras a) y b), un sistema de IA se considerará de alto riesgo cuando reúna las dos condiciones que se indican a continuación:

   a) que el sistema de IA esté destinado a ser utilizado como componente de seguridad de un producto que entre en el ámbito de aplicación de los actos legislativos de armonización de la Unión enumerados en el anexo I, o que el propio sistema de IA sea uno de dichos productos, y

   b) que el producto del que el sistema de IA sea componente de seguridad con arreglo a la letra a), o el propio sistema de IA como producto, deba someterse a una evaluación de la conformidad de terceros para su introducción en el mercado o puesta en servicio con arreglo a los actos legislativos de armonización de la Unión enumerados en el anexo I.

1 bis. A efectos del presente Reglamento, incluido el apartado 1 del presente artículo, los sistemas de IA que se utilicen únicamente para aspectos no relacionados con la seguridad en los ámbitos de la asistencia al usuario, la optimización del rendimiento, la eficiencia del servicio, la automatización, la comodidad o el control de calidad no se considerarán componentes de seguridad.

1 ter. No obstante lo dispuesto en el apartado 1 bis, los sistemas de IA cuyo fallo o defecto de funcionamiento pueda poner en peligro la salud y la seguridad se considerarán componentes de seguridad.

1 quater. Se considerará que no cumplen la condición establecida en el apartado 1, letra b), los productos que deban someterse a una evaluación de la conformidad de terceros únicamente debido a riesgos distintos de los riesgos para la salud y la seguridad, en particular los riesgos relacionados con la distribución del espectro radioeléctrico o las interferencias electromagnéticas que no afecten a la salud y la seguridad.

2. Además de los sistemas de IA de alto riesgo a que se refiere el apartado 1, también se considerarán de alto riesgo los sistemas de IA contemplados en el anexo III.

3. No obstante lo dispuesto en el apartado 2, un sistema de IA a que se refiere el anexo III no se considerará de alto riesgo cuando no plantee un riesgo importante de causar un perjuicio a la salud, la seguridad o los derechos fundamentales de las personas físicas, también al no influir sustancialmente en el resultado de la toma de decisiones.

El párrafo primero se aplicará cuando se cumpla cualquiera de las condiciones siguientes:

   a) que el sistema de IA esté destinado a realizar una tarea de procedimiento limitada;

   b) que el sistema de IA esté destinado a mejorar el resultado de una actividad humana previamente realizada;

   c) que el sistema de IA esté destinado a detectar patrones de toma de decisiones o desviaciones con respecto a patrones de toma de decisiones anteriores y no esté destinado a sustituir la valoración humana previamente realizada sin una revisión humana adecuada, ni a influir en ella, o

   d) que el sistema de IA esté destinado a realizar una tarea preparatoria para una evaluación que sea pertinente a efectos de los casos de uso enumerados en el anexo III.

No obstante lo dispuesto en el párrafo primero, los sistemas de IA a que se refiere el anexo III siempre se considerarán de alto riesgo cuando el sistema de IA efectúe la elaboración de perfiles de personas físicas.

4. El proveedor que considere que un sistema de IA contemplado en el anexo III no es de alto riesgo documentará su evaluación antes de que dicho sistema sea introducido en el mercado o puesto en servicio. Dicho proveedor estará sujeto a la obligación de registro establecida en el artículo 49, apartado 2. A petición de las autoridades nacionales competentes, el proveedor facilitará la documentación de la evaluación.

5. La Comisión, previa consulta al Consejo Europeo de Inteligencia Artificial (en lo sucesivo, «Consejo de IA»), y a más tardar el 2 de febrero de 2026, proporcionará directrices que especifiquen la aplicación práctica del presente artículo en consonancia con el artículo 96, junto con una lista exhaustiva de ejemplos prácticos de casos de uso de sistemas de IA que sean de alto riesgo y que no sean de alto riesgo.

6. La Comisión estará facultada para adoptar actos delegados con arreglo al artículo 97 al objeto de modificar el apartado 3, párrafo segundo, del presente artículo, añadiendo nuevas condiciones a las establecidas en dicho apartado, o modificando estas, cuando existan pruebas concretas y fiables de la existencia de sistemas de IA que entren en el ámbito de aplicación del anexo III, pero que no planteen un riesgo importante de causar un perjuicio a la salud, la seguridad o los derechos fundamentales de las personas físicas.

7. La Comisión adoptará actos delegados con arreglo al artículo 97 al objeto de modificar el apartado 3, párrafo segundo, del presente artículo, suprimiendo cualquiera de las condiciones establecidas en él, cuando existan pruebas concretas y fiables de que es necesario para mantener el nivel de protección de la salud, la seguridad y los derechos fundamentales previsto en el presente Reglamento.

8. Ninguna modificación de las condiciones establecidas en el apartado 3, párrafo segundo, adoptada de conformidad con los apartados 6 y 7 del presente artículo, reducirá el nivel global de protección de la salud, la seguridad y los derechos fundamentales previsto en el presente Reglamento, y cualquier modificación garantizará la coherencia con los actos delegados adoptados con arreglo al artículo 7, apartado 1, y tendrá en cuenta la evolución tecnológica y del mercado.

ARTÍCULO 7
MODIFICACIONES DEL ANEXO III

1. La Comisión estará facultada para adoptar actos delegados con arreglo al artículo 97 al objeto de modificar el anexo III mediante la adición o modificación de casos de uso de

sistemas de IA de alto riesgo cuando se reúnan las dos condiciones siguientes:

a) que los sistemas de IA estén destinados a ser utilizados en cualquiera de los ámbitos que figuran en el anexo III, y

b) que los sistemas de IA planteen un riesgo de perjudicar la salud y la seguridad o de tener repercusiones negativas en los derechos fundamentales, y que dicho riesgo sea equivalente a, o mayor que, el riesgo de perjuicio o de repercusiones negativas que plantean los sistemas de IA de alto riesgo que ya se mencionan en el anexo III.

2. Cuando evalúe la condición prevista en el apartado 1, letra b), la Comisión tendrá en cuenta los criterios siguientes:

a) la finalidad prevista del sistema de IA;

b) la medida en que se haya utilizado o sea probable que se utilice un sistema de IA;

c) la naturaleza y la cantidad de los datos tratados y utilizados por el sistema de IA, en particular si se tratan categorías especiales de datos personales;

d) el grado de autonomía con el que actúa el sistema de IA y la posibilidad de que un ser humano anule una decisión o recomendaciones que puedan dar lugar a un perjuicio;

e) la medida en que la utilización de un sistema de IA ya haya causado un perjuicio a la salud y la seguridad, haya tenido repercusiones negativas en los derechos fundamentales o haya dado lugar a problemas importantes en relación con la probabilidad de dicho perjuicio o dichas repercusiones negativas, según demuestren, por ejemplo, los informes o las alegaciones documentadas que se presenten a las autoridades nacionales competentes o cualquier otro informe, según proceda;

f) el posible alcance de dicho perjuicio o dichas repercusiones negativas, en particular en lo que respecta a su intensidad y su capacidad para afectar a varias personas o afectar de manera desproporcionada a un determinado colectivo de personas;

g) la medida en que las personas que podrían sufrir dicho perjuicio o dichas repercusiones negativas dependan del resultado generado por un sistema de IA, en particular porque, por motivos prácticos o jurídicos, no sea razonablemente posible renunciar a dicho resultado;

h) la medida en que exista un desequilibrio de poder o las personas que podrían sufrir dicho perjuicio o dichas repercusiones negativas se encuentren en una posición de vulnerabilidad respecto del responsable del despliegue de un sistema de IA, en particular debido a su situación, autoridad, conocimientos, circunstancias económicas o sociales, o edad;

i) la medida en que sea fácil corregir o revertir el resultado generado utilizando un sistema de IA, teniendo en cuenta las soluciones técnicas disponibles para corregirlo o revertirlo y sin que deba considerarse que los resultados que afectan negativamente a la salud, la seguridad o los derechos fundamentales son fáciles de corregir o revertir;

j) la probabilidad de que el despliegue del sistema de IA resulte beneficioso para las personas, los colectivos o la sociedad en general, y la magnitud de este beneficio, incluidas posibles mejoras en la seguridad de los productos;

k) la medida en que el Derecho de la Unión vigente establezca:

i) vías de recurso efectivas en relación con los riesgos que plantea un sistema de IA, con exclusión de las acciones por daños y perjuicios,

ii) medidas efectivas para prevenir o reducir notablemente esos riesgos.

3. La Comisión estará facultada para adoptar actos delegados con arreglo al artículo 97 al objeto de modificar la lista del anexo III mediante la supresión de sistemas de IA de alto riesgo cuando se reúnan las dos condiciones siguientes:

a) que los sistemas de IA de alto riesgo de que se trate ya no planteen riesgos considerables para los derechos fundamentales, la salud o la seguridad, teniendo en cuenta los criterios enumerados en el apartado 2;

b) que la supresión no reduzca el nivel general de protección de la salud, la seguridad y los derechos fundamentales con arreglo al Derecho de la Unión.

SECCIÓN 2
REQUISITOS DE LOS SISTEMAS DE IA DE ALTO RIESGO

ARTÍCULO 8
CUMPLIMIENTO DE LOS REQUISITOS

1. Los sistemas de IA de alto riesgo cumplirán los requisitos establecidos en la presente sección, teniendo en cuenta sus finalidades previstas, así como el estado actual de la técnica generalmente reconocido en materia de IA y tecnologías relacionadas con la IA. A la hora de garantizar el cumplimiento de dichos requisitos se tendrá en cuenta el sistema de gestión de riesgos a que se refiere el artículo 9.

2. Cuando un producto contenga un sistema de IA al que se apliquen los requisitos del presente Reglamento, así como los requisitos de los actos legislativos de armonización de la Unión enumerados en el anexo I, sección A, los proveedores serán responsables de garantizar que su producto cumpla plenamente todos los requisitos aplicables en virtud de los actos legislativos de armonización de la Unión que sean aplicables. Para garantizar el cumplimiento de los sistemas de IA de alto riesgo a que se refiere el apartado 1 de los requisitos establecidos en la presente sección, y con el fin de garantizar la coherencia, evitar duplicidades y reducir al mínimo las cargas adicionales, los proveedores podrán optar por integrar, según proceda, los procesos de prueba y presentación de información necesarios, y la información y la documentación que faciliten con respecto a su producto en documentación y procedimientos que ya existan y exijan los actos legislativos de armonización de la Unión enumerados en el anexo I, sección A.

ARTÍCULO 9
SISTEMA DE GESTIÓN DE RIESGOS

1. Se establecerá, implantará, documentará y mantendrá un sistema de gestión de riesgos en relación con los sistemas de IA de alto riesgo.

2. El sistema de gestión de riesgos se entenderá como un proceso iterativo continuo planificado y ejecutado durante todo el ciclo de vida de un sistema de IA de alto riesgo, que requerirá revisiones y actualizaciones sistemáticas periódicas. Constará de las siguientes etapas:

a) la determinación y el análisis de los riesgos conocidos y previsibles que el sistema de IA de alto riesgo pueda plantear para la salud, la seguridad o los derechos fundamentales cuando el sistema de IA de alto riesgo se utilice de conformidad con su finalidad prevista;

b) la estimación y la evaluación de los riesgos que podrían surgir cuando el sistema de IA de alto riesgo se utilice de conformidad con su finalidad prevista y cuando se le dé un uso indebido razonablemente previsible;

c) la evaluación de otros riesgos que podrían surgir, a partir del análisis de los datos recogidos con el sistema de vigilancia poscomercialización a que se refiere el artículo 72;

d) la adopción de medidas adecuadas y específicas de gestión de riesgos diseñadas para hacer frente a los riesgos detectados con arreglo a la letra a).

3. Los riesgos a que se refiere el presente artículo son únicamente aquellos que pueden mitigarse o eliminarse razonablemente mediante el desarrollo o el diseño del sistema de IA de alto riesgo o el suministro de información técnica adecuada.

4. Las medidas de gestión de riesgos mencionadas en el apartado 2, letra d), tendrán debidamente en cuenta los efectos y la posible interacción derivados de la aplicación combinada de los requisitos establecidos en la presente sección, con vistas a reducir al mínimo los riesgos de manera más eficaz al tiempo que se logra un equilibrio adecuado en la aplicación de las medidas para cumplir dichos requisitos.

5. Las medidas de gestión de riesgos mencionadas en el apartado 2, letra d), considerarán aceptables los riesgos residuales pertinentes asociados a cada peligro, así como el riesgo residual general de los sistemas de IA de alto riesgo.

A la hora de determinar las medidas de gestión de riesgos más adecuadas, se procurará:

a) eliminar o reducir los riesgos detectados y evaluados de conformidad con el apartado 2 en la medida en que sea técnicamente viable mediante un diseño y un desarrollo adecuados del sistema de IA de alto riesgo;

b) implantar, cuando proceda, unas medidas de mitigación y control apropiadas que hagan frente a los riesgos que no puedan eliminarse;

c) proporcionar la información requerida conforme al artículo 13 y, cuando proceda, impartir formación a los responsables del despliegue.

Con vistas a eliminar o reducir los riesgos asociados a la utilización del sistema de IA de alto riesgo, se tendrán debidamente en cuenta los conocimientos técnicos, la experiencia, la educación y la formación que se espera que posea el responsable del despliegue, así como el contexto en el que está previsto que se utilice el sistema.

6. Los sistemas de IA de alto riesgo serán sometidos a pruebas destinadas a determinar cuáles son las medidas de gestión de riesgos más adecuadas y específicas. Dichas pruebas comprobarán que los sistemas de IA de alto riesgo funcionan de manera coherente con su finalidad prevista y cumplen los requisitos establecidos en la presente sección.

7. Los procedimientos de prueba podrán incluir pruebas en condiciones reales de conformidad con el artículo 60.

8. Las pruebas de los sistemas de IA de alto riesgo se realizarán, según proceda, en cualquier momento del proceso de desarrollo y, en todo caso, antes de su introducción en el mercado o puesta en servicio. Las pruebas se realizarán utilizando parámetros y umbrales de probabilidades previamente definidos que sean adecuados para la finalidad prevista del sistema de IA de alto riesgo.

9. Cuando se implante el sistema de gestión de riesgos previsto en los apartados 1 a 7, los proveedores prestarán atención a si, en vista de su finalidad prevista, es probable que el sistema de IA de alto riesgo afecte negativamente a las personas menores de dieciocho años y, en su caso, a otros colectivos vulnerables.

10. En el caso de los proveedores de sistemas de IA de alto riesgo que estén sujetos a requisitos relativos a procesos internos de gestión de riesgos con arreglo a otras disposiciones pertinentes del Derecho de la Unión, los aspectos previstos en los apartados 1 a 9 podrán formar parte de los procedimientos de gestión de riesgos establecidos con arreglo a dicho Derecho, o combinarse con ellos.

ARTÍCULO 10
DATOS Y GOBERNANZA DE DATOS

1. Los sistemas de IA de alto riesgo que utilizan técnicas que implican el entrenamiento de modelos de IA con datos se desarrollarán a partir de conjuntos de datos de entrenamiento, validación y prueba que cumplan los criterios de calidad a que se refieren los apartados 2, 3 y 4 del presente artículo y el artículo 4 bis, apartado 1, siempre que se utilicen dichos conjuntos de datos.

2. Los conjuntos de datos de entrenamiento, validación y prueba se someterán a prácticas de gobernanza y gestión de datos adecuadas para la finalidad prevista del sistema de IA de alto riesgo. Dichas prácticas se centrarán, en particular, en lo siguiente:

a) las decisiones pertinentes relativas al diseño;

b) los procesos de recogida de datos y el origen de los datos y, en el caso de los datos personales, la finalidad original de la recogida de datos;

c) las operaciones de tratamiento oportunas para la preparación de los datos, como la anotación, el etiquetado, la depuración, la actualización, el enriquecimiento y la agregación;

d) la formulación de supuestos, en particular en lo que respecta a la información que se supone que miden y representan los datos;

e) una evaluación de la disponibilidad, la cantidad y la adecuación de los conjuntos de datos necesarios;

f) el examen atendiendo a posibles sesgos que puedan afectar a la salud y la seguridad de las personas, afectar negativamente a los derechos fundamentales o dar lugar a algún tipo de discriminación prohibida por el Derecho de la Unión, especialmente cuando las salidas de datos influyan en las informaciones de entrada de futuras operaciones;

g) medidas adecuadas para detectar, prevenir y mitigar posibles sesgos detectados con arreglo a la letra f);

h) la detección de lagunas o deficiencias pertinentes en los datos que impidan el cumplimiento del presente Reglamento, y la forma de subsanarlas.

3. Los conjuntos de datos de entrenamiento, validación y prueba serán pertinentes, suficientemente representativos y, en la mayor medida posible, carecerán de errores y

estarán completos en vista de su finalidad prevista. Asimismo, tendrán las propiedades estadísticas adecuadas, por ejemplo, cuando proceda, en lo que respecta a las personas o los colectivos de personas en relación con los cuales está previsto que se utilice el sistema de IA de alto riesgo. Los conjuntos de datos podrán reunir esas características para cada conjunto de datos individualmente o para una combinación de estos.

4. Los conjuntos de datos tendrán en cuenta, en la medida necesaria para la finalidad prevista, las características o elementos particulares del entorno geográfico, contextual, conductual o funcional específico en el que está previsto que se utilice el sistema de IA de alto riesgo.

6. Para el desarrollo de sistemas de IA de alto riesgo que no emplean técnicas que implican el entrenamiento de modelos de IA, los apartados 2, 3 y 4 del presente artículo y el artículo 4 bis, apartado 1, se aplicarán únicamente a los conjuntos de datos de prueba.

ARTÍCULO 11
DOCUMENTACIÓN TÉCNICA

1. La documentación técnica de un sistema de IA de alto riesgo se elaborará antes de su introducción en el mercado o puesta en servicio, y se mantendrá actualizada.

Dicha documentación técnica se redactará de modo que demuestre que el sistema de IA de alto riesgo cumple los requisitos establecidos en la presente sección y que proporcione de manera clara y completa a las autoridades nacionales competentes y a los organismos notificados la información necesaria para evaluar la conformidad del sistema de IA con dichos requisitos. Contendrá, como mínimo, los elementos contemplados en el anexo IV. Las pymes —incluidas las empresas emergentes— y las pequeñas empresas de mediana capitalización podrán presentar los elementos de la documentación técnica especificada en el anexo IV de manera simplificada. A tal fin, la Comisión establecerá un formulario simplificado de documentación técnica orientado a las necesidades de las pymes —incluidas las empresas emergentes— y las pequeñas empresas de mediana capitalización. Cuando una pyme —incluidas las empresas emergentes— o una pequeña empresa de mediana capitalización opte por presentar la información exigida en el anexo IV de manera simplificada, utilizará el formulario a que se refiere el presente apartado. Los organismos notificados aceptarán dicho formulario a efectos de la evaluación de la conformidad.

2. Cuando se introduzca en el mercado o se ponga en servicio un sistema de IA de alto riesgo asociado a un producto que entre en el ámbito de aplicación de los actos legislativos de armonización de la Unión mencionados en el anexo I, sección A, se elaborará un único conjunto de documentos técnicos que contenga toda la información mencionada en el apartado 1, así como la información que exijan dichos actos legislativos.

3. La Comisión estará facultada para adoptar actos delegados con arreglo al artículo 97 al objeto de modificar el anexo IV, cuando sea necesario, para garantizar que, en vista de los avances técnicos, la documentación técnica proporcione toda la información necesaria para evaluar si el sistema cumple los requisitos establecidos en la presente sección.

ARTÍCULO 12
CONSERVACIÓN DE REGISTROS

1. Los sistemas de IA de alto riesgo permitirán técnicamente el registro automático de acontecimientos (en lo sucesivo, «archivos de registro») a lo largo de todo el ciclo de vida del sistema.

2. Para garantizar un nivel de trazabilidad del funcionamiento del sistema de IA de alto riesgo que resulte adecuado para la finalidad prevista del sistema, las capacidades de registro permitirán que se registren acontecimientos pertinentes para:

a) la detección de situaciones que puedan dar lugar a que el sistema de IA de alto riesgo presente un riesgo en el sentido del artículo 79, apartado 1, o a una modificación sustancial;

b) la facilitación de la vigilancia poscomercialización a que se refiere el artículo 72, y

c) la vigilancia del funcionamiento de los sistemas de IA de alto riesgo a que se refiere el artículo 26, apartado 5.

3. En el caso de los sistemas de IA de alto riesgo mencionados en el anexo III, punto 1, letra a), las capacidades de registro incluirán, como mínimo:

a) un registro del período de cada uso del sistema (la fecha y la hora de inicio y la fecha y la hora de finalización de cada uso);

b) la base de datos de referencia con la que el sistema ha cotejado los datos de entrada;

c) los datos de entrada con los que la búsqueda ha arrojado una correspondencia;

d) la identificación de las personas físicas implicadas en la verificación de los resultados que se mencionan en el artículo 14, apartado 5.

ARTÍCULO 13
TRANSPARENCIA Y COMUNICACIÓN DE INFORMACIÓN A LOS RESPONSABLES DEL DESPLIEGUE

1. Los sistemas de IA de alto riesgo se diseñarán y desarrollarán de un modo que se garantice que funcionan con un nivel de transparencia suficiente para que los responsables del despliegue interpreten y usen correctamente sus resultados de salida. Se garantizará un tipo y un nivel de transparencia adecuados para que el proveedor y el responsable del despliegue cumplan las obligaciones pertinentes previstas en la sección 3.

2. Los sistemas de IA de alto riesgo irán acompañados de las instrucciones de uso correspondientes en un formato digital o de otro tipo adecuado, las cuales incluirán información concisa, completa, correcta y clara que sea pertinente, accesible y comprensible para los responsables del despliegue.

3. Las instrucciones de uso contendrán al menos la siguiente información:

a) la identidad y los datos de contacto del proveedor y, en su caso, de su representante autorizado;

b) las características, capacidades y limitaciones del funcionamiento del sistema de IA de alto riesgo, con inclusión de:

i) su finalidad prevista,

ii) el nivel de precisión (incluidos los parámetros para medirla), solidez y ciberseguridad mencionado en el artículo 15 con respecto al cual se haya probado y validado el sistema de IA de alto riesgo y que puede esperarse, así como cualquier circunstancia conocida y previsible que pueda afectar al nivel de precisión, solidez y ciberseguridad esperado,

iii) cualquier circunstancia conocida o previsible, asociada a la utilización del sistema de IA de alto riesgo conforme a su finalidad prevista o a un uso indebido razonablemente previsible, que pueda dar lugar a riesgos para la salud y la seguridad o los derechos fundamentales a que se refiere el artículo 9, apartado 2,

iv) en su caso, las capacidades y características técnicas del sistema de IA de alto riesgo para proporcionar información pertinente para explicar sus resultados de salida,

v) cuando proceda, su funcionamiento con respecto a determinadas personas o determinados colectivos de personas en relación con los que esté previsto utilizar el sistema,

vi) cuando proceda, especificaciones relativas a los datos de entrada, o cualquier otra información pertinente en relación con los conjuntos de datos de entrenamiento, validación y prueba usados, teniendo en cuenta la finalidad prevista del sistema de IA de alto riesgo,

vii) en su caso, información que permita a los responsables del despliegue interpretar los resultados de salida del sistema de IA de alto riesgo y utilizarla adecuadamente;

c) los cambios en el sistema de IA de alto riesgo y su funcionamiento predeterminados por el proveedor en el momento de efectuar la evaluación de la conformidad inicial, en su caso;

d) las medidas de supervisión humana a que se hace referencia en el artículo 14, incluidas las medidas técnicas establecidas para facilitar la interpretación de los resultados de salida de los sistemas de IA de alto riesgo por parte de los responsables del despliegue;

e) los recursos informáticos y de hardware necesarios, la vida útil prevista del sistema de IA de alto riesgo y las medidas de mantenimiento y cuidado necesarias (incluida su frecuencia) para garantizar el correcto funcionamiento de dicho sistema, también en lo que respecta a las actualizaciones del software;

f) cuando proceda, una descripción de los mecanismos incluidos en el sistema de IA de alto riesgo que permita a los responsables del despliegue recabar, almacenar e interpretar correctamente los archivos de registro de conformidad con el artículo 12.

ARTÍCULO 14
SUPERVISIÓN HUMANA

1. Los sistemas de IA de alto riesgo se diseñarán y desarrollarán de modo que puedan ser vigilados de manera efectiva por personas físicas durante el período que estén en uso, lo que incluye dotarlos de herramientas de interfaz humano-máquina adecuadas.

2. El objetivo de la supervisión humana será prevenir o reducir al mínimo los riesgos para la salud, la seguridad o los derechos fundamentales que pueden surgir cuando se utiliza un sistema de IA de alto riesgo conforme a su finalidad prevista o cuando se le da un uso indebido razonablemente previsible, en particular cuando dichos riesgos persistan a pesar de la aplicación de otros requisitos establecidos en la presente sección.

3. Las medidas de supervisión serán proporcionales a los riesgos, al nivel de autonomía y al contexto de uso del sistema de IA de alto riesgo, y se garantizarán bien mediante uno de los siguientes tipos de medidas, bien mediante ambos:

a) las medidas que el proveedor defina y que integre, cuando sea técnicamente viable, en el sistema de IA de alto riesgo antes de su introducción en el mercado o su puesta en servicio;

b) las medidas que el proveedor defina antes de la introducción del sistema de IA de alto riesgo en el mercado o de su puesta en servicio y que sean adecuadas para que las ponga en práctica el responsable del despliegue.

4. A efectos de la puesta en práctica de lo dispuesto en los apartados 1, 2 y 3, el sistema de IA de alto riesgo se ofrecerá al responsable del despliegue de tal modo que las personas físicas a quienes se encomiende la supervisión humana puedan, según proceda y de manera proporcionada a:

a) entender adecuadamente las capacidades y limitaciones pertinentes del sistema de IA de alto riesgo y poder vigilar debidamente su funcionamiento, por ejemplo, con vistas a detectar y resolver anomalías, problemas de funcionamiento y comportamientos inesperados;

b) ser conscientes de la posible tendencia a confiar automáticamente o en exceso en los resultados de salida generados por un sistema de IA de alto riesgo («sesgo de automatización»), en particular con aquellos sistemas que se utilizan para aportar información o recomendaciones con el fin de que personas físicas adopten una decisión;

c) interpretar correctamente los resultados de salida del sistema de IA de alto riesgo, teniendo en cuenta, por ejemplo, los métodos y herramientas de interpretación disponibles;

d) decidir, en cualquier situación concreta, no utilizar el sistema de IA de alto riesgo o descartar, invalidar o revertir los resultados de salida que este genere;

e) intervenir en el funcionamiento del sistema de IA de alto riesgo o interrumpir el sistema pulsando un botón de parada o mediante un procedimiento similar que permita que el sistema se detenga de forma segura.

5. En el caso de los sistemas de IA de alto riesgo mencionados en el anexo III, punto 1, letra a), las medidas a que se refiere el apartado 3 del presente artículo garantizarán, además, que el responsable del despliegue no actúe ni tome ninguna decisión basándose en la identificación generada por el sistema, salvo si al menos dos personas físicas con la competencia, formación y autoridad necesarias han verificado y confirmado por separado dicha identificación.

El requisito de la verificación por parte de al menos dos personas físicas por separado no se aplicará a los sistemas de IA de alto riesgo utilizados con fines de garantía del cumplimiento del Derecho, de migración, de control fronterizo o de asilo cuando el Derecho nacional o de la Unión considere que la aplicación de este requisito es desproporcionada.

ARTÍCULO 15
PRECISIÓN, SOLIDEZ Y CIBERSEGURIDAD

1. Los sistemas de IA de alto riesgo se diseñarán y desarrollarán de modo que alcancen un nivel adecuado de precisión, solidez y ciberseguridad y funcionen de manera uniforme en esos sentidos durante todo su ciclo de vida.
2. Para abordar los aspectos técnicos sobre la forma de medir los niveles adecuados de precisión y solidez establecidos en el apartado 1 y cualquier otro parámetro de rendimiento pertinente, la Comisión, en cooperación con las partes interesadas y organizaciones pertinentes, como las autoridades de metrología y de evaluación comparativa, fomentará, según proceda, el desarrollo de parámetros de referencia y metodologías de medición.
3. En las instrucciones de uso que acompañen a los sistemas de IA de alto riesgo se indicarán los niveles de precisión de dichos sistemas, así como los parámetros pertinentes para medirla.
4. Los sistemas de IA de alto riesgo serán lo más resistentes posible en lo que respecta a los errores, fallos o incoherencias que pueden surgir en los propios sistemas o en el entorno en el que funcionan, en particular a causa de su interacción con personas físicas u otros sistemas. Se adoptarán medidas técnicas y organizativas a este respecto.

La solidez de los sistemas de IA de alto riesgo puede lograrse mediante soluciones de redundancia técnica, tales como copias de seguridad o planes de prevención contra fallos.

Los sistemas de IA de alto riesgo que continúan aprendiendo tras su introducción en el mercado o puesta en servicio se desarrollarán de tal modo que se elimine o reduzca lo máximo posible el riesgo de que los resultados de salida que pueden estar sesgados influyan en la información de entrada de futuras operaciones (bucles de retroalimentación) y se garantice que dichos bucles se subsanen debidamente con las medidas de reducción de riesgos adecuadas.

5. Los sistemas de IA de alto riesgo serán resistentes a los intentos de terceros no autorizados de alterar su uso, sus resultados de salida o su funcionamiento aprovechando las vulnerabilidades del sistema.

Las soluciones técnicas encaminadas a garantizar la ciberseguridad de los sistemas de IA de alto riesgo serán adecuadas a las circunstancias y los riesgos pertinentes.

Entre las soluciones técnicas destinadas a subsanar vulnerabilidades específicas de la IA figurarán, según corresponda, medidas para prevenir, detectar, combatir, resolver y controlar los ataques que traten de manipular el conjunto de datos de entrenamiento («envenenamiento de datos»), o los componentes entrenados previamente utilizados en el entrenamiento («envenenamiento de modelos»), la información de entrada diseñada para hacer que el modelo de IA cometa un error («ejemplos adversarios» o «evasión de modelos»), los ataques a la confidencialidad o los defectos en el modelo.

SECCIÓN 3
OBLIGACIONES DE LOS PROVEEDORES Y RESPONSABLES DEL DESPLIEGUE DE SISTEMAS DE IA DE ALTO RIESGO Y DE OTRAS PARTES

ARTÍCULO 16
OBLIGACIONES DE LOS PROVEEDORES DE SISTEMAS DE IA DE ALTO RIESGO

Los proveedores de sistemas de IA de alto riesgo:

a) velarán por que sus sistemas de IA de alto riesgo cumplan los requisitos definidos en la sección 2;

b) indicarán en el sistema de IA de alto riesgo o, cuando no sea posible, en el embalaje del sistema o en la documentación que lo acompañe, según proceda, su nombre, su nombre comercial registrado o marca registrada y su dirección de contacto;

c) contarán con un sistema de gestión de la calidad que cumpla lo dispuesto en el artículo 17;

d) conservarán la documentación a que se refiere el artículo 18;

e) cuando estén bajo su control, conservarán los archivos de registro generados automáticamente por sus sistemas de IA de alto riesgo a que se refiere el artículo 19;

f) se asegurarán de que los sistemas de IA de alto riesgo sean sometidos al procedimiento pertinente de evaluación de la conformidad a que se refiere el artículo 43 antes de su introducción en el mercado o puesta en servicio;

g) elaborarán una declaración UE de conformidad en virtud de lo dispuesto en el artículo 47;

h) colocará el marcado CE en el sistema de IA de alto riesgo o, cuando no sea posible, en su embalaje o en la documentación que lo acompañe, para indicar la conformidad con el presente Reglamento, de acuerdo con lo dispuesto en el artículo 48;

i) cumplirán las obligaciones de registro a que se refiere el artículo 49, apartado 1;

j) adoptarán las medidas correctoras necesarias y facilitarán la información exigida en el artículo 20;

k) demostrarán, previa solicitud motivada de la autoridad nacional competente, la conformidad del sistema de IA de alto riesgo con los requisitos establecidos en la sección 2;

l) velarán por que el sistema de IA de alto riesgo cumpla requisitos de accesibilidad de conformidad con las Directivas (UE) 2016/2102 y (UE) 2019/882.

ARTÍCULO 17
SISTEMA DE GESTIÓN DE LA CALIDAD

1. Los proveedores de sistemas de IA de alto riesgo establecerán un sistema de gestión de la calidad que garantice el cumplimiento del presente Reglamento. Dicho sistema deberá consignarse de manera sistemática y ordenada en documentación en la que se recojan las políticas, los procedimientos y las instrucciones e incluirá, al menos, los siguientes aspectos:

a) una estrategia para el cumplimiento de la normativa, incluido el cumplimiento de los procedimientos de evaluación de la conformidad y de los procedimientos de gestión de las modificaciones de los sistemas de IA de alto riesgo;

b) las técnicas, los procedimientos y las actuaciones sistemáticas que se utilizarán en el diseño y el control y la verificación del diseño del sistema de IA de alto riesgo;

c) las técnicas, los procedimientos y las actuaciones sistemáticas que se utilizarán en el desarrollo del sistema de IA de alto riesgo y en el control y el aseguramiento de la calidad de este;

d) los procedimientos de examen, prueba y validación que se llevarán a cabo antes, durante y después del desarrollo del sistema de IA de alto riesgo, así como la frecuencia con que se ejecutarán;

e) las especificaciones técnicas, incluidas las normas, que se aplicarán y, cuando las normas armonizadas pertinentes no se apliquen en su totalidad o no cubran todos los requisitos pertinentes establecidos en la sección 2, los medios que se utilizarán para velar por que el sistema de IA de alto riesgo cumpla dichos requisitos;

f) los sistemas y procedimientos de gestión de datos, lo que incluye su adquisición, recopilación, análisis, etiquetado, almacenamiento, filtrado, prospección, agregación, conservación y cualquier otra operación relacionada con los datos que se lleve a cabo antes de la introducción en el mercado o puesta en servicio de sistemas de IA de alto riesgo y con esa finalidad;

g) el sistema de gestión de riesgos que se menciona en el artículo 9;

h) el establecimiento, aplicación y mantenimiento de un sistema de vigilancia poscomercialización de conformidad con el artículo 72;

i) los procedimientos asociados a la notificación de un incidente grave con arreglo al artículo 73;

j) la gestión de la comunicación con las autoridades nacionales competentes, otras autoridades pertinentes, incluidas las que permiten acceder a datos o facilitan el acceso a ellos, los organismos notificados, otros operadores, los clientes u otras partes interesadas;

k) los sistemas y procedimientos para llevar un registro de toda la documentación e información pertinente;

l) la gestión de los recursos, incluidas medidas relacionadas con la seguridad del suministro;

m) un marco de rendición de cuentas que defina las responsabilidades del personal directivo y de otra índole en relación con todos los aspectos enumerados en este apartado.

2. La aplicación de los aspectos mencionados en el apartado 1 será proporcional al tamaño de la organización del proveedor, en particular si el proveedor es una pyme, incluidas las empresas emergentes o las pequeñas empresas de mediana capitalización. Los proveedores respetarán, en todo caso, el grado de rigor y el nivel de protección requerido para garantizar la conformidad de sus sistemas de IA de alto riesgo con el presente Reglamento.

3. Los proveedores de sistemas de IA de alto riesgo que estén sujetos a obligaciones relativas a los sistemas de gestión de la calidad o una función equivalente con arreglo al Derecho sectorial pertinente de la Unión podrán incluir los aspectos enumerados en el apartado 1 como parte de los sistemas de gestión de la calidad con arreglo a dicho Derecho.

4. En el caso de los proveedores que sean entidades financieras sujetas a requisitos relativos a su gobernanza, sus sistemas o sus procesos internos en virtud del Derecho de la Unión en materia de servicios financieros, se considerará que se ha cumplido la obligación de establecer un sistema de gestión de la calidad, salvo en relación con lo dispuesto en el apartado 1, letras g), h) e i), del presente artículo cuando se respeten las normas sobre los sistemas o procesos de gobernanza interna de acuerdo con el Derecho pertinente de la Unión en materia de servicios financieros. A tal fin, se tendrán en cuenta todas las normas armonizadas que se mencionan en el artículo 40.

ARTÍCULO 18
CONSERVACIÓN DE LA DOCUMENTACIÓN

1. Durante un período de diez años a contar desde la introducción en el mercado o la puesta en servicio del sistema de IA de alto riesgo, el proveedor mantendrá a disposición de las autoridades nacionales competentes:

a) la documentación técnica a que se refiere el artículo 11;

b) la documentación relativa al sistema de gestión de la calidad a que se refiere el artículo 17;

c) la documentación relativa a los cambios aprobados por los organismos notificados, si procede;

d) las decisiones y otros documentos expedidos por los organismos notificados, si procede;

e) la declaración UE de conformidad contemplada en el artículo 47.

2. Cada Estado miembro determinará las condiciones en las que la documentación a que se refiere el apartado 1 permanecerá a disposición de las autoridades nacionales competentes durante el período indicado en dicho apartado en los casos en que un proveedor o su representante autorizado establecido en su territorio quiebre o cese en su actividad antes del final de dicho período.

3. Los proveedores que sean entidades financieras sujetas a requisitos relativos a su gobernanza, sus sistemas o sus procesos internos en virtud del Derecho de la Unión en materia de servicios financieros mantendrán la documentación técnica como parte de la documentación conservada en virtud del Derecho pertinente de la Unión en materia de servicios financieros.

ARTÍCULO 19
ARCHIVOS DE REGISTRO GENERADOS AUTOMÁTICAMENTE

1. Los proveedores de sistemas de IA de alto riesgo conservarán los archivos de registro a que se refiere el artículo 12, apartado 1, que los sistemas de IA de alto riesgo generen automáticamente en la medida en que dichos archivos estén bajo su control. Sin perjuicio del Derecho aplicable de la Unión o nacional, los archivos de registro se conservarán durante un período de tiempo adecuado para la finalidad prevista del sistema de IA de alto riesgo, de al menos seis meses, salvo que el Derecho de la Unión o nacional aplicable, en particular el Derecho de la Unión en materia de protección de datos personales, disponga otra cosa.

2. Los proveedores que sean entidades financieras sujetas a requisitos relativos a su gobernanza, sus sistemas o sus procesos internos en virtud del Derecho de la Unión en materia de servicios financieros mantendrán los archivos de registro generados automáticamente por sus sistemas de IA de alto riesgo como parte de la documentación

conservada en virtud del Derecho pertinente en materia de servicios financieros.

ARTÍCULO 20
MEDIDAS CORRECTORAS Y OBLIGACIÓN DE INFORMACIÓN

1. Los proveedores de sistemas de IA de alto riesgo que consideren o tengan motivos para considerar que un sistema de IA de alto riesgo que han introducido en el mercado o puesto en servicio no es conforme con el presente Reglamento adoptarán inmediatamente las medidas correctoras necesarias para que sea conforme, para retirarlo del mercado, desactivarlo o recuperarlo, según proceda. Informarán de ello a los distribuidores del sistema de IA de alto riesgo de que se trate y, en su caso, a los responsables del despliegue, al representante autorizado y a los importadores.
2. Cuando un sistema de IA de alto riesgo presente un riesgo en el sentido del artículo 79, apartado 1, y el proveedor tenga conocimiento de dicho riesgo, este investigará inmediatamente las causas, en colaboración con el responsable del despliegue que lo haya notificado, en su caso, e informará a las autoridades de vigilancia del mercado competentes respecto al sistema de IA de alto riesgo de que se trate y, cuando proceda, al organismo notificado que haya expedido un certificado para dicho sistema de conformidad con lo dispuesto en el artículo 44, en particular sobre la naturaleza del incumplimiento y sobre cualquier medida correctora adoptada.

ARTÍCULO 21
COOPERACIÓN CON LAS AUTORIDADES COMPETENTES

1. Los proveedores de sistemas de IA de alto riesgo, previa solicitud motivada de una autoridad competente, proporcionarán a dicha autoridad toda la información y la documentación necesarias para demostrar la conformidad del sistema de IA de alto riesgo con los requisitos establecidos en la sección 2, en una lengua que la autoridad pueda entender fácilmente y que sea una de las lenguas oficiales de las instituciones de la Unión, indicada por el Estado miembro de que se trate.
2. Previa solicitud motivada de una autoridad competente, los proveedores darán también a dicha autoridad, cuando proceda, acceso a los archivos de registro generados automáticamente del sistema de IA de alto riesgo a que se refiere el artículo 12, apartado 1, en la medida en que dichos archivos estén bajo su control.
3. Toda información obtenida por una autoridad competente con arreglo al presente artículo se tratará de conformidad con las obligaciones de confidencialidad establecidas en el artículo 78.

ARTÍCULO 22
REPRESENTANTES AUTORIZADOS DE LOS PROVEEDORES DE SISTEMAS DE IA DE ALTO RIESGO

1. Antes de comercializar sus sistemas de IA de alto riesgo en el mercado de la Unión, los proveedores establecidos en terceros países tendrán que nombrar, mediante un mandato escrito, a un representante autorizado que esté establecido en la Unión.
2. Los proveedores permitirán que su representante autorizado pueda efectuar las tareas especificadas en el mandato recibido del proveedor.
3. Los representantes autorizados efectuarán las tareas especificadas en el mandato recibido del proveedor. Facilitarán a las autoridades de vigilancia del mercado, cuando lo soliciten, una copia del mandato en una de las lenguas oficiales de las instituciones de la Unión según lo indicado por la autoridad de competente. A los efectos del presente Reglamento, el mandato habilitará al representante autorizado para realizar las tareas siguientes:
   a) verificar que se han elaborado la declaración UE de conformidad a que se refiere el artículo 47 y la documentación técnica a que se refiere el artículo 11 y que el proveedor ha llevado a cabo un procedimiento de evaluación de la conformidad adecuado;
   b) conservar a disposición de las autoridades competentes y de las autoridades u organismos nacionales a que se refiere el artículo 74, apartado 10, durante un período de diez años a contar desde la introducción en el mercado o la puesta en servicio del sistema de IA de alto riesgo, los datos de contacto del proveedor que haya nombrado al representante autorizado, una copia de la declaración UE de conformidad a que se refiere el artículo 47, la documentación técnica y, en su caso, el certificado expedido por el organismo notificado;
   c) proporcionar a una autoridad competente, previa solicitud motivada, toda la información y la documentación, incluida la mencionada en el presente párrafo, letra b), que sean necesarias para demostrar la conformidad de un sistema de IA de alto riesgo con los requisitos establecidos en la sección 2, incluido el acceso a los archivos de registro a que se refiere el artículo 12, apartado 1, generados automáticamente por ese sistema, en la medida en que dichos archivos estén bajo el control del proveedor;
   d) cooperar con las autoridades competentes, previa solicitud motivada, en todas las acciones que estas emprendan en relación con el sistema de IA de alto riesgo, en particular para reducir y mitigar los riesgos que este presente;
   e) cuando proceda, cumplir las obligaciones de registro a que se refiere el artículo 49, apartado 1, o si el registro lo lleva a cabo el propio proveedor, garantizar que la información a que se refiere el anexo VIII, sección A, punto 3, es correcta.

   El mandato habilitará al representante autorizado para que las autoridades competentes se pongan en contacto con él, además de con el proveedor o en lugar de con el proveedor, con referencia a todas las cuestiones relacionadas con la garantía del cumplimiento del presente Reglamento.
4. El representante autorizado pondrá fin al mandato si considera o tiene motivos para considerar que el proveedor contraviene las obligaciones que le atañen con arreglo al presente Reglamento. En tal caso, además, informará de inmediato de la terminación del mandato y de los motivos de esta medida a la autoridad de vigilancia del mercado pertinente, así como, cuando proceda, al organismo notificado pertinente.

ARTÍCULO 23
OBLIGACIONES DE LOS IMPORTADORES

1. Antes de introducir un sistema de IA de alto riesgo en el mercado, los importadores se asegurarán de que el sistema sea conforme con el presente Reglamento verificando que:
   a) el proveedor del sistema de IA de alto riesgo haya llevado a cabo el procedimiento de evaluación de la conformidad pertinente a que se refiere el artículo 43;
   b) el proveedor haya elaborado la documentación técnica de conformidad con el artículo 11 y el anexo IV;
   c) el sistema lleve el marcado CE exigido y vaya acompañado de la declaración UE de conformidad a que se refiere el artículo 47 y de las instrucciones de uso;
   d) el proveedor haya designado a un representante autorizado de conformidad con el artículo 22, apartado 1.
2. Si el importador tiene motivos suficientes para considerar que un sistema de IA de alto riesgo no es conforme con el presente Reglamento, ha sido falsificado o va acompañado de documentación falsificada, no lo introducirá en el mercado hasta que se haya conseguido la conformidad de dicho sistema. Si el sistema de IA de alto riesgo presenta un riesgo en el sentido del artículo 79, apartado 1, el importador informará de ello al proveedor del sistema, a los representantes autorizados y a las autoridades de vigilancia del mercado.
3. Los importadores indicarán, en el embalaje del sistema de IA de alto riesgo o en la documentación que lo acompañe, cuando proceda, su nombre, su nombre comercial registrado o marca registrada y su dirección de contacto.
4. Mientras sean responsables de un sistema de IA de alto riesgo, los importadores se asegurarán de que las condiciones de almacenamiento o transporte, cuando proceda, no comprometan el cumplimiento de los requisitos establecidos en la sección 2 por parte de dicho sistema.
5. Los importadores conservarán, durante un período de diez años a contar desde la introducción en el mercado o la puesta en servicio del sistema de IA de alto riesgo, una copia del certificado expedido por el organismo notificado, en su caso, de las instrucciones de uso y de la declaración UE de conformidad a que se refiere el artículo 47.
6. Los importadores proporcionarán a las autoridades competentes pertinentes, previa solicitud motivada, toda la información y la documentación, incluidas las referidas en el apartado 5, que sean necesarias para demostrar la conformidad de un sistema de IA de alto riesgo con los requisitos establecidos en la sección 2 en una lengua que estas puedan entender fácilmente. A tal efecto, velarán asimismo por que la documentación técnica pueda ponerse a disposición de esas autoridades.
7. Los importadores cooperarán con las autoridades competentes pertinentes en cualquier medida que estas adopten en relación con un sistema de IA de alto riesgo introducido en el mercado por los importadores, en particular para reducir y mitigar los riesgos que este presente.

ARTÍCULO 24
OBLIGACIONES DE LOS DISTRIBUIDORES

1. Antes de comercializar un sistema de IA de alto riesgo, los distribuidores verificarán que este lleve el marcado CE exigido, que vaya acompañado de una copia de la declaración UE de conformidad a que se refiere el artículo 47 y de las instrucciones de uso, y que el proveedor y el importador de dicho sistema, según corresponda, hayan cumplido sus obligaciones establecidas en el artículo 16, letras b) y c), y el artículo 23, apartado 3, respectivamente.
2. Si un distribuidor considera o tiene motivos para considerar, con arreglo a la información en su poder, que un sistema de IA de alto riesgo no es conforme con los requisitos establecidos en la sección 2, no lo comercializará hasta que se haya conseguido esa conformidad. Además, si el sistema de IA de alto riesgo presenta un riesgo en el sentido del artículo 79, apartado 1, el distribuidor informará de ello al proveedor o importador del sistema, según corresponda.
3. Mientras sean responsables de un sistema de IA de alto riesgo, los distribuidores se asegurarán de que las condiciones de almacenamiento o transporte, cuando proceda, no comprometen el cumplimiento por parte del sistema de los requisitos establecidos en la sección 2.
4. Los distribuidores que consideren o tengan motivos para considerar, con arreglo a la información en su poder, que un sistema de IA de alto riesgo que han comercializado no es conforme con los requisitos establecidos en la sección 2 adoptarán las medidas correctoras necesarias para que sea conforme, para retirarlo del mercado o recuperarlo, o velarán por que el proveedor, el importador u otro operador pertinente, según proceda, adopte dichas medidas correctoras. Cuando un sistema de IA de alto riesgo presente un riesgo en el sentido del artículo 79, apartado 1, su distribuidor informará inmediatamente de ello al proveedor o al importador del sistema y a las autoridades competentes respecto al sistema de IA de alto riesgo de que se trate y dará detalles, en particular, sobre la no conformidad y las medidas correctoras adoptadas.
5. Previa solicitud motivada de una autoridad competente pertinente, los distribuidores de un sistema de IA de alto riesgo proporcionarán a esa autoridad toda la información y la documentación relativas a sus actuaciones con arreglo a los apartados 1 a 4 que sean necesarias para demostrar que dicho sistema cumple los requisitos establecidos en la sección 2.
6. Los distribuidores cooperarán con las autoridades competentes pertinentes en cualquier medida que estas adopten en relación con un sistema de IA de alto riesgo comercializado por los distribuidores, en particular para reducir o mitigar los riesgos que este presente.

ARTÍCULO 25
RESPONSABILIDADES A LO LARGO DE LA CADENA DE VALOR DE LA IA

1. Cualquier distribuidor, importador, responsable del despliegue o tercero será considerado proveedor de un sistema de IA de alto riesgo a los efectos del presente Reglamento y estará sujeto a las obligaciones del proveedor previstas en el artículo 16 en cualquiera de las siguientes circunstancias:
   a) cuando ponga su nombre o marca en un sistema de IA de alto riesgo previamente introducido en el mercado o puesto en servicio, sin perjuicio de los acuerdos contractuales que estipulen que las obligaciones se asignan de otro modo;
   b) cuando modifique sustancialmente un sistema de IA de alto riesgo que ya haya sido introducido en el mercado o

puesto en servicio de tal manera que siga siendo un sistema de IA de alto riesgo con arreglo al artículo 6;

c) cuando modifique la finalidad prevista de un sistema de IA, incluido un sistema de IA de uso general, que no haya sido considerado de alto riesgo y ya haya sido introducido en el mercado o puesto en servicio, de tal manera que el sistema de IA de que se trate se convierta en un sistema de IA de alto riesgo de conformidad con el artículo 6.

2. Cuando se den las circunstancias mencionadas en el apartado 1, el proveedor que inicialmente haya introducido en el mercado el sistema de IA o lo haya puesto en servicio dejará de ser considerado proveedor de ese sistema de IA específico a efectos del presente Reglamento.

Ese proveedor inicial cooperará estrechamente con los nuevos proveedores, pondrá a disposición la información necesaria y proporcionará el acceso técnico y otra asistencia que pueda esperarse razonablemente para el cumplimiento de las obligaciones establecidas en el presente Reglamento, en particular en lo que respecta al cumplimiento de la evaluación de la conformidad de los sistemas de IA de alto riesgo.

En particular, la obligación establecida en el párrafo segundo incluirá, cuando sea pertinente para los fines en él especificados, las obligaciones de:

a) poner a disposición documentación técnica suficiente para evaluar el cumplimiento de los requisitos establecidos en el artículo 16;

b) informar a los nuevos proveedores sobre las limitaciones y los modos de fallo conocidos, y

c) proporcionar a los nuevos proveedores un acceso técnico específico, incluido para la prueba y la validación.

El presente apartado no se aplicará en los casos en que el proveedor inicial haya indicado claramente que su sistema de IA no debe ser transformado en un sistema de IA de alto riesgo y, por lo tanto, no está sujeto a la obligación de cooperar con los nuevos proveedores y entregarles la documentación.

3. En el caso de los sistemas de IA de alto riesgo que sean componentes de seguridad de productos contemplados en los actos legislativos de armonización de la Unión enumerados en el anexo I, sección A, el fabricante del producto será considerado proveedor del sistema de IA de alto riesgo y estará sujeto a las obligaciones previstas en el artículo 16 en alguna de las siguientes circunstancias:

a) que el sistema de IA de alto riesgo se introduzca en el mercado junto con el producto bajo el nombre o la marca del fabricante del producto;

b) que el sistema de IA de alto riesgo se ponga en servicio bajo el nombre o la marca del fabricante del producto después de que el producto haya sido introducido en el mercado.

4. El proveedor de un sistema de IA de alto riesgo y el tercero que suministre un sistema de IA, un modelo de IA, herramientas, servicios, componentes o procesos que se utilicen o integren en un sistema de IA de alto riesgo especificarán, mediante acuerdo escrito, la información, las capacidades, el acceso técnico y otra asistencia que sean necesarios, sobre la base del estado de la técnica generalmente reconocido, para que el proveedor del sistema de IA de alto riesgo pueda cumplir plenamente las obligaciones establecidas en el presente Reglamento. El presente apartado no se aplicará a los terceros que pongan a disposición del público herramientas, servicios, procesos o componentes que no sean modelos de IA de uso general en el marco de una licencia libre y de código abierto.

La Oficina de IA podrá elaborar y recomendar cláusulas contractuales tipo, de carácter voluntario, entre los proveedores de sistemas de IA de alto riesgo y terceros que suministren herramientas, servicios, componentes o procesos que se utilicen o integren en los sistemas de IA de alto riesgo. Cuando elabore esas cláusulas contractuales tipo de carácter voluntario, la Oficina de IA tendrá en cuenta los posibles requisitos contractuales aplicables en determinados sectores o modelos de negocio. Las cláusulas contractuales tipo de carácter voluntario se publicarán y estarán disponibles gratuitamente en un formato electrónico fácilmente utilizable.

5. Los apartados 2 y 3 se entenderán sin perjuicio de la necesidad de observar y proteger los derechos de propiedad intelectual e industrial, la información empresarial confidencial y los secretos comerciales, de conformidad con el Derecho de la Unión y nacional.

ARTÍCULO 26
OBLIGACIONES DE LOS RESPONSABLES DEL DESPLIEGUE DE SISTEMAS DE IA DE ALTO RIESGO

1. Los responsables del despliegue de sistemas de IA de alto riesgo adoptarán medidas técnicas y organizativas adecuadas para garantizar que utilizan dichos sistemas con arreglo a las instrucciones de uso que los acompañen, de acuerdo con los apartados 3 y 6.

2. Los responsables del despliegue encomendarán la supervisión humana a personas físicas que tengan la competencia, la formación y la autoridad necesarias.

3. Las obligaciones previstas en los apartados 1 y 2 no afectan a otras obligaciones que el Derecho nacional o de la Unión imponga a los responsables del despliegue ni a su libertad para organizar sus propios recursos y actividades con el fin de poner en práctica las medidas de supervisión humana que indique el proveedor.

4. Sin perjuicio de lo dispuesto en los apartados 1 y 2, el responsable del despliegue se asegurará de que los datos de entrada sean pertinentes y suficientemente representativos en vista de la finalidad prevista del sistema de IA de alto riesgo, en la medida en que ejerza el control sobre dichos datos.

5. Los responsables del despliegue vigilarán el funcionamiento del sistema de IA de alto riesgo basándose en las instrucciones de uso y, cuando proceda, informarán a los proveedores con arreglo al artículo 72. Cuando los responsables del despliegue tengan motivos para considerar que utilizar el sistema de IA de alto riesgo conforme a sus instrucciones puede dar lugar a que ese sistema de AI presente un riesgo en el sentido del artículo 79, apartado 1, informarán, sin demora indebida, al proveedor o distribuidor y a la autoridad de vigilancia del mercado pertinente y suspenderán el uso de ese sistema. Cuando los responsables del despliegue detecten un incidente grave, informarán asimismo inmediatamente de dicho incidente, en primer lugar, al proveedor y, a continuación, al importador o distribuidor y a la autoridad de vigilancia del mercado pertinente. En el caso de que el responsable del despliegue no consiga contactar con el proveedor, el artículo 73 se aplicará mutatis mutandis. Esta obligación no comprenderá los datos operativos sensibles

de los responsables del despliegue de sistemas de IA que sean autoridades garantes del cumplimiento del Derecho.

En el caso de los responsables del despliegue que sean entidades financieras sujetas a requisitos relativos a su gobernanza, sus sistemas o sus procesos internos en virtud del Derecho de la Unión en materia de servicios financieros, se considerará que se ha cumplido la obligación de vigilancia prevista en el párrafo primero cuando se respeten las normas sobre sistemas, procesos y mecanismos de gobernanza interna de acuerdo con el Derecho pertinente en materia de servicios financieros.

6. Los responsables del despliegue de sistemas de IA de alto riesgo conservarán los archivos de registro que los sistemas de IA de alto riesgo generen automáticamente en la medida en que dichos archivos estén bajo su control, durante un período de tiempo adecuado para la finalidad prevista del sistema de IA de alto riesgo, de al menos seis meses, salvo que se disponga otra cosa en el Derecho de la Unión o nacional aplicable, en particular en el Derecho de la Unión en materia de protección de datos personales.

Los responsables del despliegue que sean entidades financieras sujetas a requisitos relativos a su gobernanza, sus sistemas o sus procesos internos en virtud del Derecho de la Unión en materia de servicios financieros mantendrán los archivos de registro como parte de la documentación conservada en virtud del Derecho de la Unión en materia de servicios financieros.

7. Antes de poner en servicio o utilizar un sistema de IA de alto riesgo en el lugar de trabajo, los responsables del despliegue que sean empleadores informarán a los representantes de los trabajadores y a los trabajadores afectados de que estarán expuestos a la utilización del sistema de IA de alto riesgo. Esta información se facilitará, cuando proceda, con arreglo a las normas y procedimientos establecidos en el Derecho de la Unión y nacional y conforme a las prácticas en materia de información a los trabajadores y sus representantes.

8. Los responsables del despliegue de sistemas de IA de alto riesgo que sean autoridades públicas o instituciones, órganos y organismos de la Unión cumplirán las obligaciones de registro a que se refiere el artículo 49. Cuando dichos responsables del despliegue constaten que el sistema de IA de alto riesgo que tienen previsto utilizar no ha sido registrado en la base de datos de la UE a que se refiere el artículo 71, no utilizarán dicho sistema e informarán al proveedor o al distribuidor.

9. Cuando proceda, los responsables del despliegue de sistemas de IA de alto riesgo utilizarán la información facilitada conforme al artículo 13 del presente Reglamento para cumplir la obligación de llevar a cabo una evaluación de impacto relativa a la protección de datos que les imponen el artículo 35 del Reglamento (UE) 2016/679 o el artículo 27 de la Directiva (UE) 2016/680.

10. No obstante lo dispuesto en la Directiva (UE) 2016/680, en el marco de una investigación cuya finalidad sea la búsqueda selectiva de una persona sospechosa de haber cometido un delito o condenada por ello, el responsable del despliegue de un sistema de IA de alto riego de identificación biométrica remota en diferido solicitará, ex ante o sin demora indebida y a más tardar en un plazo de cuarenta y ocho horas, a una autoridad judicial o administrativa cuyas decisiones sean vinculantes y estén sujetas a revisión judicial, una autorización para utilizar ese sistema, salvo cuando se utilice para la identificación inicial de un posible sospechoso sobre la base de hechos objetivos y verificables vinculados directamente al delito. Cada utilización deberá limitarse a lo que resulte estrictamente necesario para investigar un delito concreto.

En caso de que se deniegue la autorización contemplada en el párrafo primero, dejará de utilizarse el sistema de identificación biométrica remota en diferido objeto de la solicitud de autorización con efecto inmediato y se eliminarán los datos personales asociados al uso del sistema de IA de alto riesgo para el que se solicitó la autorización.

Dicho sistema de IA de alto riego de identificación biométrica remota en diferido no se utilizará en ningún caso a los efectos de la garantía del cumplimiento del Derecho de forma indiscriminada, sin que exista relación alguna con un delito, un proceso penal, una amenaza real y actual o real y previsible de delito, o con la búsqueda de una persona desaparecida concreta. Se velará por que las autoridades garantes del cumplimiento del Derecho no puedan adoptar ninguna decisión que produzca efectos jurídicos adversos para una persona exclusivamente sobre la base de los resultados de salida de dichos sistemas de identificación biométrica remota en diferido.

El presente apartado se entiende sin perjuicio del artículo 9 del Reglamento (UE) 2016/679 y del artículo 10 de la Directiva (UE) 2016/680 para el tratamiento de los datos biométricos.

Con independencia de la finalidad o del responsable del despliegue, se documentará toda utilización de tales sistemas de IA de alto riesgo en el expediente policial pertinente y se pondrá a disposición, previa solicitud, de la autoridad de vigilancia del mercado pertinente y de la autoridad nacional de protección de datos, quedando excluida la divulgación de datos operativos sensibles relacionados con la garantía del cumplimiento del Derecho. El presente párrafo se entenderá sin perjuicio de los poderes conferidas por la Directiva (UE) 2016/680 a las autoridades de control.

Los responsables del despliegue presentarán informes anuales a la autoridad de vigilancia del mercado pertinente y a la autoridad nacional de protección de datos sobre el uso que han hecho de los sistemas de identificación biométrica remota en diferido, quedando excluida la divulgación de datos operativos sensibles relacionados con la garantía del cumplimiento del Derecho. Los informes podrán agregarse de modo que cubran más de un despliegue.

Los Estados miembros podrán adoptar, de conformidad con el Derecho de la Unión, leyes más restrictivas sobre el uso de sistemas de identificación biométrica remota en diferido.

11. Sin perjuicio de lo dispuesto en el artículo 50 del presente Reglamento, los responsables del despliegue de los sistemas de IA de alto riesgo a que se refiere el anexo III que tomen decisiones o ayuden a tomar decisiones relacionadas con personas físicas informarán a las personas físicas de que están expuestas a la utilización de los sistemas de IA de alto riesgo. En el caso de los sistemas de IA de alto riesgo que se utilicen a los efectos de la garantía del cumplimiento del Derecho, se aplicará el artículo 13 de la Directiva (UE) 2016/680.

12. Los responsables del despliegue cooperarán con las autoridades competentes pertinentes en cualquier medida que estas adopten en relación con el sistema de IA de alto riesgo con el objetivo de aplicar el presente Reglamento.

ARTÍCULO 27
EVALUACIÓN DE IMPACTO RELATIVA A LOS DERECHOS FUNDAMENTALES PARA LOS SISTEMAS DE IA DE ALTO RIESGO

1. Antes de desplegar uno de los sistemas de IA de alto riesgo a que se refiere el artículo 6, apartado 2, con excepción de los sistemas de IA de alto riesgo destinados a ser utilizados en el ámbito enumerado en el anexo III, punto 2, los responsables del despliegue que sean organismos de Derecho público, o entidades privadas que prestan servicios públicos, y los responsable del despliegue de sistemas de IA de alto riesgo a que se refiere el anexo III, punto 5, letras b) y c), llevarán a cabo una evaluación del impacto que la utilización de dichos sistemas puede tener en los derechos fundamentales. A tal fin, los responsables del despliegue llevarán a cabo una evaluación que consistirá en:
   a) una descripción de los procesos del responsable del despliegue en los que se utilizará el sistema de IA de alto riesgo en consonancia con su finalidad prevista;
   b) una descripción del período de tiempo durante el cual se prevé utilizar cada sistema de IA de alto riesgo y la frecuencia con la que está previsto utilizarlo;
   c) las categorías de personas físicas y colectivos que puedan verse afectados por su utilización en el contexto específico;
   d) los riesgos de perjuicio específicos que puedan afectar a las categorías de personas físicas y colectivos determinadas con arreglo a la letra c) del presente apartado, teniendo en cuenta la información facilitada por el proveedor con arreglo al artículo 13;
   e) una descripción de la aplicación de medidas de supervisión humana, de acuerdo con las instrucciones de uso;
   f) las medidas que deben adoptarse en caso de que dichos riesgos se materialicen, incluidos los acuerdos de gobernanza interna y los mecanismos de reclamación.
2. La obligación descrita con arreglo al apartado 1 se aplicará al primer uso del sistema de IA de alto riesgo. En casos similares, el responsable del despliegue podrá basarse en evaluaciones de impacto relativas a los derechos fundamentales realizadas previamente o a evaluaciones de impacto existentes realizadas por los proveedores. Si, durante el uso del sistema de IA de alto riesgo, el responsable del despliegue considera que alguno de los elementos enumerados en el apartado 1 ha cambiado o ha dejado de estar actualizado, adoptará las medidas necesarias para actualizar la información.
3. Una vez realizada la evaluación a que se refiere el apartado 1 del presente artículo, el responsable del despliegue notificará sus resultados a la autoridad de vigilancia del mercado, presentando el modelo cumplimentado a que se refiere el apartado 5 del presente artículo. En el caso contemplado en el artículo 46, apartado 1, los responsables del despliegue podrán quedar exentos de esta obligación de notificación.
4. Si ya se cumplen cualesquiera de las obligaciones establecidas en el presente artículo mediante la evaluación de impacto relativa a la protección de datos realizada en virtud del artículo 35 del Reglamento (UE) 2016/679 o del artículo 27 de la Directiva (UE) 2016/680, el responsable del despliegue podrá, al llevar a cabo la evaluación de impacto relativa a los derechos fundamentales a que se refiere el apartado 1 del presente artículo, incluir referencias cruzadas a las secciones pertinentes de dicha evaluación de impacto relativa a la protección de datos o incluir las partes pertinentes de esta en la evaluación de impacto relativa a los derechos fundamentales.
5. La Oficina de IA elaborará un modelo de cuestionario, incluido mediante una herramienta automatizada, a fin de facilitar que los responsables del despliegue cumplan sus obligaciones en virtud del presente artículo de manera simplificada. Este modelo ofrecerá a los responsables del despliegue, cuando proceda, la posibilidad de incluir referencias cruzadas a las secciones pertinentes de la evaluación de impacto relativa a la protección de datos o de incluir las partes pertinentes de esta en la evaluación de impacto relativa a los derechos fundamentales, en virtud del apartado 4.

SECCIÓN 4
AUTORIDADES NOTIFICANTES Y ORGANISMOS NOTIFICADOS

ARTÍCULO 28
AUTORIDADES NOTIFICANTES

1. Cada Estado miembro nombrará o constituirá al menos una autoridad notificante que será responsable de establecer y llevar a cabo los procedimientos necesarios para la evaluación, designación y notificación de los organismos de evaluación de la conformidad, así como de su supervisión. Dichos procedimientos se desarrollarán por medio de la cooperación entre las autoridades notificantes de todos los Estados miembros.
2. Los Estados miembros podrán decidir que la evaluación y la supervisión contempladas en el apartado 1 sean realizadas por un organismo nacional de acreditación en el sentido del Reglamento (CE) n. o 765/2008 y con arreglo a este.
3. Las autoridades notificantes se constituirán, se organizarán y funcionarán de forma que no surjan conflictos de intereses con los organismos de evaluación de la conformidad y que se garantice la imparcialidad y objetividad de sus actividades.
4. Las autoridades notificantes se organizarán de forma que las decisiones relativas a la notificación de los organismos de evaluación de la conformidad sean adoptadas por personas competentes distintas de las que llevaron a cabo la evaluación de dichos organismos.
5. Las autoridades notificantes no ofrecerán ni ejercerán ninguna actividad que efectúen los organismos de evaluación de la conformidad, ni ningún servicio de consultoría de carácter comercial o competitivo.
6. Las autoridades notificantes preservarán la confidencialidad de la información obtenida, de conformidad con lo dispuesto en el artículo 78.
7. Las autoridades notificantes dispondrán de suficiente personal competente para efectuar adecuadamente sus tareas. Cuando proceda, el personal competente tendrá los conocimientos especializados necesarios para ejercer sus funciones, en ámbitos como las tecnologías de la información, la IA y el Derecho, incluida la supervisión de los derechos fundamentales.
8. Las autoridades notificantes designadas en virtud del presente Reglamento que sean responsables de los sistemas de IA regulados por los actos legislativos de armonización

de la Unión enumerados en el anexo I, sección A, garantizarán que el organismo de evaluación de la conformidad que solicite la designación tanto en virtud del presente Reglamento como de los actos legislativos de armonización de la Unión enumerados en el anexo I, sección A, pueda presentar una solicitud única y someterse a un procedimiento de evaluación unificado para ser designado en virtud del presente Reglamento y de los actos legislativos de armonización de la Unión enumerados en el anexo I, sección A, cuando la legislación de armonización pertinente de la Unión disponga dicha solicitud única y dicho procedimiento de evaluación unificado. A tal fin, las autoridades notificantes designadas en virtud del presente Reglamento y las designadas en virtud de los actos legislativos de armonización de la Unión enumerados en el anexo I, sección A, cooperarán en sus evaluaciones.

La solicitud única y el procedimiento de evaluación unificado a que se refiere el presente apartado también se pondrán a disposición de los organismos notificados ya designados en virtud de los actos legislativos de armonización de la Unión enumerados en el anexo I, sección A, cuando dichos organismos notificados soliciten su designación en virtud del presente Reglamento, siempre que la legislación de armonización de la Unión pertinente disponga dicho procedimiento.

Un organismo de evaluación de la conformidad designado en virtud de más de uno de los actos de la legislación de armonización de la Unión enumerado en el anexo I, sección A, solo tendrá que presentar una única solicitud para ser designado en virtud del presente Reglamento. La designación en virtud del presente Reglamento será aplicable a todos los actos legislativos de armonización de la Unión enumerados en el anexo I, sección A, para los cuales se designe al organismo de evaluación de la conformidad.

La solicitud única y el procedimiento de evaluación unificado evitarán duplicidades innecesarias, se basarán en los procedimientos existentes de designación con arreglo a los actos legislativos de armonización de la Unión enumerados en el anexo I, sección A, y garantizarán el cumplimiento de los requisitos relativos a los organismos notificados con arreglo tanto al presente Reglamento como a los actos legislativos de armonización de la Unión pertinentes.

9. Una autoridad notificante que haya sido designada en virtud de los actos legislativos de armonización de la Unión enumerados en el anexo I, sección A, es también la autoridad notificante a efectos de la solicitud única y del procedimiento de evaluación unificado a que se refiere el apartado 8, a menos que el Estado miembro designe otra autoridad notificante a efectos del presente Reglamento.

ARTÍCULO 29
SOLICITUD DE NOTIFICACIÓN POR PARTE DE UN ORGANISMO DE EVALUACIÓN DE LA CONFORMIDAD

1. Los organismos de evaluación de la conformidad presentarán una solicitud de notificación ante la autoridad notificante del Estado miembro en el que estén establecidos.
2. La solicitud de notificación irá acompañada de una descripción de las actividades de evaluación de la conformidad, del módulo o módulos de evaluación de la conformidad y los tipos de sistemas de IA en relación con los cuales el organismo de evaluación de la conformidad se considere competente, así como de un certificado de acreditación, si lo hay, expedido por un organismo nacional de acreditación, que declare que el organismo de evaluación de la conformidad cumple los requisitos establecidos en el artículo 31.

Se añadirá cualquier documento válido relacionado con las designaciones existentes del organismo notificado solicitante en virtud de cualquier otro acto de la legislación de armonización de la Unión.

3. Si el organismo de evaluación de la conformidad de que se trate no puede facilitar un certificado de acreditación, entregará a la autoridad notificante todas las pruebas documentales necesarias para verificar, reconocer y supervisar periódicamente que cumple los requisitos establecidos en el artículo 31.
4. En lo que respecta a los organismos notificados designados en virtud de cualquier otro acto legislativo de armonización de la Unión, todos los documentos y certificados vinculados a dichas designaciones podrán utilizarse para apoyar y acelerar su procedimiento de designación en virtud del presente Reglamento, según proceda.

Los organismos notificados que sean designados en virtud de cualquiera de los actos legislativos de armonización de la Unión enumerados en el anexo I, sección A, y se sometan a un procedimiento de evaluación unificado a que se refiere el artículo 28, apartado 8, presentarán la solicitud única de evaluación a la autoridad notificante designada en virtud de dichos actos legislativos de armonización de la Unión.

El organismo notificado actualizará la documentación a que se refieren los apartados 2 y 3 del presente artículo cuando se produzcan cambios pertinentes, para que la autoridad responsable de los organismos notificados pueda supervisar y comprobar que se siguen cumpliendo todos los requisitos establecidos en el artículo 31.

ARTÍCULO 30
PROCEDIMIENTO DE NOTIFICACIÓN

1. Las autoridades notificantes solo podrán notificar organismos de evaluación de la conformidad que hayan cumplido los requisitos establecidos en el artículo 31.
2. Las autoridades notificantes notificarán a la Comisión y a los demás Estados miembros, sobre la base de la lista de códigos, categorías y tipos correspondientes de sistemas de IA que figura en el anexo XIV y mediante el sistema de notificación electrónica desarrollado y gestionado por la Comisión, cada organismo de evaluación de la conformidad a que se refiere el apartado 1.

La Comisión estará facultada para adoptar actos delegados con arreglo al artículo 97 por los que se modifique el anexo XIV, a la luz del progreso técnico, de los avances del conocimiento o de nuevos datos científicos, mediante la adición de un nuevo código, categoría o tipo de sistema de IA a la lista de códigos, categorías y tipos correspondientes de sistemas de IA, mediante la retirada de dicha lista de un código, categoría o tipo de sistema de IA que figure en ella o mediante el traslado de un código o tipo de sistema de IA de una categoría a otra.

3. La notificación a que se refiere el apartado 2 del presente artículo incluirá información detallada de las actividades de evaluación de la conformidad, el módulo o módulos de evaluación de la conformidad y los tipos de sistemas de IA afectados, así como la certificación de competencia pertinente. Si la notificación no está basada en el

certificado de acreditación a que se refiere el artículo 29, apartado 2, la autoridad notificante facilitará a la Comisión y a los demás Estados miembros las pruebas documentales que demuestren la competencia del organismo de evaluación de la conformidad y las disposiciones existentes destinadas a garantizar que se supervisará periódicamente al organismo y que este continuará satisfaciendo los requisitos establecidos en el artículo 31.

4. El organismo de evaluación de la conformidad de que se trate únicamente podrá realizar las actividades de un organismo notificado si la Comisión o los demás Estados miembros no formulan ninguna objeción en el plazo de dos semanas tras la notificación de una autoridad notificante cuando esta incluya el certificado de acreditación a que se refiere el artículo 29, apartado 2, o de dos meses tras la notificación de la autoridad notificante cuando esta incluya las pruebas documentales a que se refiere el artículo 29, apartado 3.
5. Cuando se formulen objeciones, la Comisión iniciará sin demora consultas con los Estados miembros pertinentes y el organismo de evaluación de la conformidad. En vista de todo ello, la Comisión enviará su decisión al Estado miembro afectado y al organismo de evaluación de la conformidad pertinente.

ARTÍCULO 31
REQUISITOS RELATIVOS A LOS ORGANISMOS NOTIFICADOS

1. Los organismos notificados se establecerán de conformidad con el Derecho nacional de los Estados miembros y tendrán personalidad jurídica.
2. Los organismos notificados satisfarán los requisitos organizativos, de gestión de la calidad, recursos y procesos, necesarios para el desempeño de sus funciones, así como los requisitos adecuados en materia de ciberseguridad.
3. La estructura organizativa, la distribución de las responsabilidades, la línea jerárquica y el funcionamiento de los organismos notificados ofrecerán confianza en su desempeño y en los resultados de las actividades de evaluación de la conformidad que realicen los organismos notificados.
4. Los organismos notificados serán independientes del proveedor de un sistema de IA de alto riesgo en relación con el cual lleven a cabo actividades de evaluación de la conformidad. Los organismos notificados serán independientes de cualquier otro operador con un interés económico en los sistemas de IA de alto riesgo que se evalúen, así como de cualquier competidor del proveedor. Ello no será óbice para el uso de sistemas de IA de alto riesgo evaluados que sean necesarios para las actividades del organismo de evaluación de la conformidad o para el uso de tales sistemas de alto riesgo con fines personales.
5. Los organismos de evaluación de la conformidad, sus máximos directivos y el personal responsable de la realización de las tareas de evaluación de la conformidad no intervendrán directamente en el diseño, el desarrollo, la comercialización o el uso de dichos sistemas de IA de alto riesgo, ni tampoco representarán a las partes que llevan a cabo estas actividades. Además, no efectuarán ninguna actividad que pudiera entrar en conflicto con su independencia de criterio o su integridad en relación con las actividades de evaluación de la conformidad para las que han sido notificados. Ello se aplicará especialmente a los servicios de consultoría.
6. Los organismos notificados estarán organizados y gestionados de modo que se garantice la independencia, objetividad e imparcialidad de sus actividades. Los organismos notificados documentarán e implantarán una estructura y procedimientos que garanticen la imparcialidad y permitan promover y poner en práctica los principios de imparcialidad aplicables en toda su organización, a todo su personal y en todas sus actividades de evaluación.
7. Los organismos notificados contarán con procedimientos documentados que garanticen que su personal, sus comités, sus filiales, sus subcontratistas y todos sus organismos asociados o personal de organismos externos mantengan, de conformidad con el artículo 78, la confidencialidad de la información que llegue a su poder en el desempeño de las actividades de evaluación de la conformidad, excepto en aquellos casos en que la ley exija su divulgación. El personal de los organismos notificados estará sujeto al secreto profesional en lo que respecta a toda la información obtenida en el ejercicio de las funciones que les hayan sido encomendadas en virtud del presente Reglamento, salvo en relación con las autoridades notificantes del Estado miembro en el que desarrollen sus actividades.
8. Los organismos notificados contarán con procedimientos para desempeñar sus actividades que tengan debidamente en cuenta el tamaño de los proveedores, el sector en que operan, su estructura y el grado de complejidad del sistema de IA de que se trate.
9. Los organismos notificados suscribirán un seguro de responsabilidad adecuado para sus actividades de evaluación de la conformidad, salvo que la responsabilidad la asuma el Estado miembro en que estén establecidos con arreglo al Derecho nacional o que el propio Estado miembro sea directamente responsable de la evaluación de la conformidad.
10. Los organismos notificados serán capaces de llevar a cabo todas sus tareas con arreglo al presente Reglamento con el máximo grado de integridad profesional y la competencia técnica necesaria en el ámbito específico, tanto si dichas tareas las efectúan los propios organismos notificados como si se realizan en su nombre y bajo su responsabilidad.
11. Los organismos notificados contarán con competencias técnicas internas suficientes para poder evaluar de manera eficaz las tareas que lleven a cabo agentes externos en su nombre. El organismo notificado dispondrá permanentemente de suficiente personal administrativo, técnico, jurídico y científico que tenga experiencia y conocimientos relativos a los tipos de sistemas de IA, los datos y la computación de datos pertinentes y a los requisitos establecidos en la sección 2.
12. Los organismos notificados participarán en las actividades de coordinación según lo previsto en el artículo 38. Asimismo, tomarán parte directamente o mediante representación en organizaciones europeas de normalización, o se asegurarán de mantenerse al corriente de la situación actualizada de las normas pertinentes.

ARTÍCULO 32
PRESUNCIÓN DE CONFORMIDAD CON LOS REQUISITOS RELATIVOS A LOS ORGANISMOS NOTIFICADOS

Cuando un organismo de evaluación de la conformidad demuestre que cumple los criterios establecidos en las normas armonizadas pertinentes, o en partes de estas, cuyas referencias estén publicadas en el Diario Oficial de la Unión Europea, se presumirá que cumple los requisitos establecidos en el artículo 31 en la medida en que las normas armonizadas aplicables contemplen esos mismos requisitos.

ARTÍCULO 33
FILIALES DE ORGANISMOS NOTIFICADOS Y SUBCONTRATACIÓN

1. Cuando un organismo notificado subcontrate tareas específicas relacionadas con la evaluación de la conformidad o recurra a una filial, se asegurará de que el subcontratista o la filial cumplan los requisitos establecidos en el artículo 31 e informará a la autoridad notificante en consecuencia.
2. Los organismos notificados asumirán la plena responsabilidad de las tareas realizadas por cualesquiera subcontratistas o filiales.
3. Las actividades solo podrán subcontratarse o delegarse en una filial previo consentimiento del proveedor. Los organismos notificados pondrán a disposición del público una lista de sus filiales.
4. Los documentos pertinentes sobre la evaluación de las cualificaciones del subcontratista o de la filial y el trabajo que estos realicen en virtud del presente Reglamento se mantendrán a disposición de la autoridad notificante durante un período de cinco años a partir de la fecha de finalización de la subcontratación.

ARTÍCULO 34
OBLIGACIONES OPERATIVAS DE LOS ORGANISMOS NOTIFICADOS

1. Los organismos notificados verificarán la conformidad de los sistemas de IA de alto riesgo siguiendo los procedimientos de evaluación de la conformidad establecidos en el artículo 43.
2. Los organismos notificados evitarán cargas innecesarias para los proveedores cuando desempeñen sus actividades, y tendrán debidamente en cuenta el tamaño del proveedor, el sector en que opera, su estructura y el grado de complejidad del sistema de IA de alto riesgo de que se trate, en particular con vistas a reducir al mínimo las cargas administrativas y los costes del cumplimiento para las microempresas y pequeñas empresas en el sentido de la Recomendación 2003/361/CE. El organismo notificado respetará, sin embargo, el grado de rigor y el nivel de protección requeridos para que el sistema de IA de alto riesgo cumpla los requisitos del presente Reglamento.
3. Los organismos notificados pondrán a disposición de la autoridad notificante mencionada en el artículo 28, y le presentarán cuando se les pida, toda la documentación pertinente, incluida la documentación de los proveedores, a fin de que dicha autoridad pueda llevar a cabo sus actividades de evaluación, designación, notificación y supervisión, y de facilitar la evaluación descrita en la presente sección.

ARTÍCULO 35
NÚMEROS DE IDENTIFICACIÓN Y LISTAS DE ORGANISMOS NOTIFICADOS

1. La Comisión asignará un número de identificación único a cada organismo notificado, incluso cuando un organismo sea notificado con arreglo a más de un acto de la Unión.
2. La Comisión hará pública la lista de organismos notificados con arreglo al presente Reglamento, incluidos sus números de identificación y las actividades para las que hayan sido notificados. La Comisión se asegurará de que la lista se mantenga actualizada.

ARTÍCULO 36
CAMBIOS EN LAS NOTIFICACIONES

1. La autoridad notificante notificará a la Comisión y a los demás Estados miembros cualquier cambio pertinente en la notificación de un organismo notificado a través del sistema de notificación electrónica a que se refiere el artículo 30, apartado 2.
2. Los procedimientos establecidos en los artículos 29 y 30 se aplicarán a las ampliaciones del ámbito de aplicación de la notificación.

Para modificaciones de la notificación distintas de las ampliaciones de su ámbito de aplicación, se aplicarán los procedimientos establecidos en los apartados 3 a 9.

3. Cuando un organismo notificado decida poner fin a sus actividades de evaluación de la conformidad, informará de ello a la autoridad notificante y a los proveedores afectados tan pronto como sea posible y, cuando se trate de un cese planeado, al menos un año antes de poner fin a sus actividades. Los certificados del organismo notificado podrán seguir siendo válidos durante un plazo de nueve meses después del cese de las actividades del organismo notificado, siempre que otro organismo notificado haya confirmado por escrito que asumirá la responsabilidad de los sistemas de IA de alto riesgo cubiertos por dichos certificados. Este último organismo notificado realizará una evaluación completa de los sistemas de IA de alto riesgo afectados antes del vencimiento de ese plazo de nueve meses y antes de expedir nuevos certificados para esos sistemas. Si el organismo notificado ha puesto fin a sus actividades, la autoridad notificante retirará la designación.
4. Si una autoridad notificante tiene motivo suficiente para considerar que un organismo notificado ya no cumple los requisitos establecidos en el artículo 31 o no está cumpliendo sus obligaciones, la autoridad notificante investigará el asunto sin demora y con la máxima diligencia. En ese contexto, informará al organismo notificado de que se trate acerca de las objeciones formuladas y le ofrecerá la posibilidad de exponer sus puntos de vista. Si la autoridad notificante llega a la conclusión de que el organismo notificado ya no cumple los requisitos establecidos en el artículo 31 o no está cumpliendo sus obligaciones, dicha autoridad limitará, suspenderá o retirará la designación, según el caso, dependiendo de la gravedad del incumplimiento de dichos requisitos u obligaciones. Asimismo, informará de ello inmediatamente a la Comisión y a los demás Estados miembros.
5. Cuando su designación haya sido suspendida, limitada o retirada total o parcialmente, el organismo notificado

informará a los proveedores afectados a más en un plazo de diez días.

6. En caso de la limitación, suspensión o retirada de una designación, la autoridad notificante adoptará las medidas oportunas para garantizar que los archivos del organismo notificado de que se trate se conserven, y para ponerlos a disposición de las autoridades notificantes de otros Estados miembros y de las autoridades de vigilancia del mercado, a petición de estas.
7. En caso de la limitación, suspensión o retirada de una designación, la autoridad notificante:
   a) evaluará las repercusiones en los certificados expedidos por el organismo notificado;
   b) presentará a la Comisión y a los demás Estados miembros un informe con sus conclusiones en un plazo de tres meses a partir de la notificación de los cambios en la designación;
   c) exigirá al organismo notificado que suspenda o retire, en un plazo razonable determinado por la autoridad, todo certificado indebidamente expedido, a fin de garantizar la conformidad continua de los sistemas de IA de alto riesgo en el mercado;
   d) informará a la Comisión y a los Estados miembros de los certificados cuya suspensión o retirada haya exigido;
   e) facilitará a las autoridades nacionales competentes del Estado miembro en el que el proveedor tenga su domicilio social toda la información pertinente sobre los certificados cuya suspensión o retirada haya exigido; dicha autoridad tomará las medidas oportunas, cuando sea necesario, para evitar un riesgo para la salud, la seguridad o los derechos fundamentales.
8. Salvo en el caso de los certificados expedidos indebidamente, y cuando una designación haya sido suspendida o limitada, los certificados mantendrán su validez en una de las circunstancias siguientes:
   a) cuando, en el plazo de un mes a partir de la suspensión o la limitación, la autoridad notificante haya confirmado que no existe riesgo alguno para la salud, la seguridad o los derechos fundamentales en relación con los certificados afectados por la suspensión o la limitación y haya fijado un calendario de acciones para subsanar la suspensión o la limitación, o
   b) cuando la autoridad notificante haya confirmado que no se expedirán, modificarán ni volverán a expedir certificados relacionados con la suspensión mientras dure la suspensión o limitación, y declare si el organismo notificado tiene o no la capacidad, durante el período de la suspensión o limitación, de seguir supervisando los certificados expedidos y siendo responsable de ellos; cuando la autoridad notificante determine que el organismo notificado no tiene la capacidad de respaldar los certificados expedidos, el proveedor del sistema cubierto por el certificado deberá confirmar por escrito a las autoridades nacionales competentes del Estado miembro en que tenga su domicilio social, en un plazo de tres meses a partir de la suspensión o limitación, que otro organismo notificado cualificado va a asumir temporalmente las funciones del organismo notificado para supervisar los certificados y ser responsable de ellos durante el período de la suspensión o limitación.
9. Salvo en el caso de los certificados expedidos indebidamente, y cuando se haya retirado una designación, los certificados mantendrán su validez durante nueve meses en las circunstancias siguientes:
   a) la autoridad nacional competente del Estado miembro en el que tiene su domicilio social el proveedor del sistema de IA de alto riesgo cubierto por el certificado ha confirmado que no existe ningún riesgo para la salud, la seguridad o los derechos fundamentales asociado al sistema de IA de alto riesgo de que se trate, y
   b) otro organismo notificado ha confirmado por escrito que asumirá la responsabilidad inmediata de dichos sistemas de IA y completa su evaluación en el plazo de doce meses a partir de la retirada de la designación.

En las circunstancias a que se refiere el párrafo primero, la autoridad nacional competente del Estado miembro en el que tenga su domicilio social el proveedor del sistema cubierto por el certificado podrá prorrogar la validez provisional de los certificados por plazos adicionales de tres meses, sin exceder de doce meses en total.

La autoridad nacional competente o el organismo notificado que asuman las funciones del organismo notificado afectado por el cambio de la designación informarán de ello inmediatamente a la Comisión, a los demás Estados miembros y a los demás organismos notificados.

ARTÍCULO 37
CUESTIONAMIENTO DE LA COMPETENCIA DE LOS ORGANISMOS NOTIFICADOS

1. La Comisión investigará, cuando sea necesario, todos los casos en los que existan razones para dudar de la competencia de un organismo notificado o del cumplimiento continuo, por parte de un organismo notificado, de los requisitos establecidos en el artículo 31 y de sus responsabilidades aplicables.
2. La autoridad notificante facilitará a la Comisión, a petición de esta, toda la información pertinente relativa a la notificación o el mantenimiento de la competencia del organismo notificado de que se trate.
3. La Comisión garantizará el tratamiento confidencial de acuerdo con el artículo 78 de toda la información delicada recabada en el transcurso de sus investigaciones en virtud del presente artículo.
4. Cuando la Comisión determine que un organismo notificado no cumple o ha dejado de cumplir los requisitos para su notificación, informará al Estado miembro notificante en consecuencia y le solicitará que adopte las medidas correctoras necesarias, incluidas la suspensión o la retirada de la designación en caso necesario. Si el Estado miembro no adopta las medidas correctoras necesarias, la Comisión, mediante un acto de ejecución, podrá suspender, limitar o retirar la designación. Dicho acto de ejecución se adoptará con arreglo al procedimiento de examen contemplado en el artículo 98, apartado 2.

ARTÍCULO 38
COORDINACIÓN DE LOS ORGANISMOS NOTIFICADOS

1. La Comisión se asegurará de que se instaure y se mantenga convenientemente, en relación con los sistemas de IA de alto riesgo, una adecuada coordinación y cooperación entre los organismos notificados activos en los procedimientos de evaluación de la conformidad en virtud del presente Reglamento, en forma de grupo sectorial de organismos notificados.

2. Cada autoridad notificante se asegurará de que los organismos notificados por ella participen en el trabajo del grupo a que se refiere el apartado 1, directamente o por medio de representantes designados.
3. La Comisión dispondrá que se organicen intercambios de conocimientos y mejores prácticas entre autoridades notificantes.

ARTÍCULO 39
ORGANISMOS DE EVALUACIÓN DE LA CONFORMIDAD DE TERCEROS PAÍSES

Los organismos de evaluación de la conformidad establecidos en virtud del Derecho de un tercer país con el que la Unión haya celebrado un acuerdo podrán ser autorizados a desempeñar las actividades de los organismos notificados con arreglo al presente Reglamento, siempre que cumplan los requisitos establecidos en el artículo 31 o garanticen un nivel equivalente de cumplimiento.

SECCIÓN 5
NORMAS, EVALUACIÓN DE LA CONFORMIDAD, CERTIFICADOS, REGISTRO

ARTÍCULO 40
NORMAS ARMONIZADAS Y DOCUMENTOS DE NORMALIZACIÓN

1. Los sistemas de IA de alto riesgo o los modelos de IA de uso general que sean conformes con normas armonizadas, o partes de estas, cuyas referencias estén publicadas en el Diario Oficial de la Unión Europea de conformidad con el Reglamento (UE) n. o 1025/2012 se presumirá que son conformes con los requisitos establecidos en la sección 2 del presente capítulo o, en su caso, con las obligaciones establecidas en el capítulo V, secciones 2 y 3, del presente Reglamento, en la medida en que dichas normas contemplen estos requisitos u obligaciones.
2. De conformidad con el artículo 10 del Reglamento (UE) n. o 1025/2012, la Comisión formulará, sin demora indebida, peticiones de normalización que contemplen todos los requisitos establecidos en la sección 2 del presente capítulo y, según proceda, las peticiones de normalización que contemplen las obligaciones establecidas en el capítulo V, secciones 2 y 3, del presente Reglamento. La petición de normalización también incluirá la solicitud de documentos sobre los procesos de presentación de información y documentación a fin de mejorar el funcionamiento de los de los sistemas de IA desde el punto de vista de los recursos, como la reducción del consumo de energía y de otros recursos del sistema de IA de alto riesgo durante su ciclo de vida, así como sobre el desarrollo eficiente desde el punto de vista energético de los modelos de IA de uso general. Cuando prepare una petición de normalización, la Comisión consultará al Consejo de IA y a las partes interesadas pertinentes, incluido el foro consultivo.

Cuando dirija una petición de normalización a las organizaciones europeas de normalización, la Comisión especificará que las normas deben ser claras, coherentes —también con las normas elaboradas en diversos sectores para los productos regulados por los actos legislativos de armonización de la Unión vigentes enumerados en el anexo I— y destinadas a garantizar que los sistemas de IA de alto riesgo o los modelos de IA de uso general introducidos en el mercado o puestos en servicio en la Unión cumplan los requisitos u obligaciones pertinentes establecidos en el presente Reglamento.

La Comisión solicitará a las organizaciones europeas de normalización que aporten pruebas de que han hecho todo lo posible por cumplir los objetivos a que se refieren los párrafos primero y segundo del presente apartado, de conformidad con el artículo 24 del Reglamento (UE) n. o 1025/2012.

La Comisión solicitará a las organizaciones europeas de normalización, de conformidad con el Reglamento (UE) n. o 1025/2012 del Parlamento Europeo y del Consejo (1) y sin demora indebida, que elaboren documentos de normalización —incluidas, en su caso, normas armonizadas— para facilitar el cumplimiento conjunto, y la correspondiente presunción de conformidad, de los requisitos u obligaciones establecidos en el capítulo III, secciones 2 y 3, del presente Reglamento y de los requisitos y obligaciones pertinentes establecidos en los actos legislativos de armonización de la Unión enumerados en el anexo I del presente Reglamento.

3. Los participantes en el proceso de normalización tratarán de promover la inversión y la innovación en IA, también incrementando la seguridad jurídica, así como la competitividad y el crecimiento del mercado de la Unión, de contribuir al refuerzo de la cooperación mundial en pro de la normalización, teniendo en cuenta las normas internacionales existentes en el ámbito de la IA que son coherentes con los valores, derechos fundamentales e intereses de la Unión, y de mejorar la gobernanza multilateral, garantizando una representación equilibrada de los intereses y la participación efectiva de todas las partes interesadas pertinentes de conformidad con los artículos 5, 6 y 7 del Reglamento (UE) n. o 1025/2012.

ARTÍCULO 41
ESPECIFICACIONES COMUNES

1. La Comisión podrá adoptar actos de ejecución por los que se establezcan especificaciones comunes para los requisitos establecidos en la sección 2 del presente capítulo o, según corresponda, para las obligaciones establecidas en el capítulo V, secciones 2 y 3, siempre que se hayan cumplido las siguientes condiciones:
   a) la Comisión ha solicitado, de conformidad con el artículo 10, apartado 1, del Reglamento (UE) n. o 1025/2012, a una o varias organizaciones europeas de normalización que elaboren una norma armonizada para los requisitos establecidos en la sección 2 del presente capítulo, o según corresponda, para las obligaciones establecidas en el capítulo V, secciones 2 y 3, y:
      i) la solicitud no ha sido aceptada por ninguna de las organizaciones europeas de normalización, o

(1) Reglamento (UE) n. o 1025/2012 del Parlamento Europeo y del Consejo, de 25 de octubre de 2012, sobre la normalización europea, por el que se modifican las Directivas 89/686/CEE y 93/15/CEE del Consejo y las Directivas 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE y 2009/105/CE del Parlamento Europeo y del Consejo y por el que se deroga la Decisión 87/95/CEE del Consejo y la Decisión n. o 1673/2006/CE del Parlamento Europeo y del Consejo (DO L 316 de 14.11.2012, p. 12, ELI: http://data.europa.eu/eli/reg/2012/1025/oj).

      ii) las normas armonizadas que responden a dicha solicitud no se han entregado en el plazo establecido

de conformidad con el artículo 10, apartado 1, del Reglamento (UE) n. o 1025/2012, o

iii) las normas armonizadas pertinentes responden de forma insuficiente a las preocupaciones en materia de derechos fundamentales, o

iv) las normas armonizadas no se ajustan a la solicitud, y

b) no se ha publicado en el Diario Oficial de la Unión Europea ninguna referencia a normas armonizadas que regulen los requisitos establecidos en la sección 2 del presente capítulo, o según proceda, las obligaciones a que se refiere el capítulo V, secciones 2 y 3, de conformidad con el Reglamento (UE) n. o 1025/2012 y no se prevé la publicación de tal referencia en un plazo razonable.

Al elaborar las disposiciones comunes, la Comisión consultará al foro consultivo a que se refiere el artículo 67.

Los actos de ejecución a que se refiere el párrafo primero del presente apartado se adoptarán de conformidad con el procedimiento de examen contemplado en el artículo 98, apartado 2.

2. Antes de elaborar un proyecto de acto de ejecución, la Comisión informará al comité a que se refiere el artículo 22 del Reglamento (UE) n. o 1025/2012 de que considera que se cumplen las condiciones establecidas en el apartado 1 del presente artículo.

3. Se presumirá que los sistemas de IA de alto riesgo o los modelos de IA de uso general que sean conformes con las especificaciones comunes a que se refiere el apartado 1, o partes de dichas especificaciones, son conformes con los requisitos establecidos en la sección 2 del presente capítulo o, según corresponda, para cumplir con las obligaciones a que se refiere el capítulo V, secciones 2 y 3, en la medida en que dichas especificaciones comunes contemplen esos requisitos o esas obligaciones.

4. Cuando una norma armonizada sea adoptada por una organización europea de normalización y propuesta a la Comisión con el fin de publicar su referencia en el Diario Oficial de la Unión Europea, la Comisión evaluará la norma armonizada de conformidad con el Reglamento (UE) n. o 1025/2012. Cuando la referencia a una norma armonizada se publique en el Diario Oficial de la Unión Europea, la Comisión derogará los actos de ejecución a que se refiere el apartado 1, o las partes de dichos actos que contemplen los mismos requisitos establecidos en la sección 2 del presente capítulo o, según corresponda, las mismas obligaciones establecidas en el capítulo V, secciones 2 y 3.

5. Cuando los proveedores de sistemas de IA de alto riesgo o los modelos de IA de uso general no cumplan las especificaciones comunes mencionadas en el apartado 1, justificarán debidamente que han adoptado soluciones técnicas que cumplan los requisitos a que se refiere la sección 2 del presente capítulo o, según corresponda, cumplan con las obligaciones establecidas en el capítulo V, secciones 2 y 3, en un nivel como mínimo equivalente a aquellos.

6. Cuando un Estado miembro considere que una especificación común no cumple plenamente los requisitos establecidos en la sección 2, o, según corresponda, no cumple con las obligaciones establecidas en el capítulo V, secciones 2 y 3, informará de ello a la Comisión con una explicación detallada. La Comisión evaluará dicha información y, en su caso, modificará el acto de ejecución por el que se establece la especificación común de que se trate.

ARTÍCULO 42
PRESUNCIÓN DE CONFORMIDAD CON DETERMINADOS REQUISITOS

1. Se presumirá que los sistemas de IA de alto riesgo que hayan sido entrenados y probados con datos que reflejan el entorno geográfico, conductual, contextual o funcional específico en el que esté previsto su uso cumplen los requisitos pertinentes establecidos en el artículo 10, apartado 4.

2. Se presumirá que los sistemas de IA de alto riesgo que cuenten con un certificado o una declaración de conformidad en virtud de un esquema de ciberseguridad con arreglo al Reglamento (UE) 2019/881 cuyas referencias estén publicadas en el Diario Oficial de la Unión Europea cumplen los requisitos de ciberseguridad establecidos en el artículo 15 del presente Reglamento en la medida en que el certificado de ciberseguridad o la declaración de conformidad, o partes de estos, contemplen dichos requisitos.

3. Cuando un sistema de IA de alto riesgo entre en el ámbito de aplicación del Reglamento (UE) 2024/2847 y se cumplan las condiciones establecidas en el artículo 12, apartado 1, de dicho Reglamento, se considerará que dicho sistema cumple los requisitos de ciberseguridad establecidos en el artículo 15 del presente Reglamento.

ARTÍCULO 43
EVALUACIÓN DE LA CONFORMIDAD

1. En el caso de los sistemas de IA de alto riesgo enumerados en el anexo III, punto 1, cuando, al demostrar el cumplimiento de los requisitos establecidos en la sección 2 por parte de un sistema de IA de alto riesgo, el proveedor haya aplicado las normas armonizadas a que se refiere el artículo 40, o bien, en su caso, las especificaciones comunes a que se refiere el artículo 41, el proveedor optará por uno de los procedimientos de evaluación de la conformidad siguientes:

a) el fundamentado en el control interno, mencionado en el anexo VI, o

b) el fundamentado en la evaluación del sistema de gestión de la calidad y la evaluación de la documentación técnica, con la participación de un organismo notificado, mencionado en el anexo VII.

Al demostrar el cumplimiento de los requisitos establecidos en la sección 2 por parte de un sistema de IA de alto riesgo, el proveedor se atendrá al procedimiento de evaluación de la conformidad establecido en el anexo VII cuando:

a) las normas armonizadas a que se refiere el artículo 40 no existan, y no se disponga de las especificaciones comunes a que se refiere el artículo 41;

b) el proveedor no haya aplicado la norma armonizada, o solo haya aplicado parte de esta;

c) existan las especificaciones comunes a que se refiere la letra a), pero el proveedor no las haya aplicado;

d) una o varias de las normas armonizadas a que se refiere la letra a) se hayan publicado con una limitación, y únicamente en la parte de la norma objeto de la limitación.

A efectos del procedimiento de evaluación de la conformidad mencionado en el anexo VII, el proveedor podrá escoger cualquiera de los organismos notificados. No obstante, cuando se prevea la puesta en servicio del sistema de IA de alto riesgo por parte de las autoridades garantes del cumplimiento del Derecho, las autoridades de inmigración o las autoridades de asilo, o por las instituciones, órganos u organismos de la Unión, la autoridad de vigilancia del mercado mencionada en el artículo 74, apartado 8 o 9, según proceda, actuará como organismo notificado.

2. En el caso de los sistemas de IA de alto riesgo mencionados en el anexo III, puntos 2 a 8, los proveedores se atendrán al procedimiento de evaluación de la conformidad fundamentado en un control interno a que se refiere el anexo VI, que no contempla la participación de un organismo notificado.

3. En el caso de los sistemas de IA de alto riesgo regulados por los actos legislativos de armonización de la Unión enumerados en el anexo I, sección A, el proveedor del sistema se atendrá al procedimiento de evaluación de la conformidad pertinente exigido de conformidad con los actos legislativos de armonización de la Unión pertinentes. Los requisitos establecidos en la sección 2 del presente capítulo se aplicarán a dichos sistemas de IA de alto riesgo y formarán parte de dicha evaluación. También se llevará a cabo una evaluación del sistema de gestión de la calidad establecido en el artículo 17, y se aplicarán los puntos 3, 4.3, 4.4 y 4.5, el punto 4.6, párrafo quinto, y el punto 5 del anexo VII.

A efectos de dicha evaluación de la conformidad, los organismos notificados que hayan sido notificados con arreglo a los actos legislativos de armonización de la Unión enumerados en el anexo I, sección A, estarán facultados para evaluar la conformidad de los sistemas de IA de alto riesgo con los requisitos establecidos en la sección 2 del presente capítulo, a condición de que el cumplimiento por parte de dichos organismos notificados de los requisitos establecidos en el artículo 31, apartados 4, 5, 10 y 11, se haya evaluado en el contexto del procedimiento de notificación con arreglo a los actos legislativos de armonización de la Unión pertinentes, lo que se demuestra mediante la evaluación efectuada en el marco de la notificación existente. Sin perjuicio de lo dispuesto en el artículo 28, dichos organismos notificados que hayan sido notificados de conformidad con los actos legislativos de armonización de la Unión enumerados en el anexo I, sección A, solicitarán su designación de conformidad con la sección 4 del presente capítulo a más tardar el 28 de enero de 2028.

Cuando un acto legislativo de armonización de la Unión enumerado en el anexo I, sección A, permita al fabricante del producto recurrir a una evaluación de la conformidad en la que no participen terceros a condición de que el fabricante haya aplicado normas armonizadas para garantizar el cumplimiento de todos los requisitos pertinentes, dicho fabricante solamente podrá recurrir dicha opción si también ha aplicado normas armonizadas o, en su caso, especificaciones comunes previstas en el artículo 41 que contemplen todos los requisitos establecidos en la sección 2 del presente capítulo. La clasificación de un producto como sistema de IA de alto riesgo de conformidad con el artículo 6, apartado 1, no afecta a las opciones relativas al procedimiento de evaluación de la conformidad de que disponen los fabricantes de productos regulados por los actos legislativos de armonización de la Unión enumerados en el anexo I, sección A, incluida, en su caso, la opción de basarse en normas armonizadas. Los fabricantes de dichos productos no están obligados a optar por un procedimiento de evaluación de la conformidad que implique una evaluación de la conformidad de terceros solo por motivo de que el producto incluya un sistema de IA de alto riesgo como componente de seguridad cuando no lo exijan los actos legislativos de armonización de la Unión enumerados en el anexo I, sección A.

En el caso de los sistemas de IA de alto riesgo que estén regulados por los actos legislativos de armonización de la Unión enumerados en el anexo I, sección A, y que entren en alguna de las categorías enumeradas en el anexo III, el proveedor del sistema se atendrá al procedimiento de evaluación de la conformidad pertinente exigido en virtud de los actos legislativos de armonización de la Unión enumerados el anexo I, sección A.

4. Los sistemas de IA de alto riesgo que ya hayan sido objeto de un procedimiento de evaluación de la conformidad se someterán a un nuevo procedimiento de evaluación de la conformidad en caso de modificación sustancial, con independencia de si está prevista una distribución posterior del sistema modificado o de si este continúa siendo utilizado por el responsable del despliegue actual.

En el caso de los sistemas de IA de alto riesgo que continúen aprendiendo tras su introducción en el mercado o su puesta en servicio, los cambios en el sistema de IA de alto riesgo y su funcionamiento que hayan sido predeterminados por el proveedor en el momento de la evaluación inicial de la conformidad y figuren en la información recogida en la documentación técnica mencionada en el anexo IV, punto 2, letra f), no constituirán modificaciones sustanciales.

5. La Comisión estará facultada para adoptar actos delegados con arreglo al artículo 97 al objeto de modificar los anexos VI y VII actualizándolos a la luz del progreso técnico.

6. La Comisión estará facultada para adoptar actos delegados de conformidad con el artículo 97 al objeto de modificar los apartados 1 y 2 del presente artículo a fin de someter a los sistemas de IA de alto riesgo mencionados en el anexo III, puntos 2 a 8, al procedimiento de evaluación de la conformidad a que se refiere el anexo VII o a partes de este. La Comisión adoptará dichos actos delegados teniendo en cuenta la eficacia del procedimiento de evaluación de la conformidad fundamentado en un control interno mencionado en el anexo VI para prevenir o reducir al mínimo los riesgos para la salud, la seguridad y la protección de los derechos fundamentales que plantean estos sistemas, así como la disponibilidad de capacidades y recursos adecuados por parte de los organismos notificados.

ARTÍCULO 44
CERTIFICADOS

1. Los certificados expedidos por los organismos notificados con arreglo al anexo VII se redactarán en una lengua que las autoridades pertinentes del Estado miembro en el que esté establecido el organismo notificado puedan entender fácilmente.

2. Los certificados serán válidos para el período que indiquen, que no excederá de cinco años para los sistemas de IA contemplados en el anexo I, y cuatro años para los sistemas de IA contemplados en el anexo III. A solicitud del proveedor, la validez de un certificado podrá prorrogarse por períodos adicionales no superiores a cinco años para los sistemas de IA contemplados en el anexo I, y cuatro

años para los sistemas de IA contemplados en el anexo III, sobre la base de una nueva evaluación con arreglo a los procedimientos de evaluación de la conformidad aplicables. Todo suplemento de un certificado mantendrá su validez a condición de que el certificado al que complementa sea válido.

3. Si un organismo notificado observa que un sistema de IA ya no cumple los requisitos establecidos en la sección 2, suspenderá o retirará, teniendo en cuenta el principio de proporcionalidad, el certificado expedido o le impondrá restricciones, a menos que se garantice el cumplimiento de dichos requisitos mediante medidas correctoras adecuadas adoptadas por el proveedor del sistema en un plazo adecuado determinado por el organismo notificado. El organismo notificado motivará su decisión.

Existirá un procedimiento de recurso frente a las decisiones de los organismos notificados, también respecto a los certificados de conformidad expedidos.

ARTÍCULO 45
OBLIGACIONES DE INFORMACIÓN DE LOS ORGANISMOS NOTIFICADOS

1. Los organismos notificados informarán a la autoridad notificante:
   a) de cualquier certificado de la Unión de evaluación de la documentación técnica, de cualquier suplemento a dichos certificados y de cualesquiera aprobaciones de sistemas de gestión de la calidad expedidas con arreglo a los requisitos establecidos en el anexo VII;
   b) de cualquier denegación, restricción, suspensión o retirada de un certificado de la Unión de evaluación de la documentación técnica o de una aprobación de un sistema de gestión de la calidad expedida con arreglo a los requisitos establecidos en el anexo VII;
   c) de cualquier circunstancia que afecte al ámbito de aplicación o a las condiciones de notificación;
   d) de cualquier solicitud de información sobre las actividades de evaluación de la conformidad que hayan recibido de las autoridades de vigilancia del mercado;
   e) previa solicitud, de las actividades de evaluación de la conformidad realizadas dentro del ámbito de aplicación de su notificación y de cualquier otra actividad realizada, incluidas las actividades transfronterizas y las subcontrataciones.
2. Cada organismo notificado informará a los demás organismos notificados:
   a) de las aprobaciones de sistemas de gestión de la calidad que haya rechazado, suspendido o retirado y, previa solicitud, de las aprobaciones de sistemas de gestión de la calidad que haya expedido;
   b) de los certificados de la Unión de evaluación de la documentación técnica o los suplementos a dichos certificados que haya rechazado, retirado, suspendido o restringido de cualquier otro modo y, previa solicitud, de los certificados o los suplementos a estos que haya expedido.
3. Cada organismo notificado proporcionará a los demás organismos notificados que realicen actividades de evaluación de la conformidad similares y relativas a los mismos tipos de sistemas de IA información pertinente sobre cuestiones relacionadas con resultados negativos y, previa solicitud, con resultados positivos de las evaluaciones de la conformidad.
4. Los organismos notificados preservarán la confidencialidad de la información obtenida, de conformidad con lo dispuesto en el artículo 78.

ARTÍCULO 46
EXENCIÓN DEL PROCEDIMIENTO DE EVALUACIÓN DE LA CONFORMIDAD

1. Como excepción a lo dispuesto en el artículo 43 y previa solicitud debidamente motivada, cualquier autoridad de vigilancia del mercado podrá autorizar la introducción en el mercado o la puesta en servicio de sistemas de IA de alto riesgo específicos en el territorio del Estado miembro de que se trate por motivos excepcionales de seguridad pública o con el fin de proteger la vida y la salud de las personas, el medio ambiente o activos fundamentales de la industria y de las infraestructuras. Dicha autorización se concederá por un período limitado, mientras se lleven a cabo los procedimientos de evaluación de la conformidad necesarios, teniendo en cuenta los motivos excepcionales que justifiquen la exención. La conclusión de los procedimientos de que se trate se alcanzará sin demora indebida.
2. En una situación de urgencia debidamente justificada por motivos excepcionales de seguridad pública o en caso de amenaza específica, importante e inminente para la vida o la seguridad física de las personas físicas, las autoridades garantes del cumplimiento del Derecho o las autoridades de protección civil podrán poner en servicio un sistema de IA de alto riesgo específico sin la autorización a que se refiere el apartado 1, siempre que se solicite dicha autorización durante o después de la utilización sin demora indebida. Si se deniega la autorización a que se refiere el apartado 1, se suspenderá el uso del sistema de IA de alto riesgo con efecto inmediato y se desecharán inmediatamente todos los resultados y toda la información de salida producidos por dicho uso.
3. La autorización a que se refiere el apartado 1 solo se expedirá si la autoridad de vigilancia del mercado llega a la conclusión de que el sistema de IA de alto riesgo cumple los requisitos establecidos en la sección 2. La autoridad de vigilancia del mercado informará a la Comisión y a los demás Estados miembros de toda autorización expedida de conformidad con los apartados 1 y 2. Esta obligación no comprenderá los datos operativos sensibles relativos a las actividades de las autoridades garantes del cumplimiento del Derecho.
4. Si, en el plazo de quince días naturales tras la recepción de la información indicada en el apartado 3, ningún Estado miembro ni la Comisión presentan objeción alguna sobre una autorización expedida por una autoridad de vigilancia del mercado de un Estado miembro con arreglo al apartado 1, la autorización se considerará justificada.
5. Si, en el plazo de quince días naturales tras la recepción de la notificación a que se refiere el apartado 3, un Estado miembro formula objeciones contra una autorización expedida por una autoridad de vigilancia del mercado de otro Estado miembro, o si la Comisión considera que la autorización vulnera el Derecho de la Unión o que la conclusión de los Estados miembros relativa al cumplimiento del sistema a que se refiere el apartado 3 es infundada, la Comisión celebrará consultas con el Estado

miembro pertinente sin demora. Se consultará a los operadores de que se trate y se les ofrecerá la posibilidad de exponer sus puntos de vista. En vista de todo ello, la Comisión decidirá si la autorización está justificada o no. La Comisión enviará su decisión al Estado miembro afectado y a los operadores pertinentes.

6. Si la Comisión considera que la autorización no está justificada, la autoridad de vigilancia del mercado del Estado miembro de que se trate la retirará.

7. En el caso de los sistemas de IA de alto riesgo asociados a productos regulados por los actos legislativos de armonización de la Unión enumerados en el anexo I, sección A, solo se aplicarán las exenciones de la evaluación de la conformidad establecidas en dichos actos legislativos de armonización de la Unión.

ARTÍCULO 47
DECLARACIÓN UE DE CONFORMIDAD

1. El proveedor redactará una declaración UE de conformidad por escrito en un formato legible por máquina, con firma electrónica o manuscrita, para cada sistema de IA de alto riesgo y la mantendrá a disposición de las autoridades nacionales competentes durante un período de diez años a contar desde la introducción del sistema de IA de alto riesgo en el mercado o su puesta en servicio. En la declaración UE de conformidad se especificará el sistema de IA de alto riesgo para el que ha sido redactada. Se entregará una copia de la declaración UE de conformidad a las autoridades nacionales competentes pertinentes que lo soliciten.

2. En la declaración UE de conformidad constará que el sistema de IA de alto riesgo de que se trate cumple los requisitos establecidos en la sección 2. La declaración UE de conformidad contendrá la información indicada en el anexo V y se traducirá a una lengua que puedan entender fácilmente las autoridades nacionales competentes del Estado o Estados miembros en que se introduzca en el mercado o comercialice el sistema de IA de alto riesgo.

3. Cuando los sistemas de IA de alto riesgo estén sujetos a otros actos legislativos de armonización de la Unión que también exijan una declaración UE de conformidad, se elaborará una única declaración UE de conformidad con respecto a todos el Derecho de la Unión aplicable al sistema de IA de alto riesgo. La declaración contendrá toda la información necesaria para determinar los actos legislativos de armonización de la Unión a los que se refiere la declaración.

4. Al elaborar la declaración UE de conformidad, el proveedor asumirá la responsabilidad del cumplimiento de los requisitos establecidos en la sección 2. El proveedor mantendrá actualizada la declaración UE de conformidad según proceda.

5. La Comisión estará facultada para adoptar actos delegados con arreglo al artículo 97 al objeto de modificar el anexo V actualizando el contenido de la declaración UE de conformidad establecida en dicho anexo, con el fin de introducir elementos que resulten necesarios a la luz del progreso técnico.

ARTÍCULO 48
MARCADO CE

1. El marcado CE estará sujeto a los principios generales establecidos en el artículo 30 del Reglamento (CE) n. o 765/2008.

2. En el caso de los sistemas de IA de alto riesgo que se proporcionan digitalmente, se utilizará un marcado CE digital, únicamente si es fácilmente accesible a través de la interfaz desde la que se accede a dicho sistema o mediante un código fácilmente accesible legible por máquina u otros medios electrónicos.

3. El marcado CE se colocará de manera visible, legible e indeleble en los sistemas de IA de alto riesgo. Cuando esto no sea posible o no pueda garantizarse debido a la naturaleza del sistema de IA de alto riesgo, se colocará en el embalaje o en los documentos adjuntos, según proceda.

4. En su caso, el marcado CE irá seguido del número de identificación del organismo notificado responsable de los procedimientos de evaluación de la conformidad establecidos en el artículo 43. El número de identificación del organismo notificado lo colocará él mismo o, siguiendo sus instrucciones, el proveedor o el representante autorizado del proveedor. El número de identificación figurará también en todo el material publicitario en el que se mencione que el sistema de IA de alto riesgo cumple los requisitos de marcado CE.

5. Cuando los sistemas de IA de alto riesgo estén sujetos a otras disposiciones del Derecho de la Unión que también requieran la colocación del marcado CE, este indicará que los sistemas de IA de alto riesgo también cumplen los requisitos de esas otras disposiciones.

ARTÍCULO 49
REGISTRO

1. Antes de introducir en el mercado o de poner en servicio un sistema de IA de alto riesgo enumerado en el anexo III, con excepción de los sistemas de IA de alto riesgo mencionados en el anexo III, punto 2, el proveedor o, en su caso, el representante autorizado, registrarán su sistema y a ellos mismos en la base de datos de la UE a que se refiere el artículo 71.

2. Antes de introducir en el mercado o poner en servicio un sistema de IA sobre el que el proveedor haya llegado a la conclusión de que no es de alto riesgo de conformidad con el artículo 6, apartado 3, dicho proveedor o, en su caso, el representante autorizado, registrarán ese sistema y a ellos mismos en la base de datos de la UE a que se refiere el artículo 71.

3. Antes de poner en servicio o utilizar un sistema de IA de alto riesgo enumerado en el anexo III, con excepción de los sistemas de IA de alto riesgo mencionados en el anexo III, punto 2, los responsables del despliegue de sistemas de IA de alto riesgo que sean autoridades públicas, instituciones, órganos u organismos de la Unión, o personas que actúen en su nombre, se registrarán, seleccionarán el sistema y registrarán su utilización en la base de datos de la UE a que se refiere el artículo 71.

4. En el caso de los sistemas de IA de alto riesgo mencionados en el anexo III, puntos 1, 6 y 7, en los ámbitos de la garantía del cumplimiento del Derecho, la migración, el asilo y la gestión del control fronterizo, el registro a que se refieren los apartados 1, 2 y 3 del presente artículo se efectuará en

una sección segura no pública de la base de datos de la UE a que se refiere el artículo 71 e incluirá únicamente la información, según proceda, a la que se hace referencia en:

a) el anexo VIII, sección A, puntos 1 a 10, con excepción de los puntos 6, 8 y 9;

b) el anexo VIII, sección B, puntos 1 a 5 y puntos 8 y 9;

c) el anexo VIII, sección C, puntos 1 a 3;

d) el anexo IX, puntos 1, 2, 3 y 5.

Únicamente la Comisión y las autoridades nacionales a que se refiere el artículo 74, apartado 8, tendrán acceso a las secciones restringidas respectivas de la base de datos de la UE enumeradas en el párrafo primero del presente apartado.

5. Los sistemas de IA de alto riesgo a que se refiere el anexo III, punto 2, se registrarán a nivel nacional.

Fuente: Reglamento (UE) 2024/1689, texto consolidado a 27 de julio de 2026. Transcripción del PDF aportado; se han omitido las marcas editoriales de consolidación y las cabeceras de página.

Resumen del Capítulo III — Sistemas de inteligencia artificial de alto riesgo

Reglamento (UE) 2024/1689 · Texto consolidado a 27/07/2026 · Páginas 17–59 · Artículos 6 a 49

Este es uno de los capítulos más importantes del Reglamento Europeo de Inteligencia Artificial para las empresas.

La idea fundamental es que determinados sistemas de IA pueden utilizarse, pero requieren controles especiales cuando pueden afectar significativamente a la seguridad, la salud o los derechos fundamentales de las personas.

A diferencia del capítulo II, que establece prácticas prohibidas, el capítulo III regula los sistemas de alto riesgo que pueden desarrollarse, comercializarse y utilizarse cumpliendo determinadas obligaciones.

El capítulo está dividido en cinco secciones.

1. Clasificación de los sistemas de IA de alto riesgo

Artículos 6 y 7 · Páginas 17–20

El Reglamento identifica dos grandes categorías de sistemas de IA de alto riesgo.

A. Sistemas vinculados a productos regulados por la legislación europea

Son sistemas de IA que funcionan como componentes de seguridad de determinados productos, o que constituyen esos productos, cuando están sujetos a la evaluación de conformidad de terceros prevista en la normativa sectorial correspondiente.

Por ejemplo, determinados sistemas de IA integrados en productos sanitarios, maquinaria o equipos industriales.

B. Sistemas utilizados en determinadas actividades sensibles

El anexo III identifica ocho ámbitos en los que determinadas aplicaciones de IA se consideran de alto riesgo.

Ámbito	Ejemplo práctico
Biometría	Identificación biométrica remota y determinados sistemas de reconocimiento de emociones
Infraestructuras críticas	IA que controla componentes de seguridad del suministro eléctrico o del agua
Educación	IA que determina admisiones o evalúa resultados académicos
Empleo y recursos humanos	IA que selecciona candidatos, decide promociones o evalúa trabajadores
Servicios esenciales	IA que evalúa la solvencia de personas físicas o riesgos en seguros de vida y salud
Aplicación de la ley	IA utilizada en determinadas investigaciones policiales
Migración y fronteras	IA que ayuda a evaluar determinadas solicitudes de asilo
Justicia y democracia	IA que asiste en determinadas decisiones judiciales o pretende influir en elecciones

¿Todas las aplicaciones de estos ámbitos son de alto riesgo?

No necesariamente.

El artículo 6 contempla excepciones cuando el sistema no presenta un riesgo importante para las personas y se limita, por ejemplo, a realizar tareas administrativas o preparatorias, mejorar actividades humanas previas o detectar patrones sin sustituir una valoración humana adecuada.

Sin embargo, cuando el sistema del anexo III realiza **elaboración de perfiles de personas físicas**, se considera siempre de alto riesgo.

El proveedor que aplique una excepción debe justificar y documentar su clasificación y cumplir las obligaciones de registro correspondientes.

Aplicación empresarial: una IA que organiza documentos de recursos humanos no tiene por qué ser de alto riesgo. Una IA diseñada para seleccionar candidatos o determinar ascensos puede serlo, dependiendo de sus funciones y de las excepciones aplicables.

2. Requisitos de los sistemas de IA de alto riesgo

Artículos 8 a 15 · Páginas 20–28

Esta sección fija las condiciones técnicas y organizativas que deben cumplir los sistemas de alto riesgo.

Artículo	Requisito	¿Qué significa en la práctica?
8	Cumplimiento general	El sistema debe satisfacer los requisitos legales aplicables.
9	Gestión de riesgos	Identificar, evaluar, controlar y revisar los riesgos durante todo su ciclo de vida.
10	Calidad y gobernanza de datos	Controlar la calidad, representatividad y posibles sesgos de los datos utilizados.
11	Documentación técnica	Mantener documentación que permita verificar cómo funciona el sistema y si cumple los requisitos.
12	Conservación de registros	Permitir el registro automático de acontecimientos relevantes para facilitar la trazabilidad.
13	Transparencia	Facilitar instrucciones e información suficientes para interpretar y utilizar correctamente los resultados.
14	Supervisión humana	Permitir que personas capacitadas supervisen el sistema e intervengan cuando sea necesario.
15	Precisión, solidez y ciberseguridad	Mantener niveles adecuados de exactitud, resistencia a errores y protección frente a ataques.

Los cuatro requisitos más importantes para una empresa

Gestión de riesgos. El sistema debe someterse a controles continuos. No basta con comprobar su funcionamiento durante la instalación; hay que considerar también los riesgos que puedan aparecer posteriormente.

Calidad de los datos. Cuando se utilizan datos para entrenar, validar o probar los modelos, deben ser pertinentes, suficientemente representativos y lo más completos y correctos posible. También deben analizarse los posibles sesgos discriminatorios.

Supervisión humana. La IA no debe impedir que las personas responsables comprendan sus resultados, detecten errores, eviten una confianza excesiva en sus recomendaciones e intervengan cuando corresponda.

Seguridad y trazabilidad. Deben existir mecanismos apropiados para registrar el funcionamiento, detectar incidencias y proteger la integridad del sistema.

Ejemplo en un ERP

Imaginemos que una empresa incorpora una IA que analiza el rendimiento de los empleados y recomienda decisiones sobre promociones o despidos.

Si se clasifica como sistema de alto riesgo, el proveedor debe asegurar, entre otras cosas, que la solución:

- Dispone de controles adecuados sobre la calidad de los datos.
- Permite comprender y revisar sus recomendaciones.

- Facilita la supervisión humana efectiva.
- Documenta los riesgos y las medidas para mitigarlos.
- Mantiene mecanismos de trazabilidad y seguridad.

Importante: que una herramienta utilice IA para generar informes, realizar previsiones de ventas o automatizar la contabilización de facturas no significa, por sí solo, que sea de alto riesgo.

3. Obligaciones de proveedores, usuarios e integradores de IA

Artículos 16 a 27 · Páginas 28–40

Esta sección es especialmente relevante porque **distribuye las responsabilidades entre quienes fabrican, comercializan, integran y utilizan sistemas de IA de alto riesgo**.

A. Obligaciones de los proveedores (artículos 16–21)

Los proveedores deben garantizar que sus sistemas cumplen los requisitos establecidos.

Entre sus principales obligaciones se encuentran:

- Implantar un sistema de gestión de la calidad.
- Elaborar y mantener la documentación técnica.
- Realizar las evaluaciones de conformidad que correspondan.
- Mantener registros y mecanismos de trazabilidad.
- Emitir la declaración UE de conformidad y colocar el marcado CE.
- Registrar determinados sistemas en la base de datos europea.
- Vigilar el funcionamiento de los sistemas después de su comercialización.
- Adoptar medidas correctoras y colaborar con las autoridades.

El artículo 18 establece, como regla general, la conservación de determinada documentación durante **10 años** desde la introducción en el mercado o puesta en servicio.

B. Obligaciones de importadores y distribuidores (artículos 22–24)

Quienes comercialicen sistemas de alto riesgo también tienen responsabilidades.

Deben comprobar que los productos cumplen las exigencias correspondientes, verificar la documentación y colaborar con las autoridades cuando se detecten irregularidades.

No pueden comercializar conscientemente sistemas que incumplan los requisitos aplicables sin adoptar las medidas correspondientes.

C. Responsabilidades de los integradores (artículo 25)

Muy relevante para integraciones ERP

Este artículo establece que un distribuidor, importador, cliente u otro tercero puede convertirse jurídicamente en proveedor cuando:

- Comercializa un sistema de alto riesgo bajo su propio nombre o marca.
- Realiza una modificación sustancial de un sistema de alto riesgo.
- Cambia la finalidad prevista de un sistema de IA y provoca que pase a considerarse de alto riesgo.

Ejemplo práctico: una empresa integra un motor de IA en un ERP para que analice candidatos y decida automáticamente cuáles deben continuar un proceso de selección.

Si esa integración modifica sustancialmente el sistema o cambia su finalidad de forma que lo convierte en uno de alto riesgo, el integrador podría asumir las obligaciones propias de un proveedor.

Por tanto, no basta con indicar que la tecnología procede de un tercero. Es necesario analizar qué funciones se incorporan y quién es responsable del sistema resultante.

D. Obligaciones de las empresas que utilizan IA (artículo 26)

Este es probablemente el artículo más importante para una empresa que utiliza un sistema de IA de alto riesgo adquirido a un tercero.

Obligación	Aplicación práctica
Uso conforme a instrucciones	Utilizar la IA dentro de las condiciones establecidas por el proveedor.
Supervisión humana	Asignar personal capacitado y con autoridad para supervisarla.
Calidad de los datos de entrada	Asegurar su pertinencia y representatividad cuando estén bajo control de la empresa.
Vigilancia del funcionamiento	Detectar riesgos, errores e incidencias.
Conservación de registros	Mantener los registros automáticos bajo su control, generalmente durante al menos seis meses.
Información a los trabajadores	Informar a los trabajadores afectados y a sus representantes antes de utilizar IA de alto riesgo en el lugar de trabajo.
Información a personas afectadas	En los supuestos previstos, comunicar que se utiliza IA de alto riesgo para tomar o apoyar decisiones sobre ellas.
Comunicación de incidentes	Informar cuando corresponda y suspender la utilización si existen determinados riesgos.

Obligación específica en recursos humanos

El artículo 26.7 establece que, antes de introducir un sistema de IA de alto riesgo en el lugar de trabajo, el empleador debe informar a los representantes de los trabajadores y a los trabajadores afectados.

Esto es especialmente importante cuando se incorpora IA para selección de personal, evaluación del rendimiento, asignación de tareas o determinadas decisiones laborales.

La obligación consiste en informar conforme a las reglas aplicables, sin que este artículo establezca por sí solo una autorización sindical general para implantar cualquier sistema.

E. Evaluación de impacto sobre los derechos fundamentales (artículo 27)

Determinados responsables del despliegue deben realizar una evaluación previa de las consecuencias que el sistema puede tener sobre las personas.

Esta obligación afecta, en los supuestos establecidos por el artículo, a organismos públicos, entidades privadas que prestan servicios públicos y responsables de determinados sistemas de evaluación crediticia y seguros.

La evaluación debe contemplar el contexto de utilización, las personas afectadas, los riesgos, la supervisión humana y las medidas previstas ante posibles daños.

Importante: no todas las empresas privadas que utilizan IA de alto riesgo están obligadas automáticamente a realizar esta evaluación específica. Depende del tipo de organización y del sistema utilizado, sin perjuicio de otras obligaciones como las del RGPD.

4. Autoridades notificantes y organismos notificados

Artículos 28 a 39 · Páginas 40–49

Esta sección regula las entidades que participan en la evaluación y certificación de determinados sistemas de IA.

Establece requisitos para garantizar su independencia, competencia técnica y supervisión.

Las autoridades notificantes son responsables de los procedimientos de evaluación, designación y supervisión de los organismos de evaluación de la conformidad.

Los organismos notificados intervienen cuando el procedimiento aplicable requiere una evaluación externa.

Aplicación empresarial: no todos los sistemas de IA de alto riesgo tienen que pasar por una certificación externa. El procedimiento depende de su clasificación y de lo establecido en el artículo 43.

5. Normas, evaluación de conformidad, certificados y registro

Artículos 40 a 49 · Páginas 49–59

Esta última sección establece cómo se demuestra y acredita el cumplimiento de los requisitos.

Artículos	Contenido	Consecuencia práctica
40–42	Normas armonizadas y presunción de conformidad	Facilitan demostrar el cumplimiento de determinados requisitos.
43	Evaluación de conformidad	Establece los procedimientos de evaluación aplicables.
44–45	Certificados y obligaciones de información	Regulan los certificados y las obligaciones de los organismos notificados.
46	Exenciones excepcionales	Permite autorizaciones especiales y limitadas en determinadas circunstancias.
47	Declaración UE de conformidad	El proveedor declara formalmente que el sistema cumple los requisitos.
48	Marcado CE	Identifica la conformidad con la normativa aplicable.
49	Registro	Establece el registro de determinados sistemas en la base de datos europea.

¿Qué significa el marcado CE?

En los sistemas de IA de alto riesgo sujetos a estas obligaciones, el marcado CE indica que el proveedor declara su conformidad con las exigencias aplicables.

Cuando se distribuyen digitalmente, el Reglamento permite utilizar un marcado CE digital accesible mediante la interfaz del sistema u otros medios electrónicos previstos.

El marcado CE no significa que todos los sistemas hayan sido evaluados por un organismo externo: algunos pueden someterse al procedimiento de control interno establecido en el Reglamento.

6. ¿Cuándo son exigibles estas obligaciones?

La modificación incorporada al texto consolidado de julio de 2026 establece un calendario diferenciado.

02/08/2025

En vigor

Sección 4 del capítulo III

Autoridades notificantes y organismos notificados.

02/12/2027

Previsto

Sistemas de alto riesgo del anexo III

Aplicación de las secciones 1, 2 y 3 a los sistemas clasificados conforme al artículo 6.2.

02/08/2028

Previsto

Sistemas de alto riesgo vinculados al anexo I

Aplicación de las secciones 1, 2 y 3 a los sistemas clasificados conforme al artículo 6.1.

Fechas del artículo 113 de la versión consolidada aportada. Sujetas a las excepciones y disposiciones transitorias correspondientes.

7. Aplicación del capítulo III a Sage 200 y otros ERP

Para entender su repercusión empresarial, podemos comparar varias funcionalidades de IA.

Funcionalidad	Valoración orientativa
Lectura OCR de facturas	No es de alto riesgo por su función habitual.
Conciliación bancaria mediante IA	No es de alto riesgo por su mera automatización.
Predicción de ventas y demanda	No es de alto riesgo por estas funciones.
Generación de informes financieros	No es de alto riesgo por su función habitual.
Evaluación de solvencia de personas físicas	Potencialmente alto riesgo.
Selección automatizada de candidatos	Potencialmente alto riesgo.
Evaluación del rendimiento individual de trabajadores	Potencialmente alto riesgo.
Asignación de tareas basada en comportamientos individuales o características personales	Potencialmente alto riesgo.
Asistente de IA que consulta información empresarial	No es de alto riesgo por realizar consultas, aunque puede tener otras obligaciones.

La clasificación definitiva exige analizar la finalidad prevista, el funcionamiento concreto y las excepciones del artículo 6. No es una clasificación oficial de productos Sage.

En una integración con Sage 200 y soluciones externas mediante APIs, conectores o MCP, será especialmente importante identificar si la IA se limita a informar, recomendar, automatizar procesos o intervenir en decisiones sobre personas.

También habrá que definir contractualmente quién proporciona el sistema, quién lo modifica, quién lo utiliza y quién responde de cada obligación.

8. Conclusión del capítulo III

El capítulo III introduce un principio fundamental: **cuanto mayor sea el riesgo que un sistema de IA representa para las personas, mayores serán las exigencias de control, documentación y supervisión**.

Para las empresas, las principales consecuencias son:

- No toda IA es de alto riesgo.
- Las aplicaciones que afectan al empleo, a determinadas decisiones financieras sobre personas o a servicios esenciales merecen especial atención.
- Los proveedores tienen obligaciones técnicas y documentales importantes.
- Los clientes que utilizan sistemas de alto riesgo también asumen responsabilidades.
- Los integradores pueden convertirse en proveedores a efectos legales cuando realizan determinadas modificaciones.
- Las decisiones apoyadas en IA de alto riesgo deben contar con las garantías de supervisión humana que correspondan.

La cuestión clave para los ERP: utilizar IA para mejorar procesos administrativos, contables, logísticos o comerciales no supone automáticamente entrar en la categoría de alto riesgo. Sin embargo, cuando esas herramientas intervienen en determinadas decisiones sobre trabajadores, candidatos o personas físicas, las obligaciones pueden cambiar considerablemente.

Este capítulo es, por tanto, el que permite distinguir entre una automatización empresarial ordinaria y una aplicación de inteligencia artificial sometida a controles regulatorios reforzados.

TEXTO OFICIAL · CAPÍTULO IV

CAPÍTULO IV
OBLIGACIONES DE TRANSPARENCIA DE LOS PROVEEDORES Y RESPONSABLES DEL DESPLIEGUE DE DETERMINADOS SISTEMAS DE IA

ARTÍCULO 50
OBLIGACIONES DE TRANSPARENCIA DE LOS PROVEEDORES Y RESPONSABLES DEL DESPLIEGUE DE DETERMINADOS SISTEMAS DE IA

1. Los proveedores garantizarán que los sistemas de IA destinados a interactuar directamente con personas físicas se diseñen y desarrollen de forma que las personas físicas de que se trate estén informadas de que están interactuando con un sistema de IA, excepto cuando resulte evidente desde el punto de vista de una persona física razonablemente informada, atenta y perspicaz, teniendo en cuenta las circunstancias y el contexto de utilización. Esta obligación no se aplicará a los sistemas de IA autorizados por ley para detectar, prevenir, investigar o enjuiciar delitos, con sujeción a las garantías adecuadas para los derechos y libertades de terceros, salvo que estos sistemas estén a disposición del público para denunciar un delito penal.

2. Los proveedores de sistemas de IA, entre los que se incluyen los sistemas de IA de uso general, que generen contenido sintético de audio, imagen, vídeo o texto, velarán por que los resultados de salida del sistema de IA estén marcados en un formato legible por máquina y que sea posible detectar que han sido generados o manipulados de manera artificial. Los proveedores velarán por que sus soluciones técnicas sean eficaces, interoperables, sólidas y fiables en la medida en que sea técnicamente viable, teniendo en cuenta las particularidades y limitaciones de los diversos tipos de contenido, los costes de aplicación y el estado actual de la técnica generalmente reconocido, según se refleje en las normas técnicas pertinentes. Esta obligación no se aplicará en la medida en que los sistemas de IA desempeñen una función de apoyo a la edición estándar o no alteren sustancialmente los datos de entrada facilitados por el responsable del despliegue o su semántica, o cuando estén autorizados por ley para detectar, prevenir, investigar o enjuiciar delitos.

3. Los responsables del despliegue de un sistema de reconocimiento de emociones o de un sistema de categorización biométrica informarán del funcionamiento del sistema a las personas físicas expuestas a él y tratarán sus datos personales de conformidad con los Reglamentos (UE) 2016/679 y (UE) 2018/1725 y con la Directiva (UE) 2016/680, según corresponda. Esta obligación no se aplicará a los sistemas de IA utilizados para la categorización biométrica y el reconocimiento de emociones que hayan sido autorizados por ley para detectar, prevenir e investigar delitos, con sujeción a las garantías adecuadas para los derechos y libertades de terceros y de conformidad con el Derecho de la Unión.

4. Los responsables del despliegue de un sistema de IA que genere o manipule imágenes o contenidos de audio o vídeo que constituyan una ultrafalsificación harán público que estos contenidos o imágenes han sido generados o manipulados de manera artificial. Esta obligación no se aplicará cuando la ley autorice su uso para para detectar, prevenir, investigar o enjuiciar delitos. ◄ Cuando el contenido forme parte de una obra o programa manifiestamente creativos, satíricos, artísticos, de ficción o análogos, las obligaciones de transparencia establecidas en el presente apartado se limitarán a la obligación de hacer pública la existencia de dicho contenido generado o manipulado artificialmente de una manera adecuada que no dificulte la exhibición o el disfrute de la obra.

Los responsables del despliegue de un sistema de IA que genere o manipule texto que se publique con el fin de informar al público sobre asuntos de interés público divulgarán que el texto se ha generado o manipulado de manera artificial. Esta obligación no se aplicará cuando el uso esté autorizado por ley para detectar, prevenir, investigar o enjuiciar delitos, o cuando el contenido generado por IA haya sido sometido a un proceso de revisión humana o de control editorial y cuando una persona física o jurídica tenga la responsabilidad editorial por la publicación del contenido.

5. La información a que se refieren los apartados 1 a 4 se facilitará a las personas físicas de que se trate de manera clara y distinguible a más tardar con ocasión de la primera interacción o exposición. La información se ajustará a los requisitos de accesibilidad aplicables.

6. Los apartados 1 a 4 no afectarán a los requisitos y obligaciones establecidos en el capítulo III y se entenderán sin perjuicio de otras obligaciones de transparencia establecidas en el Derecho nacional o de la Unión para los responsables del despliegue de sistemas de IA.

7. La Comisión fomentará y facilitará la elaboración de códigos de buenas prácticas en el ámbito de la Unión para promover la aplicación efectiva de las obligaciones relativas a la detección, el marcado y el etiquetado de contenidos generados o manipulados de manera artificial. La Comisión, teniendo en cuenta en la mayor medida posible el dictamen del Consejo de IA, evaluará si la observancia de dichos códigos de buenas prácticas es adecuada para garantizar el cumplimiento de las obligaciones previstas en los apartados 2 y 4 del presente artículo, de conformidad con el procedimiento establecido en el artículo 56, apartado 6. Si considera que el código de buenas prácticas es inadecuado, la Comisión podrá adoptar un acto de ejecución que especifique normas comunes para el cumplimiento de dichas obligaciones de conformidad con el procedimiento de examen establecido en el artículo 98, apartado 2.

Fuente: Reglamento (UE) 2024/1689, texto consolidado a 27 de julio de 2026. Transcripción del PDF aportado; se han omitido las marcas editoriales de consolidación y las cabeceras de página.

Resumen del Capítulo IV — Obligaciones de transparencia de los sistemas de IA

Reglamento (UE) 2024/1689 · Texto consolidado a 27/07/2026 · Páginas 59–60 · Artículo 50

Este capítulo establece **cuándo las empresas deben informar de que están utilizando inteligencia artificial y cuándo los contenidos generados o manipulados mediante IA deben identificarse como tales**.

La finalidad es evitar que las personas sean engañadas o confundidas respecto a si están interactuando con una máquina o consumiendo contenidos auténticos.

A diferencia del capítulo III, **estas obligaciones no se limitan a los sistemas de alto riesgo**. También pueden afectar a herramientas habituales de IA generativa, asistentes virtuales y determinadas aplicaciones empresariales.

El capítulo contiene un único artículo: el **artículo 50, Obligaciones de transparencia de los proveedores y responsables del despliegue de determinados sistemas de IA**.

1. Principales obligaciones de transparencia

1. Informar cuando una persona interactúa con IA — Art. 50.1

Los proveedores deben diseñar los sistemas destinados a interactuar directamente con personas de manera que estas sepan que están hablando con una IA.

Se exceptúan, entre otros supuestos, aquellos en los que resulte evidente para una persona razonablemente informada, atenta y perspicaz.

Ejemplo: un chatbot de atención al cliente puede requerir una indicación como «Estás interactuando con un asistente de inteligencia artificial».

2. Marcar técnicamente los contenidos sintéticos — Art. 50.2

Los proveedores de sistemas que generan audio, imágenes, vídeos o textos sintéticos deben procurar que sus resultados incorporen un marcado legible por máquina que permita detectar su origen artificial.

Las soluciones técnicas deben ser eficaces, interoperables, robustas y fiables en la medida técnicamente viable.

Se contemplan excepciones para determinadas funciones de edición estándar o modificaciones que no alteren sustancialmente los datos originales ni su significado.

Ejemplo: un generador de imágenes con IA que incorpora mecanismos técnicos para identificar que las imágenes han sido generadas artificialmente.

3. Informar sobre reconocimiento de emociones o categorización biométrica — Art. 50.3

Los responsables del despliegue deben informar a las personas expuestas al funcionamiento de estos sistemas.

El tratamiento de los datos personales debe respetar el RGPD y las demás normas aplicables.

Ejemplo: una instalación que utiliza un sistema legalmente permitido para reconocer determinadas emociones mediante datos biométricos debe informar de su utilización.

4. Identificar los vídeos, imágenes y audios ultrafalsificados — Art. 50.4

Cuando un responsable del despliegue genera o manipula contenidos que constituyen una *ultrafalsificación* o *deepfake*, debe hacer público que han sido creados o manipulados artificialmente.

Para determinadas obras creativas, satíricas, artísticas o de ficción, la obligación se adapta para no dificultar su exhibición o disfrute.

Ejemplo: un vídeo corporativo que muestra a una persona real diciendo algo que nunca dijo, generado mediante IA, puede requerir identificar expresamente su naturaleza artificial.

5. Identificar determinados textos generados por IA — Art. 50.4

Cuando se publica texto generado o manipulado con IA para informar al público sobre asuntos de interés público, debe divulgarse su origen artificial.

Existe una excepción cuando el contenido ha sido sometido a revisión humana o control editorial y una persona física o jurídica asume la responsabilidad editorial de su publicación.

Ejemplo: una noticia sobre una cuestión de interés público redactada íntegramente por IA y publicada sin revisión editorial humana.

2. ¿Quién tiene la obligación de informar?

El Reglamento diferencia las responsabilidades de proveedores y responsables del despliegue.

Obligación	Responsable principal
Diseñar un chatbot para que informe de que utiliza IA	Proveedor
Incorporar marcado técnico detectable a contenidos sintéticos	Proveedor
Informar a las personas expuestas a reconocimiento de emociones	Responsable del despliegue
Revelar que un vídeo es un deepfake	Responsable del despliegue
Identificar determinados textos de interés público generados mediante IA	Responsable del despliegue

Esta distinción es importante en los proyectos de integración: una empresa puede adquirir una solución correctamente diseñada por su proveedor y, aun así, tener sus propias obligaciones respecto de cómo la utiliza y comunica sus resultados.

3. ¿Es obligatorio identificar todo contenido generado por IA?

No. El artículo 50 establece obligaciones diferentes según la naturaleza del contenido, la función del sistema y el responsable.

Uso empresarial	¿Hay obligación de informar expresamente?
Chatbot que atiende a clientes	Generalmente sí, salvo que sea evidente que se trata de IA.
Informe interno de ventas generado por IA	No exige por sí solo un aviso visible conforme al artículo 50.4.
Corrección ortográfica mediante IA	Generalmente no, si se limita a edición estándar sin modificación sustancial.
Imagen artificial generada para una campaña publicitaria	El proveedor debe cumplir las reglas de marcado técnico; la divulgación pública depende del contenido y su naturaleza.
Vídeo deepfake de una persona identificable	Sí, con las excepciones y particularidades previstas.
Texto sobre un asunto de interés público generado por IA	Sí, salvo las excepciones legales, como determinada revisión editorial humana.
Asistente interno que consulta información del ERP	Depende de sus características, aunque conviene informar claramente de que se utiliza IA.

El marcado técnico y la información al público son cuestiones distintas. **No todo contenido sintético requiere un aviso visible**, aunque su proveedor pueda estar obligado a incorporar mecanismos técnicos de identificación.

4. ¿Cómo afecta a Sage 200 y otros ERP?

Veamos varios casos prácticos.

Asistente de IA conectado a Sage 200

Un asistente que responde preguntas sobre facturas, clientes, cobros o existencias debe analizarse según si interactúa directamente con personas y si es evidente su naturaleza artificial.

La integración mediante API o MCP no elimina las obligaciones de transparencia.

Generación de informes empresariales

La IA puede elaborar informes financieros, previsiones de tesorería o resúmenes comerciales.

El artículo 50 no exige etiquetar públicamente todos esos documentos por el simple hecho de haberse generado mediante IA. Deben analizarse las reglas técnicas aplicables al proveedor y, en su caso, la finalidad de publicación.

Atención automatizada a clientes

Una empresa que incorpora un agente conversacional para atender llamadas, responder consultas sobre pedidos o informar de incidencias debe asegurarse de que se informa adecuadamente de la interacción con IA cuando resulte obligatorio.

Creación de contenidos comerciales

Si una empresa genera vídeos con personas ficticias o manipulaciones realistas de personas existentes, debe comprobar si constituyen ultrafalsificaciones sujetas a divulgación.

No debe confundirse esta obligación con una exigencia general de etiquetar cualquier fotografía o ilustración elaborada mediante IA.

5. ¿Cuándo y cómo hay que informar?

El artículo 50.5 establece que la información debe facilitarse:

- De forma clara y distinguible.
- A más tardar en la primera interacción o exposición de la persona al sistema o contenido correspondiente.
- Respetando los requisitos de accesibilidad aplicables.

En el apartado 7, modificado en 2026, se contempla el desarrollo de códigos de buenas prácticas sobre identificación y etiquetado de contenidos artificiales. La Comisión podrá adoptar normas comunes de ejecución en las condiciones previstas si considera insuficientes dichos códigos.

6. Fecha de aplicación

02/08/2026

Aplicable

Las obligaciones del capítulo IV son aplicables con carácter general desde el 2 de agosto de 2026, conforme al artículo 113 del texto consolidado.

7. Conclusión del capítulo IV

Este capítulo introduce un principio fundamental: **las personas deben poder reconocer cuándo interactúan con determinados sistemas de IA y cuándo reciben ciertos contenidos artificiales o manipulados**.

Para una empresa, las consecuencias más importantes son distinguir las obligaciones del fabricante de las del usuario, informar sobre las interacciones con asistentes inteligentes cuando sea obligatorio y aplicar las reglas correspondientes al contenido sintético.

En el contexto de Sage 200, las mayores implicaciones prácticas estarán en los asistentes de IA, las herramientas conversacionales conectadas al ERP y la generación de contenidos destinados a terceros.

La transparencia no obliga a identificar públicamente cada proceso automatizado con IA, pero sí exige informar y marcar determinados sistemas y contenidos según las circunstancias del artículo 50.

TEXTO OFICIAL · CAPÍTULO V

CAPÍTULO V
MODELOS DE IA DE USO GENERAL

SECCIÓN 1
REGLAS DE CLASIFICACIÓN

ARTÍCULO 51
REGLAS DE CLASIFICACIÓN DE LOS MODELOS DE IA DE USO GENERAL COMO MODELOS DE IA DE USO GENERAL CON RIESGO SISTÉMICO

1. Un modelo de IA de uso general se clasificará como modelo de IA de uso general con riesgo sistémico si reúne alguna de las siguientes condiciones:
   a) tiene capacidades de gran impacto evaluadas a partir de herramientas y metodologías técnicas adecuadas, como indicadores y parámetros de referencia;
   b) con arreglo a una decisión de la Comisión, adoptada de oficio o a raíz de una alerta cualificada del grupo de expertos científicos, tiene capacidades o un impacto equivalente a los establecidos en la letra a), teniendo en cuenta los criterios establecidos en el anexo XIII.
2. Se presumirá que un modelo de IA de uso general tiene capacidades de gran impacto con arreglo al apartado 1, letra a), cuando la cantidad acumulada de cálculo utilizada para su entrenamiento, medida en operaciones de coma flotante, sea superior a 10 25 .
3. La Comisión adoptará actos delegados de conformidad con el artículo 97 para modificar los umbrales a que se refieren los apartados 1 y 2 del presente artículo, así como para complementar los parámetros de referencia e indicadores en función de los avances tecnológicos, como las mejoras algorítmicas o la mayor eficiencia del hardware, cuando sea necesario, para que los umbrales reflejen el estado actual de la técnica.

ARTÍCULO 52
PROCEDIMIENTO

1. Cuando un modelo de IA de uso general cumpla la condición a que se refiere el artículo 51, apartado 1, letra a), el proveedor pertinente lo notificará a la Comisión sin demora y, en cualquier caso, antes de transcurridas dos semanas desde que se cumpla dicho requisito o desde que se sepa que va a cumplirse. Dicha notificación incluirá la información necesaria para demostrar que se cumple el requisito pertinente. Si la Comisión tiene conocimiento de un modelo de IA de uso general que presenta riesgos sistémicos y que no ha sido notificado, podrá decidir designarlo como modelo con riesgo sistémico.
2. El proveedor de un modelo de IA de uso general que cumpla la condición a que se refiere el artículo 51, apartado 1, letra a), podrá presentar, junto con su notificación, argumentos suficientemente fundamentados que demuestren que, excepcionalmente, aunque el modelo de IA de uso general cumple dicho requisito, no presenta riesgos sistémicos, debido a sus características específicas, y no debe clasificarse, por tanto, como modelo de IA de uso general con riesgo sistémico.
3. Cuando la Comisión concluya que los argumentos presentados con arreglo al apartado 2 no están suficientemente fundamentados y que el proveedor pertinente no ha sido capaz de demostrar que el modelo de IA de uso general no presenta, debido a sus características específicas, riesgos sistémicos, rechazará dichos argumentos y el modelo de IA de uso general se considerará un modelo de IA de uso general con riesgo sistémico.
4. La Comisión podrá determinar que un modelo de IA de uso general presenta riesgos sistémicos, de oficio o a raíz de una alerta cualificada del grupo de expertos científicos con arreglo al artículo 90, apartado 1, letra a), a partir de los criterios establecidos en el anexo XIII.

La Comisión estará facultada para adoptar actos delegados de conformidad con el artículo 97 al objeto de modificar el anexo XIII especificando y actualizando los criterios establecidos en dicho anexo.

5. Previa solicitud motivada de un proveedor cuyo modelo haya sido designado como modelo de IA de uso general con riesgo sistémico con arreglo al apartado 4, la Comisión tendrá en cuenta la solicitud y podrá decidir reevaluar si puede seguir considerándose que el modelo de IA de uso general presenta riesgos sistémicos con arreglo a los criterios establecidos en el anexo XIII. Dicha solicitud contendrá motivos objetivos, detallados y nuevos que hayan surgido desde la decisión de designación. Los proveedores no podrán solicitar la reevaluación antes de transcurridos seis meses desde la decisión de designación. Si tras la reevaluación la Comisión decide mantener la designación como modelo de IA de uso general con riesgo sistémico, los proveedores no podrán solicitar otra reevaluación hasta transcurridos seis meses desde dicha decisión.
6. La Comisión velará por que se publique una lista de modelos de IA de uso general con riesgo sistémico, que mantendrá actualizada, sin perjuicio de la necesidad de respetar y proteger los derechos de propiedad intelectual e industrial y la información empresarial confidencial o los secretos comerciales de conformidad con el Derecho de la Unión y nacional.

SECCIÓN 2
OBLIGACIONES DE LOS PROVEEDORES DE MODELOS DE IA DE USO GENERAL

ARTÍCULO 53
OBLIGACIONES DE LOS PROVEEDORES DE MODELOS DE IA DE USO GENERAL

1. Los proveedores de modelos de IA de uso general:
   a) elaborarán y mantendrán actualizada la documentación técnica del modelo, incluida la información relativa al proceso de entrenamiento y realización de pruebas y los resultados de su evaluación, que contendrá, como mínimo, la información establecida en el anexo XI con el fin de facilitarla, previa solicitud, a la Oficina de IA y a las autoridades nacionales competentes;
   b) elaborarán y mantendrán actualizada información y documentación y la pondrán a disposición de los proveedores de sistemas de IA que tengan la intención de integrar el modelo de IA de uso general en sus sistemas de IA. Sin perjuicio de la necesidad de observar y proteger los derechos de propiedad intelectual e industrial y la información empresarial confidencial o los secretos comerciales de conformidad con el Derecho de la Unión y nacional, dicha información y documentación:

i) permitirá a los proveedores de sistemas de IA entender bien las capacidades y limitaciones del modelo de IA de uso general y cumplir sus obligaciones en virtud del presente Reglamento, y

ii) contendrá, como mínimo, los elementos previstos en el anexo XII;

c) establecerán directrices para cumplir el Derecho de la Unión en materia de derechos de autor y derechos afines, y en particular, para detectar y cumplir, por ejemplo, a través de tecnologías punta, una reserva de derechos expresada de conformidad con el artículo 4, apartado 3, de la Directiva (UE) 2019/790;

d) elaborarán y pondrán a disposición del público un resumen suficientemente detallado del contenido utilizado para el entrenamiento del modelo de IA de uso general, con arreglo al modelo facilitado por la Oficina de IA.

2. Las obligaciones establecidas en el apartado 1, letras a) y b), no se aplicarán a los proveedores de modelos de IA que se divulguen con arreglo a una licencia libre y de código abierto que permita el acceso, la utilización, la modificación y la distribución del modelo y cuyos parámetros, incluidos los pesos, la información sobre la arquitectura del modelo y la información sobre el uso del modelo, se pongan a disposición del público. Esta excepción no se aplicará a los modelos de IA de uso general con riesgo sistémico.

3. Los proveedores de modelos de IA de uso general cooperarán con la Comisión y las autoridades nacionales competentes, según sea necesario, en el ejercicio de sus competencias y facultades en virtud del presente Reglamento.

4. Los proveedores de modelos de IA de uso general podrán recurrir a códigos de buenas prácticas en el sentido de lo dispuesto en el artículo 56 para demostrar el cumplimiento de las obligaciones establecidas en el apartado 1 del presente artículo, hasta que se publique una norma armonizada. El cumplimiento de las normas armonizadas europeas otorga a los proveedores presunción de conformidad en la medida en que tales normas regulen dichas obligaciones. Los proveedores de modelos de IA de uso general que no se adhieran a un código de buenas prácticas aprobado o no cumplan una norma armonizada europea deberán demostrar que cumplen sus obligaciones por medios alternativos adecuados para su evaluación por parte de la Comisión.

5. A fin de facilitar el cumplimiento de lo dispuesto en el anexo XI, en particular en su punto 2, letras d) y e), la Comisión estará facultada para adoptar actos delegados de conformidad con el artículo 97 para detallar las metodologías de medición y cálculo con vistas a que la documentación sea comparable y verificable.

6. La Comisión estará facultada para adoptar actos delegados con arreglo al artículo 97, apartado 2, para modificar los anexos XI y XII en función de los avances tecnológicos.

7. Toda información o documentación obtenida en virtud del presente artículo, incluidos los secretos comerciales, se tratarán de conformidad con las obligaciones de confidencialidad establecidas en el artículo 78.

ARTÍCULO 54
REPRESENTANTES AUTORIZADOS DE LOS PROVEEDORES DE MODELOS DE IA DE USO GENERAL

1. Antes de introducir en el mercado de la Unión un modelo de IA de uso general, los proveedores establecidos en terceros países tendrán que nombrar, mediante un mandato escrito, a un representante autorizado que esté establecido en la Unión.

2. Los proveedores permitirán que su representante autorizado pueda efectuar las tareas especificadas en el mandato recibido del proveedor.

3. Los representantes autorizados efectuarán las tareas especificadas en el mandato recibido del proveedor. Facilitarán a la Oficina de IA, cuando lo solicite, una copia del mandato en una de las lenguas oficiales de las instituciones de la Unión. A los efectos del presente Reglamento, el mandato habilitará al representante autorizado para realizar las tareas siguientes:

a) comprobar que se ha elaborado la documentación técnica que se indica en el anexo XI y que el proveedor cumple todas las obligaciones a que se refiere el artículo 53 y, en su caso, el artículo 55;

b) conservar una copia de la documentación técnica que se indica en el anexo XI a disposición de la Oficina de IA y de las autoridades nacionales competentes por un período de diez años a partir de la introducción en el mercado del modelo de IA de uso general, y de los datos de contacto del proveedor que haya designado al representante autorizado;

c) facilitar a la Oficina de IA, previa solicitud motivada, toda la información y documentación, incluidas la información y documentación mencionadas en la letra b), que sean necesarias para demostrar el cumplimiento de las obligaciones establecidas en el presente capítulo;

d) cooperar con la Oficina de IA y las autoridades competentes, previa solicitud motivada, en cualquier acción que emprendan en relación con el modelo de IA de uso general, también cuando el modelo esté integrado en un sistema de IA introducido en el mercado o puesto en servicio en la Unión.

4. El mandato habilitará al representante autorizado para que la Oficina de IA o las autoridades competentes se pongan en contacto con él, además de con el proveedor o en lugar de con el proveedor, con referencia a todas las cuestiones relacionadas con la garantía del cumplimiento del presente Reglamento.

5. El representante autorizado pondrá fin al mandato si considera o tiene motivos para considerar que el proveedor contraviene sus obligaciones en virtud del presente Reglamento. En tal caso, también informará inmediatamente a la Oficina de IA del fin del mandato y de los motivos para ello.

6. La obligación establecida en el presente artículo no se aplicará a los proveedores de modelos de IA de uso general que se divulguen con arreglo a una licencia libre y de código abierto que permita el acceso, la utilización, la modificación y la distribución del modelo y cuyos parámetros, incluidos los pesos, la información sobre la arquitectura del modelo y la información sobre el uso del modelo, se pongan a disposición del público, salvo si los

citados modelos de IA de uso general presentan riesgos sistémicos.

SECCIÓN 3
OBLIGACIONES DE LOS PROVEEDORES DE MODELOS DE IA DE USO GENERAL CON RIESGO SISTÉMICO

ARTÍCULO 55
OBLIGACIONES DE LOS PROVEEDORES DE MODELOS DE IA DE USO GENERAL CON RIESGO SISTÉMICO

1. Además de las obligaciones enumeradas en los artículos 53 y 54, los proveedores de modelos de IA de uso general con riesgo sistémico:
   a) evaluarán los modelos de conformidad con protocolos y herramientas normalizados que reflejen el estado de la técnica, lo que incluye la realización y documentación de pruebas de simulación de adversarios con el modelo con vistas a detectar y mitigar riesgos sistémicos;
   b) evaluarán y mitigarán los posibles riesgos sistémicos a escala de la Unión que puedan derivarse del desarrollo, la introducción en el mercado o el uso de modelos de IA de uso general con riesgo sistémico, así como el origen de dichos riesgos;
   c) vigilarán, documentarán y comunicarán, sin demora indebida, a la Oficina de IA y, en su caso, a las autoridades nacionales competentes, la información pertinente sobre incidentes graves y las posibles medidas correctoras para resolverlos;
   d) velarán por que se establezca un nivel adecuado de protección de la ciberseguridad para el modelo de IA de uso general con riesgo sistémico y la infraestructura física del modelo.
2. Los proveedores de modelos de IA de uso general con riesgo sistémico podrán recurrir a códigos de buenas prácticas en el sentido de lo dispuesto en el artículo 56 para demostrar el cumplimiento de las obligaciones establecidas en el apartado 1 del presente artículo, hasta que se publique una norma armonizada. El cumplimiento de las normas armonizadas europeas otorga a los proveedores presunción de conformidad en la medida en que tales normas regulen dichas obligaciones. Los proveedores de modelos de IA de uso general que no se adhieran a un código de buenas prácticas aprobado o no cumplan una norma armonizada europea deberán demostrar que cumplen sus obligaciones por medios alternativos adecuados para su evaluación por parte de la Comisión.
3. Toda información o documentación obtenida en virtud del presente artículo, incluidos los secretos comerciales, se tratarán de conformidad con las obligaciones de confidencialidad establecidas en el artículo 78.

SECCIÓN 4
CÓDIGOS DE BUENAS PRÁCTICAS

ARTÍCULO 56
CÓDIGOS DE BUENAS PRÁCTICAS

1. La Oficina de IA fomentará y facilitará la elaboración de códigos de buenas prácticas a escala de la Unión a fin de contribuir a la correcta aplicación del presente Reglamento, teniendo en cuenta los planteamientos internacionales.
2. La Oficina de IA y el Consejo de IA velarán por que los códigos de buenas prácticas comprendan al menos las obligaciones establecidas en los artículos 53 y 55, entre las que se incluyen las cuestiones siguientes:
   a) los medios para garantizar que la información a que se refiere el artículo 53, apartado 1, letras a) y b), se mantenga actualizada con respecto a la evolución del mercado y los avances tecnológicos;
   b) el nivel adecuado de detalle por lo que respecta al resumen sobre el contenido utilizado para el entrenamiento;
   c) la determinación del tipo y la naturaleza de los riesgos sistémicos a escala de la Unión, incluido su origen, cuando proceda;
   d) las medidas, procedimientos y modalidades de evaluación y gestión de los riesgos sistémicos a escala de la Unión, incluida su documentación, que serán proporcionales a los riesgos y tendrán en cuenta su gravedad y probabilidad y las dificultades específicas para hacerles frente, habida cuenta de la manera en que dichos riesgos pueden surgir y materializarse a lo largo de la cadena de valor de la IA.
3. La Oficina de IA podrá invitar a todos los proveedores de modelos de IA de uso general, así como a las autoridades nacionales competentes pertinentes, a participar en la elaboración de códigos de buenas prácticas. Las organizaciones de la sociedad civil, la industria, el mundo académico y otras partes interesadas pertinentes, como los proveedores posteriores y los expertos independientes, podrán contribuir al proceso.
4. La Oficina de IA y el Consejo de IA velarán por que los códigos de buenas prácticas establezcan claramente sus objetivos específicos y contengan compromisos o medidas, como, por ejemplo, indicadores clave de rendimiento, si procede, para garantizar la consecución de dichos objetivos, y que tengan debidamente en cuenta las necesidades e intereses de todas las partes interesadas, incluidas las personas afectadas, a escala de la Unión.
5. La Oficina de IA velará por que los participantes en los códigos de buenas prácticas informen periódicamente a la Oficina de IA sobre la aplicación de los compromisos y las medidas adoptadas y sus resultados, lo que incluye su evaluación con respecto a los indicadores clave de rendimiento, si procede. Los indicadores clave de rendimiento y los compromisos de presentación de información reflejarán las diferencias de tamaño y capacidad entre los distintos participantes.
6. La Comisión y el Consejo de IA supervisarán y evaluarán periódicamente la consecución de los objetivos de los códigos de buenas prácticas por parte de los participantes y su contribución a la correcta aplicación del presente Reglamento. La Comisión, teniendo en cuenta en la mayor medida posible el dictamen del Consejo de IA, evaluará si los códigos de buenas prácticas incluyen las obligaciones establecidas en los artículos 53 y 55, y supervisará y evaluará periódicamente la consecución de sus objetivos. La Comisión publicará su evaluación de la adecuación de los códigos de buenas prácticas.
7. La Oficina de IA podrá invitar a todos los proveedores de modelos de IA de uso general a adherirse a los códigos de buenas prácticas. En el caso de los proveedores de modelos de IA de uso general que no presenten riesgos sistémicos, esta adhesión podrá limitarse a las obligaciones previstas

en el artículo 53, salvo que declaren expresamente su interés en adherirse al código completo.

8. La Oficina de IA también fomentará y facilitará, según proceda, la revisión y la adaptación de los códigos de buenas prácticas, en particular teniendo en cuenta las normas emergentes. La Oficina de IA asistirá en la evaluación de las normas disponibles.
9. Los códigos de buenas prácticas estarán finalizados a más tardar el 2 de mayo de 2025. La Oficina de IA adoptará las medidas necesarias, lo que incluye invitar a los proveedores a adherirse a los códigos de buenas prácticas con arreglo a lo dispuesto en el apartado 7.

Si un código de buenas prácticas no se ha podido finalizar a más tardar el 2 de agosto de 2025, o si la Oficina de IA lo considera inadecuado tras su evaluación con arreglo al apartado 6 del presente artículo, la Comisión podrá establecer, mediante actos de ejecución, normas comunes para el cumplimiento de las obligaciones establecidas en los artículos 53 y 55, que incluyan las cuestiones establecidas en el apartado 2 del presente artículo. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 98, apartado 2.

Fuente: Reglamento (UE) 2024/1689, texto consolidado a 27 de julio de 2026. Transcripción del PDF aportado; se han omitido las marcas editoriales de consolidación y las cabeceras de página.

Resumen del Capítulo V — Modelos de inteligencia artificial de uso general

Reglamento (UE) 2024/1689 · Texto consolidado a 27/07/2026 · Páginas 60–67 · Artículos 51 a 56

Este capítulo regula los **modelos de inteligencia artificial de uso general**, es decir, aquellos que pueden realizar una amplia variedad de tareas y utilizarse como base de numerosas aplicaciones empresariales.

Es especialmente relevante para los desarrolladores de grandes modelos de lenguaje (LLM) y para las empresas que utilizan estos modelos para construir soluciones propias.

La idea principal es que **los fabricantes de modelos de IA de uso general deben ofrecer documentación, transparencia y garantías sobre sus modelos**, con obligaciones adicionales cuando puedan generar riesgos sistémicos.

1. ¿Qué es un modelo de IA de uso general?

Un modelo de IA de uso general es aquel que puede realizar múltiples tareas diferentes y utilizarse en distintos sistemas o aplicaciones.

Por ejemplo:

- Redactar, resumir y traducir documentos.
- Interpretar preguntas formuladas en lenguaje natural.
- Analizar información y generar respuestas.
- Ayudar a programar.
- Realizar razonamientos y producir recomendaciones.
- Integrarse en asistentes empresariales o aplicaciones informáticas.

Entre los ejemplos tecnológicos se encuentran los modelos de las familias GPT, Claude, Gemini o Llama. Son ejemplos ilustrativos, no una clasificación jurídica individual de cada versión.

Diferencia entre modelo y sistema de IA

Modelo de IA de uso general

Tecnología base con capacidades generales: comprensión, generación y análisis

Integración en una solución empresarial

API, herramientas, instrucciones, conexión a bases de datos o ERP

Sistema de IA aplicado al negocio

Asistente para consultar facturas, gestionar pedidos o analizar información de Sage 200

El Reglamento diferencia las responsabilidades del proveedor del modelo de las que corresponden al proveedor o responsable del despliegue del sistema que incorpora ese modelo.

2. Sección 1. Clasificación de los modelos de uso general

Artículos 51 y 52 · Páginas 60–62

Artículo 51. Modelos de IA de uso general con riesgo sistémico

El Reglamento diferencia entre modelos de uso general ordinarios y modelos que presentan riesgos sistémicos.

Un modelo puede considerarse de riesgo sistémico si tiene capacidades de gran impacto o si la Comisión Europea determina que presenta capacidades o efectos equivalentes, atendiendo a los criterios del anexo XIII.

El artículo establece una presunción técnica cuando el entrenamiento del modelo utiliza más de \(10^{25}\) operaciones de coma flotante (FLOP).

UMBRAL TÉCNICO DE REFERENCIA

10^{25} FLOP

Por encima de este volumen acumulado de cálculo de entrenamiento, se presume que el modelo presenta capacidades de gran impacto.

No es un límite de uso para las empresas, sino un criterio de clasificación de modelos especialmente potentes.

Artículo 52. Procedimiento de clasificación

Cuando se cumple la condición de gran impacto, el proveedor debe comunicarlo a la Comisión Europea sin demora y, en cualquier caso, en un máximo de dos semanas desde que se cumple el requisito o se conoce que va a cumplirse.

La Comisión puede clasificar un modelo como de riesgo sistémico, evaluar las alegaciones del proveedor y mantener una lista pública de estos modelos.

Aplicación empresarial: una empresa que utiliza un LLM comercial mediante una API no pasa automáticamente a ser proveedora de un modelo de riesgo sistémico. Su responsabilidad depende de su papel y de las actividades que efectivamente realiza.

3. Sección 2. Obligaciones de los proveedores de modelos de IA de uso general

Artículos 53 y 54 · Páginas 62–64

Artículo 53. Obligaciones de los proveedores

Este es uno de los artículos centrales del capítulo.

Establece cuatro obligaciones principales:

Obligación	Qué exige
Documentación técnica	Mantener información sobre el modelo, su entrenamiento, pruebas y evaluaciones.
Información a integradores	Facilitar documentación sobre capacidades y limitaciones para que otros proveedores puedan incorporarlo a sus sistemas.
Derechos de autor	Establecer una política para cumplir las normas europeas sobre derechos de autor y derechos afines.
Transparencia del entrenamiento	Publicar un resumen suficientemente detallado del contenido utilizado para entrenar el modelo.

¿Qué implica cada obligación?

A. Documentación técnica

El proveedor debe disponer de documentación actualizada que permita a las autoridades conocer las características del modelo y su proceso de desarrollo y evaluación.

El anexo XI concreta la información exigible.

B. Información para terceros que integran el modelo

Cuando una empresa incorpora un modelo de IA a una solución propia, debe poder conocer sus capacidades y limitaciones a través de la documentación que corresponda facilitarle.

El anexo XII establece la información mínima que debe ponerse a disposición de los proveedores posteriores.

Este punto es especialmente relevante para los desarrolladores de software empresarial, porque les ayuda a evaluar la idoneidad del modelo y a cumplir sus propias obligaciones.

C. Respeto de los derechos de autor

Los proveedores deben establecer políticas para cumplir la legislación europea en materia de propiedad intelectual, incluida la identificación y observancia de determinadas reservas de derechos de los titulares.

D. Información sobre los datos de entrenamiento

Deben hacer público un resumen suficientemente detallado del contenido utilizado para entrenar sus modelos, siguiendo el modelo facilitado por la Oficina de IA.

No se exige publicar indiscriminadamente todos los datos ni revelar todos los secretos empresariales.

¿Qué ocurre con los modelos de código abierto?

El artículo 53.2 contempla excepciones para determinados modelos distribuidos bajo licencias libres y abiertas.

Cuando se cumplen los requisitos establecidos, pueden quedar exentos de las obligaciones de documentación técnica y de información a integradores contempladas en las letras a) y b).

Sin embargo:

- No quedan automáticamente exentos de las obligaciones relativas a derechos de autor y al resumen público del entrenamiento.
- La excepción no se aplica a modelos de IA de uso general con riesgo sistémico.

Por tanto, **que un modelo sea de código abierto no significa que esté excluido por completo del Reglamento**.

Artículo 54. Representantes autorizados

Los proveedores de modelos de IA de uso general establecidos fuera de la Unión Europea deben nombrar, como regla general, un representante autorizado establecido en la UE antes de comercializar el modelo en el mercado europeo.

Este representante sirve como interlocutor ante las autoridades y debe cumplir las funciones previstas en su mandato.

Se contempla una excepción para determinados modelos de código abierto, salvo que presenten riesgos sistémicos.

4. Sección 3. Obligaciones adicionales para modelos con riesgo sistémico

Artículo 55 · Páginas 64–65

Los proveedores de modelos de IA de uso general clasificados como de riesgo sistémico deben cumplir obligaciones adicionales a las anteriores.

Obligación adicional	Aplicación
Evaluaciones avanzadas	Realizar pruebas y evaluaciones del modelo, incluidas simulaciones de ataques.
Gestión de riesgos sistémicos	Identificar, evaluar y mitigar riesgos que puedan producirse a escala de la UE.
Notificación de incidentes graves	Documentar y comunicar los incidentes graves y las posibles medidas correctoras.
Ciberseguridad	Proteger adecuadamente el modelo y su infraestructura física.

¿Qué son los riesgos sistémicos?

Son riesgos vinculados a modelos especialmente potentes que pueden producir consecuencias importantes y propagarse a gran escala.

Entre los escenarios que pueden analizarse están la utilización maliciosa a gran escala, determinados fallos de seguridad o impactos negativos significativos sobre derechos fundamentales y seguridad.

La evaluación debe considerar el origen de los riesgos y los efectos potenciales del desarrollo, comercialización y uso del modelo.

Aplicación empresarial: estas obligaciones recaen principalmente en el proveedor del modelo de uso general con riesgo sistémico, no automáticamente en cada empresa que utiliza sus servicios.

Esto no elimina las obligaciones que puedan corresponder al sistema empresarial construido a partir de ese modelo.

5. Sección 4. Códigos de buenas prácticas

Artículo 56 · Páginas 65–67

El Reglamento establece un mecanismo para facilitar el cumplimiento de las obligaciones de los proveedores.

La Oficina de IA promueve la elaboración de códigos de buenas prácticas a escala europea.

Estos códigos deben abordar cuestiones como:

- La documentación y actualización de la información técnica.
- La transparencia sobre el contenido utilizado para el entrenamiento.
- La identificación y evaluación de riesgos sistémicos.
- La aplicación de medidas de prevención, mitigación y seguimiento.
- La medición y revisión de los compromisos asumidos.

La Comisión y el Consejo de IA evalúan su adecuación y la consecución de sus objetivos.

¿Es obligatorio adherirse?

La adhesión a los códigos no es, por sí misma, obligatoria para todos los proveedores.

Sin embargo, **las obligaciones legales sí deben cumplirse**. Los proveedores que no se adhieran a un código aprobado ni cumplan una norma armonizada deben demostrar el cumplimiento mediante otros medios adecuados.

6. ¿Cuándo entran en vigor estas obligaciones?

02/08/2025

Aplicable

Capítulo V

Aplicación general de las obligaciones relativas a los modelos de IA de uso general.

02/08/2027

Transición

Modelos comercializados antes del 2 de agosto de 2025

Fecha límite para que sus proveedores adopten las medidas necesarias para cumplir las obligaciones aplicables, conforme al artículo 111.3.

El capítulo V es aplicable desde el 2 de agosto de 2025; la transición hasta agosto de 2027 se refiere específicamente a los modelos de uso general introducidos en el mercado antes de aquella fecha.

7. ¿Cómo afecta a Sage 200 y a la integración de IA en un ERP?

En la práctica, conviene diferenciar tres situaciones.

Escenario A. Fabricante del modelo de IA

Una empresa desarrolla un modelo de uso general y lo introduce en el mercado.

Tiene que cumplir las obligaciones del capítulo V y, si el modelo presenta riesgo sistémico, los requisitos adicionales del artículo 55.

Escenario B. Desarrollador de una integración con Sage 200

Una empresa integra un modelo ya existente mediante una API o un servidor local para construir un asistente especializado en consultas contables, comerciales o financieras.

Por el simple hecho de realizar esta integración no se convierte necesariamente en proveedora del modelo de uso general. Puede, sin embargo, asumir obligaciones como proveedora del sistema de IA resultante.

Escenario C. Cliente que utiliza el asistente

Una empresa utiliza un asistente de IA conectado a Sage 200 para preguntar por facturas pendientes, analizar existencias o elaborar previsiones.

No tiene, por ese mero uso, las mismas obligaciones que el fabricante del modelo. Sí debe comprobar las obligaciones que le correspondan por utilizar el sistema y por tratar información empresarial o datos personales.

Ejemplo práctico de reparto de responsabilidades

Participante	Responsabilidad principal
Fabricante del LLM	Cumplir las obligaciones del capítulo V relativas al modelo.
Desarrollador de la integración	Evaluar sus obligaciones como proveedor del sistema de IA resultante.
Empresa usuaria	Cumplir las obligaciones aplicables al despliegue, uso y tratamiento de datos.

Esta distribución es orientativa: si una empresa modifica, comercializa o desarrolla modelos por su cuenta, su posición jurídica puede cambiar.

8. Conclusión del capítulo V

El capítulo V busca que los grandes modelos de inteligencia artificial sean más transparentes, estén adecuadamente documentados y puedan someterse a controles reforzados cuando presenten riesgos sistémicos.

Para las empresas y los desarrolladores de soluciones ERP, destacan tres conclusiones:

- **Los proveedores de modelos tienen obligaciones propias**, especialmente sobre documentación, datos de entrenamiento, propiedad intelectual y seguridad.
- **Los integradores deben distinguir entre el modelo y el sistema empresarial que construyen**, porque no se les aplican necesariamente las mismas obligaciones.
- **Los modelos con riesgo sistémico requieren controles adicionales**, especialmente sobre evaluación, mitigación de riesgos, incidentes graves y ciberseguridad.

La conclusión más relevante para una integración de IA con Sage 200 es que **utilizar un modelo comercial o abierto para construir un asistente empresarial no convierte automáticamente al integrador ni al cliente en fabricantes de ese modelo**.

No obstante, tendrán que evaluar las responsabilidades que les correspondan por el sistema que desarrollen, comercialicen o utilicen.

Todo ello debe analizarse conjuntamente con el capítulo III, si el sistema resultante es de alto riesgo, y con el capítulo IV, si está sujeto a obligaciones de transparencia.

TEXTO OFICIAL · CAPÍTULO VI

CAPÍTULO VI
MEDIDAS DE APOYO A LA INNOVACIÓN

ARTÍCULO 57
ESPACIOS CONTROLADOS DE PRUEBAS PARA LA IA

1. Los Estados miembros se asegurarán de que sus autoridades competentes establezcan al menos un espacio controlado de pruebas para la IA a escala nacional, que estará operativo a más tardar el 2 de agosto de 2027. Dicho espacio controlado de pruebas para la IA también podrá establecerse conjuntamente con las autoridades competentes de otros Estados miembros. La Comisión podrá proporcionar apoyo técnico, asesoramiento y herramientas para el establecimiento y el funcionamiento de los espacios controlados de pruebas para la IA.

La obligación prevista en el párrafo primero también podrá cumplirse mediante la participación en un espacio controlado de pruebas existente en la medida en que dicha participación proporcione un nivel de cobertura nacional equivalente a los Estados miembros participantes.

2. También podrán establecerse espacios controlados de pruebas para la IA adicionales a escala regional o local o conjuntamente con las autoridades competentes de otros Estados miembros.

3. El Supervisor Europeo de Protección de Datos podrá establecer un espacio controlado de pruebas para la IA para las instituciones, órganos y organismos de la Unión. A tal efecto, las referencias hechas en el presente capítulo a las autoridades nacionales competentes se entenderán hechas al Supervisor Europeo de Protección de Datos.

3 bis. La Oficina de IA podrá establecer un espacio controlado de pruebas para la IA a escala de la Unión para los sistemas de IA contemplados en el artículo 75, apartado 1. A tal efecto, las referencias hechas en el presente capítulo a las autoridades nacionales competentes se entenderán, cuando proceda, hechas a la Oficina de IA. Dicho espacio controlado de pruebas para la IA se pondrá en práctica en estrecha cooperación con las autoridades competentes pertinentes, en particular cuando el cumplimiento de los actos legislativos de la Unión distintos del presente Reglamento se supervise en el espacio controlado de pruebas para la IA, y proporcionará un acceso prioritario a las pymes —incluidas las empresas emergentes— y a las pequeñas empresas de mediana capitalización.

El establecimiento de un espacio controlado de pruebas para la IA a escala de la Unión por parte de la Oficina de IA se entenderá sin perjuicio de las competencias de los Estados miembros para establecer y supervisar espacios controlados de pruebas para la IA para los sistemas de IA sujetos a su supervisión.

4. Los Estados miembros velarán por que las autoridades competentes a que se refieren los apartados 1 y 2 asignen recursos suficientes para cumplir lo dispuesto en el presente artículo de manera efectiva y oportuna. Cuando proceda, las autoridades nacionales competentes cooperarán con otras autoridades pertinentes y podrán permitir la participación de otros agentes del ecosistema de la IA. El presente artículo no afectará a otros espacios controlados de pruebas establecidos en virtud del Derecho de la Unión o nacional. Los Estados miembros garantizarán un nivel adecuado de cooperación entre las autoridades que supervisan esos otros espacios controlados de pruebas y las autoridades nacionales competentes.

5. Los espacios controlados de pruebas para la IA establecidos de conformidad con el presente artículo proporcionarán un entorno controlado que fomente la innovación y facilite el desarrollo, el entrenamiento, la prueba y la validación de sistemas innovadores de IA durante un período limitado antes de su introducción en el mercado o su puesta en servicio, en virtud de un plan del espacio controlado de pruebas específico acordado entre los proveedores o proveedores potenciales y las autoridades competentes, asegurando que se disponga de las garantías adecuadas. Tales espacios controlados de pruebas podrán incluir la prueba en condiciones reales supervisadas dentro de ellos. Cuando proceda, el plan del espacio controlado de pruebas para la IA incorporará el plan de la prueba en condiciones reales a que se refieren los artículos 60 y 60 bis.

6. Las autoridades competentes proporcionarán, en su caso, orientación, supervisión y apoyo dentro del espacio controlado de pruebas para la IA con vistas a determinar los riesgos, en particular para los derechos fundamentales, la salud y la seguridad, a las pruebas y a las medidas de reducción y su eficacia en relación con las obligaciones y los requisitos del presente Reglamento y, cuando proceda, de otras disposiciones de Derecho de la Unión y nacional cuya observancia se supervise en el espacio controlado de pruebas.

7. Las autoridades competentes proporcionarán a los proveedores y proveedores potenciales que participen en el espacio controlado de pruebas para la IA orientaciones sobre las expectativas en materia de regulación y la manera de cumplir los requisitos y obligaciones establecidos en el presente Reglamento.

A petición del proveedor o proveedor potencial del sistema de IA, la autoridad competente aportará una prueba escrita de las actividades llevadas a cabo con éxito en el espacio controlado de pruebas. La autoridad competente también proporcionará un informe de salida en el que se detallen las actividades llevadas a cabo en el espacio controlado de pruebas y los resultados y resultados del aprendizaje correspondientes. Los proveedores podrán utilizar esta documentación para demostrar su cumplimiento del presente Reglamento mediante el proceso de evaluación de la conformidad o las actividades de vigilancia del mercado pertinentes. A este respecto, las autoridades de vigilancia del mercado y los organismos notificados tendrán en cuenta positivamente los informes de salida proporcionados y las pruebas escritas aportadas por la autoridad nacional competente, con vistas a acelerar los procedimientos de evaluación de la conformidad en una medida razonable.

8. Con sujeción a las disposiciones de confidencialidad del artículo 78 y con el acuerdo del proveedor o proveedor potencial, la Comisión y el Consejo de IA estarán autorizados a acceder a los informes de salida y los tendrán en cuenta, según proceda, en el ejercicio de sus funciones en virtud del presente Reglamento. Si tanto el proveedor o proveedor potencial como la autoridad nacional competente dan expresamente su acuerdo para ello, el informe de salida podrá hacerse público a través de la plataforma única de información a que se refiere el presente artículo.

9. El establecimiento de espacios controlados de pruebas para la IA tendrá por objeto contribuir a los siguientes objetivos:
   a) mejorar la seguridad jurídica para lograr el cumplimiento del presente Reglamento o, en su caso, de otras disposiciones de Derecho de la Unión y nacional aplicable;
   b) apoyar el intercambio de mejores prácticas mediante la cooperación con las autoridades que participan en el espacio controlado de pruebas para la IA;
   c) fomentar la innovación y la competitividad y facilitar el desarrollo de un ecosistema de la IA;
   d) contribuir a un aprendizaje normativo basado en datos contrastados;
   e) facilitar y acelerar el acceso al mercado de la Unión de los sistemas de IA, en particular cuando los proporcionen pymes —incluidas empresas emergentes— y pequeñas empresas de mediana capitalización.
10. Las autoridades nacionales competentes garantizarán que, en la medida en que los sistemas innovadores de IA impliquen el tratamiento de datos personales o estén comprendidos dentro del ámbito de supervisión de otras autoridades nacionales o autoridades competentes que proporcionen o apoyen el acceso a los datos, las autoridades competentes en materia de protección de datos y dichas otras autoridades nacionales o competentes estén vinculadas al funcionamiento del espacio controlado de pruebas para la IA e involucradas en la supervisión de dichos aspectos en la medida en que lo permitan sus respectivas funciones y poderes.
11. Los espacios controlados de pruebas para la IA no afectarán a las facultades de supervisión o correctoras de las autoridades competentes que supervisan los espacios controlados de pruebas, tampoco a escala regional o local. Cualquier riesgo considerable para la salud, la seguridad y los derechos fundamentales detectado durante el proceso de desarrollo y prueba de estos sistemas de IA dará lugar a una reducción adecuada. Las autoridades nacionales competentes estarán facultadas para suspender temporal o permanentemente el proceso de prueba, o la participación en el espacio controlado de pruebas si no es posible una reducción efectiva, e informarán a la Oficina de IA de dicha decisión. Con el objetivo de apoyar la innovación en materia de IA en la Unión, las autoridades nacionales competentes ejercerán sus facultades de supervisión dentro de los límites del Derecho pertinente y harán uso de su potestad discrecional a la hora de aplicar disposiciones jurídicas en relación con un proyecto específico de espacio controlado de pruebas para la IA.
12. Los proveedores y proveedores potenciales que participen en el espacio controlado de pruebas para la IA responderán, con arreglo al Derecho de la Unión y nacional en materia de responsabilidad, de cualquier daño infligido a terceros como resultado de la experimentación realizada en el espacio controlado de pruebas. Sin embargo, siempre que los proveedores potenciales respeten el plan específico y las condiciones de su participación y sigan de buena fe las orientaciones proporcionadas por la autoridad nacional competente, las autoridades no impondrán multas administrativas por infracciones del presente Reglamento. En los casos en que otras autoridades competentes responsables de otras disposiciones del Derecho de la Unión y nacional hayan participado activamente en la supervisión del sistema de IA en el espacio controlado de pruebas y hayan proporcionado orientaciones para el cumplimiento, no se impondrán multas administrativas en relación con dichas disposiciones.
13. Los espacios controlados de pruebas para la IA serán diseñados y puestos en práctica de tal manera que, cuando proceda, faciliten la cooperación transfronteriza entre las autoridades nacionales competentes.
14. Las autoridades nacionales competentes, el Supervisor Europeo de Protección de Datos y la Oficina de IA, según proceda y en el marco de sus respectivas competencias, coordinarán sus actividades y cooperarán en el marco del Consejo de IA. Podrán apoyar el establecimiento y el funcionamiento conjuntos de espacios controlados de pruebas para la IA incluido en diferentes sectores, e intercambiar buenas prácticas en relación con cuestiones conexas.
15. Las autoridades nacionales competentes informarán a la Oficina de IA y al Consejo de IA del establecimiento de un espacio controlado de pruebas y podrán solicitarles apoyo y orientación. La Oficina de IA pondrá a disposición del público una lista de los espacios controlados de pruebas previstos y existentes y la mantendrá actualizada con el fin de fomentar una mayor interacción en los espacios controlados de pruebas para la IA, así como la cooperación transfronteriza.
16. Las autoridades nacionales competentes presentarán informes anuales a la Oficina de IA y al Consejo de IA, por primera vez un año después del establecimiento del espacio controlado de pruebas para la IA y, posteriormente, cada año hasta su terminación, así como un informe final. Dichos informes proporcionarán información sobre el progreso y los resultados de la puesta en práctica de dichos espacios controlados de pruebas, incluidos mejores prácticas, incidentes, enseñanzas extraídas y recomendaciones acerca de su configuración y, en su caso, acerca de la aplicación y posible revisión del presente Reglamento, incluidos sus actos delegados y de ejecución, y sobre la aplicación de otras disposiciones de Derecho de la Unión, supervisada por las autoridades competentes en el marco del espacio controlado de pruebas. Las autoridades nacionales competentes pondrán dichos informes anuales, o resúmenes de estos, a disposición del público, en línea. La Comisión tendrá en cuenta, cuando proceda, los informes anuales en el ejercicio de sus funciones en virtud del presente Reglamento.
17. La Comisión desarrollará una interfaz única y específica que contenga toda la información pertinente relacionada con los espacios controlados de pruebas para la IA para que las partes interesadas puedan interactuar con los espacios controlados de pruebas para la IA y plantear consultas a las autoridades competentes, así como pedir orientaciones no vinculantes sobre la conformidad de productos, servicios y modelos de negocio innovadores que incorporen tecnologías de IA, de conformidad con el artículo 62, apartado 1, letra c). La Comisión se coordinará de forma proactiva con las autoridades nacionales competentes, cuando proceda.

ARTÍCULO 58
DISPOSICIONES DETALLADAS RELATIVAS A LOS ESPACIOS CONTROLADOS DE PRUEBAS PARA LA IA Y AL FUNCIONAMIENTO DE DICHOS ESPACIOS

1. A fin de evitar que se produzca una fragmentación en la Unión, la Comisión adoptará actos de ejecución que especifiquen las disposiciones detalladas para el establecimiento, el desarrollo, la puesta en práctica, el funcionamiento, la gobernanza y la supervisión de los espacios controlados de pruebas para la IA. Dichos actos de ejecución incluirán principios comunes sobre las cuestiones siguientes:
   a) los criterios de admisibilidad y selección para participar en el espacio controlado de pruebas para la IA;
   b) los procedimientos para la solicitud, la participación, la supervisión, la salida y la terminación del espacio controlado de pruebas para la IA, incluidos el plan del espacio controlado de pruebas y el informe de salida;
   c) las condiciones aplicables a los participantes;
   d) las normas detalladas aplicables a la gobernanza de los espacios controlados de pruebas para la IA contemplados en virtud del artículo 57, incluido en lo que respecta a la participación y la supervisión de las autoridades competentes en materia de protección de datos, cuando proceda, y a la coordinación y cooperación en el ámbito nacional y de la Unión.

   Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 98, apartado 2.
2. Los actos de ejecución mencionados en el apartado 1 garantizarán:
   a) que los espacios controlados de pruebas para la IA estén abiertos a cualquier proveedor o proveedor potencial de un sistema de IA que presente una solicitud y cumpla los criterios de admisibilidad y selección, que serán transparentes y equitativos, y también que las autoridades nacionales competentes informen a los solicitantes de su decisión en un plazo de tres meses a partir de la presentación de la solicitud;
   b) que los espacios controlados de pruebas para la IA permitan un acceso amplio e igualitario y se adapten a la demanda de participación; los proveedores y proveedores potenciales también podrán presentar solicitudes en asociación con responsables del despliegue y con otros terceros pertinentes;
   c) que las disposiciones detalladas y las condiciones relativas a los espacios controlados de pruebas para la IA propicien, en la medida de lo posible, que las autoridades nacionales competentes dispongan de flexibilidad para establecer y gestionar sus espacios controlados de pruebas para la IA;
   d) que el acceso a los espacios controlados de pruebas para la IA sea gratuito para las pymes, incluidas las empresas emergentes, sin perjuicio de los costes excepcionales que las autoridades nacionales competentes puedan recuperar de una forma justa y proporcionada;
   e) que se facilite a los proveedores y proveedores potenciales, mediante los resultados del aprendizaje de los espacios controlados de pruebas para la IA, el cumplimiento de las obligaciones de evaluación de la conformidad en virtud del presente Reglamento y la aplicación voluntaria de los códigos de conducta a que se refiere el artículo 95;
   f) que los espacios controlados de pruebas para la IA faciliten la participación de otros agentes pertinentes del ecosistema de la IA, como los organismos notificados y los organismos de normalización, las pymes, incluidas las empresas emergentes, las empresas, los agentes innovadores, las instalaciones de ensayo y experimentación, los laboratorios de investigación y experimentación y los centros europeos de innovación digital, los centros de excelencia y los investigadores, a fin de permitir y facilitar la cooperación con los sectores público y privado;
   g) que los procedimientos, procesos y requisitos administrativos para la solicitud, la selección, la participación y la salida del espacio controlado de pruebas para la IA sean sencillos y fácilmente inteligibles y se comuniquen claramente, a fin de facilitar la participación de las pymes, incluidas las empresas emergentes, con capacidades jurídicas y administrativas limitadas, y se racionalicen en toda la Unión, a fin de evitar la fragmentación y de que la participación en un espacio controlado de pruebas para la IA establecido por un Estado miembro o por el Supervisor Europeo de Protección de Datos esté reconocida mutua y uniformemente y tenga los mismos efectos jurídicos en toda la Unión;
   h) que la participación en el espacio controlado de pruebas para la IA se limite a un período que se ajuste a la complejidad y la escala del proyecto, y que podrá ser prorrogado por la autoridad nacional competente;
   i) que los espacios controlados de pruebas para la IA faciliten el desarrollo de herramientas e infraestructuras para la prueba, la evaluación comparativa, la evaluación y la explicación de las dimensiones de los sistemas de IA pertinentes para el aprendizaje normativo, como la precisión, la solidez y la ciberseguridad, así como de medidas para mitigar los riesgos para los derechos fundamentales y la sociedad en su conjunto.
3. Se ofrecerán a los proveedores potenciales que participen en los espacios controlados de pruebas para la IA, en particular a las pymes y las empresas emergentes, cuando proceda, servicios previos al despliegue, como orientaciones sobre la aplicación del presente Reglamento, otros servicios que aportan valor añadido, como ayuda con los documentos de normalización y la certificación, y acceso a las instalaciones de ensayo y experimentación, los centros europeos de innovación digital y los centros de excelencia.
4. Cuando las autoridades nacionales competentes estudien autorizar la realización de pruebas en condiciones reales supervisadas en el marco de un espacio controlado de pruebas para la IA que se establecerá en virtud del presente artículo, acordarán específicamente las condiciones de dichas pruebas y, en particular, las garantías adecuadas con los participantes, con vistas a proteger los derechos fundamentales, la salud y la seguridad. Cuando proceda, cooperarán con otras autoridades nacionales competentes con el fin de garantizar la coherencia de las prácticas en toda la Unión.

ARTÍCULO 59
TRATAMIENTO ULTERIOR DE DATOS PERSONALES PARA EL DESARROLLO DE DETERMINADOS SISTEMAS DE IA EN FAVOR DEL INTERÉS PÚBLICO EN EL ESPACIO CONTROLADO DE PRUEBAS PARA LA IA

1. En el espacio controlado de pruebas, los datos personales recabados lícitamente con otros fines podrán tratarse únicamente con el objetivo de desarrollar, entrenar y probar determinados sistemas de IA en el espacio controlado de pruebas cuando se cumplan todas las condiciones siguientes:
   a) que los sistemas de IA se desarrollen para que una autoridad pública u otra persona física o jurídica proteja un interés público esencial en uno o varios de los siguientes ámbitos:
      i) la seguridad y la salud públicas, incluidos la detección, el diagnóstico, la prevención, el control y el tratamiento de enfermedades y la mejora de los sistemas sanitarios,
      ii) un elevado nivel de protección y mejora de la calidad del medio ambiente, la protección de la biodiversidad, la protección contra la contaminación, las medidas de transición ecológica, la mitigación del cambio climático y las medidas de adaptación a este,
      iii) la sostenibilidad energética,
      iv) la seguridad y la resiliencia de los sistemas de transporte y la movilidad, las infraestructuras críticas y las redes,
      v) la eficiencia y la calidad de la administración pública y de los servicios públicos;
   b) que los datos tratados resulten necesarios para cumplir uno o varios de los requisitos mencionados en el capítulo III, sección 2, cuando dichos requisitos no puedan cumplirse efectivamente mediante el tratamiento de datos anonimizados o sintéticos o de otro tipo de datos no personales;
   c) que existan mecanismos de supervisión eficaces para detectar si pueden producirse durante la experimentación en el espacio controlado de pruebas riesgos elevados para los derechos y libertades de los interesados, mencionados en el artículo 35 del Reglamento (UE) 2016/679 y en el artículo 39 del Reglamento (UE) 2018/1725, así como mecanismos de respuesta para mitigar sin demora dichos riesgos y, en su caso, detener el tratamiento;
   d) que los datos personales que se traten en el contexto del espacio controlado de pruebas se encuentren en un entorno de tratamiento de datos funcionalmente separado, aislado y protegido, bajo el control del proveedor potencial, y que únicamente las personas autorizadas tengan acceso a dichos datos;
   e) que los proveedores solo puedan compartir los datos recabados originalmente de conformidad con el Derecho de la Unión en materia de protección de datos; los datos personales creados en el espacio controlado de pruebas no pueden salir del espacio controlado de pruebas;
   f) que el tratamiento de datos personales en el contexto del espacio controlado de pruebas no dé lugar a medidas o decisiones que afecten a los interesados ni afecte a la aplicación de sus derechos establecidos en el Derecho de la Unión en materia de protección de datos personales;
   g) que los datos personales tratados en el contexto del espacio controlado de pruebas se protejan mediante medidas técnicas y organizativas adecuadas y se eliminen una vez concluida la participación en dicho espacio o cuando los datos personales lleguen al final de su período de conservación;
   h) que los archivos de registro del tratamiento de datos personales en el contexto del espacio controlado de pruebas se conserven mientras dure la participación en el espacio controlado de pruebas, salvo que se disponga otra cosa en el Derecho de la Unión o el Derecho nacional;
   i) que se conserve una descripción completa y detallada del proceso y la lógica subyacentes al entrenamiento, la prueba y la validación del sistema de IA junto con los resultados del proceso de prueba como parte de la documentación técnica a que se refiere el anexo IV;
   j) que se publique una breve síntesis del proyecto de IA desarrollado en el espacio controlado de pruebas, junto con sus objetivos y resultados previstos, en el sitio web de las autoridades competentes; esta obligación no comprenderá los datos operativos sensibles relativos a las actividades de las autoridades garantes del cumplimiento del Derecho, del control fronterizo, de la inmigración o del asilo.
2. Cuando se lleve a cabo con fines de prevención, investigación, detección o enjuiciamiento de delitos o de ejecución de sanciones penales, incluidas la protección frente a amenazas para la seguridad pública y la prevención de dichas amenazas, y bajo el control y la responsabilidad de las autoridades garantes del cumplimiento del Derecho, el tratamiento de datos personales en los espacios controlados de pruebas para la IA se basará en un Derecho específico, de la Unión o nacional y cumplirá las condiciones acumulativas que se indican en el apartado 1.
3. El apartado 1 se entiende sin perjuicio del Derecho de la Unión o nacional que proscriba el tratamiento de datos personales con fines distintos de los expresamente mencionados en dichos actos, así como sin perjuicio del Derecho de la Unión o nacional que establezca las bases para el tratamiento de datos personales necesario para desarrollar, probar o entrenar sistemas innovadores de IA o de cualquier otra base jurídica, de conformidad con el Derecho de la Unión en materia de protección de datos personales.

ARTÍCULO 60
PRUEBAS DE SISTEMAS DE IA DE ALTO RIESGO EN CONDICIONES REALES FUERA DE LOS ESPACIOS CONTROLADOS DE PRUEBAS PARA LA IA

1. Los proveedores o proveedores potenciales de sistemas de IA de alto riesgo enumerados en el anexo III o regulados por los actos legislativos de armonización de la Unión enumerados en el anexo I, sección A, podrán realizar pruebas de sistemas de IA de alto riesgo en condiciones reales fuera de los espacios controlados de pruebas para la IA de conformidad con el presente artículo y con el plan de la prueba en condiciones reales a que se refiere el presente artículo, sin perjuicio de las prohibiciones establecidas en el artículo 5.

La Comisión adoptará, mediante un acto de ejecución, los elementos detallados del plan de la prueba en condiciones

reales. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 98, apartado 2.

El presente apartado se entiende sin perjuicio del Derecho de la Unión o nacional en materia de pruebas en condiciones reales de sistemas de IA de alto riesgo asociados a productos regulados por los actos legislativos de armonización de la Unión enumerados en el anexo I.

2. Los proveedores o proveedores potenciales podrán realizar pruebas de los sistemas de IA de alto riesgo mencionados en el anexo III o regulados por los actos legislativos de armonización de la Unión enumerados en el anexo I, sección A, en condiciones reales en cualquier momento antes de la introducción en el mercado o la puesta en servicio del sistema de IA de alto riesgo por cuenta propia o en asociación con uno o varios responsables del despliegue o responsables del despliegue potenciales.

3. Las pruebas de sistemas de IA de alto riesgo en condiciones reales con arreglo al presente artículo se entenderán sin perjuicio de cualquier revisión ética que se exija en el Derecho de la Unión o nacional.

4. Los proveedores o proveedores potenciales podrán realizar pruebas en condiciones reales solamente cuando se cumplan todas las condiciones siguientes:

a) el proveedor o proveedor potencial ha elaborado un plan de la prueba en condiciones reales y lo ha presentado a la autoridad de vigilancia del mercado del Estado miembro en que se vayan a realizar las pruebas en condiciones reales;

b) la autoridad de vigilancia del mercado del Estado miembro en que se vayan a realizar las pruebas en condiciones reales ha aprobado las pruebas en condiciones reales y el plan de la prueba en condiciones reales; si la autoridad de vigilancia del mercado no responde en un plazo de treinta días, se entenderá que las pruebas en condiciones reales y el plan de la prueba en condiciones reales han sido aprobados; cuando el Derecho nacional no contemple una aprobación tácita, las pruebas en condiciones reales estarán sujetas a una autorización también en este caso;

c) el proveedor o proveedor potencial, con excepción de los proveedores o proveedores potenciales de sistemas de IA de alto riesgo mencionados en el anexo III, puntos 1, 6 y 7, en los ámbitos de la garantía del cumplimiento del Derecho, la migración, el asilo y la gestión del control fronterizo, así como de los sistemas de IA de alto riesgo mencionados en el punto 2 del anexo III ha registrado las pruebas en condiciones reales de conformidad con el artículo 71, apartado 4, con un número de identificación único para toda la Unión y la información indicada en el anexo IX; el proveedor o proveedor potencial de sistemas de IA de alto riesgo a que se refiere el anexo III, puntos 1, 6 y 7, en los ámbitos de la garantía del cumplimiento del Derecho, la migración, el asilo y la gestión del control fronterizo, ha registrado las pruebas en condiciones reales en la parte no pública de la base de datos de la UE de conformidad con el artículo 49, apartado 4, letra d), con un número de identificación único para toda la Unión y la información indicada en este; el proveedor o proveedor potencial de sistemas de IA de alto riesgo a que se refiere el anexo III, punto 2, ha registrado las pruebas en condiciones reales de conformidad con el artículo 49, apartado 5;

d) el proveedor o proveedor potencial que realiza las pruebas en condiciones reales está establecido en la Unión o ha designado a un representante legal que está establecido en la Unión;

e) los datos recabados y tratados a efectos de las pruebas en condiciones reales únicamente se transferirán a terceros países si se aplican las garantías adecuadas y aplicables en virtud del Derecho de la Unión;

f) las pruebas en condiciones reales no duran más de lo necesario para lograr sus objetivos y, en cualquier caso, no más de seis meses, que podrán prorrogarse por un período adicional de seis meses, con sujeción al envío de una notificación previa por parte del proveedor o proveedor potencial a la autoridad de vigilancia del mercado, acompañada por una explicación de la necesidad de dicha prórroga;

g) los sujetos de las pruebas en condiciones reales que sean personas pertenecientes a colectivos vulnerables debido a su edad o a una discapacidad cuentan con protección adecuada;

h) cuando un proveedor o proveedor potencial organice las pruebas en condiciones reales en cooperación con uno o varios responsables del despliegue o responsables del despliegue potenciales, estos últimos habrán sido informados de todos los aspectos de las pruebas que resulten pertinentes para su decisión de participar y habrán recibido las instrucciones de uso pertinentes del sistema de IA a que se refiere el artículo 13; el proveedor o proveedor potencial y el responsable del despliegue o responsable del despliegue potencial alcanzarán un acuerdo en que se detallen sus funciones y responsabilidades con vistas a garantizar el cumplimiento de las disposiciones relativas a las pruebas en condiciones reales con arreglo al presente Reglamento y a otras disposiciones de Derecho de la Unión y nacional aplicable;

i) los sujetos de las pruebas en condiciones reales han dado su consentimiento informado de conformidad con el artículo 61 o, en el ámbito de la garantía del cumplimiento del Derecho, en el que intentar obtener el consentimiento informado impediría que se probara el sistema de IA, las pruebas en sí y los resultados de las pruebas en condiciones reales no tendrán ningún efecto negativo sobre los sujetos, cuyos datos personales se suprimirán una vez realizada la prueba;

j) las pruebas en condiciones reales son supervisadas de manera efectiva por el proveedor o el proveedor potencial y por los responsables del despliegue o los responsables del despliegue potenciales mediante personas adecuadamente cualificadas en el ámbito pertinente y con la capacidad, formación y autoridad necesarias para realizar sus tareas;

k) se pueden revertir y descartar de manera efectiva las predicciones, recomendaciones o decisiones del sistema de IA.

5. Cualquier sujeto de las pruebas en condiciones reales o su representante legalmente designado, según proceda, podrá, sin sufrir por ello perjuicio alguno y sin tener que proporcionar ninguna justificación, abandonar las pruebas en cualquier momento retirando su consentimiento informado y solicitar la supresión inmediata y permanente de sus datos personales. La retirada del consentimiento informado no afectará a las actividades ya completadas.

6. De conformidad con el artículo 75, los Estados miembros conferirán a sus autoridades de vigilancia del mercado poderes para exigir a los proveedores y proveedores potenciales que faciliten información, realizar sin previo aviso inspecciones a distancia o in situ y controlar la realización de las pruebas en condiciones reales y los sistemas de IA de alto riesgo relacionados. Las autoridades de vigilancia del mercado harán uso de dichos poderes para garantizar que las pruebas en condiciones reales se desarrollen de manera segura.
7. Se informará de cualquier incidente grave detectado en el transcurso de las pruebas en condiciones reales a la autoridad nacional de vigilancia del mercado de conformidad con el artículo 73. El proveedor o proveedor potencial adoptará medidas de reducción inmediatas o, en su defecto, suspenderá las pruebas en condiciones reales hasta que se produzca dicha reducción o pondrá fin a las pruebas. El proveedor o proveedor potencial establecerá un procedimiento para la rápida recuperación del sistema de IA en caso de que se ponga fin a las pruebas en condiciones reales.
8. El proveedor o proveedor potencial notificará a la autoridad nacional de vigilancia del mercado del Estado miembro en que se vayan a realizar las pruebas en condiciones reales la suspensión o la terminación de las pruebas en condiciones reales y los resultados finales.
9. El proveedor o proveedor potencial será responsable, conforme al Derecho de la Unión y nacional en materia de responsabilidad aplicable, de cualquier daño causado en el transcurso de sus pruebas en condiciones reales.

ARTÍCULO 60 BIS
PRUEBAS DE SISTEMAS DE IA DE ALTO RIESGO REGULADOS POR LOS ACTOS LEGISLATIVOS DE ARMONIZACIÓN DE LA UNIÓN ENUMERADOS EN EL ANEXO I, SECCIÓN B, EN CONDICIONES REALES FUERA DE LOS ESPACIOS CONTROLADOS DE PRUEBAS PARA LA IA

1. Los Estados miembros podrán permitir, de conformidad con el presente artículo, que los proveedores o proveedores potenciales de productos basados en la IA regulados por los actos legislativos de armonización de la Unión enumerados en el anexo I, sección B, realicen pruebas de sistemas de IA de alto riesgo en condiciones reales fuera de los espacios controlados de pruebas para la IA con el fin de evaluar y comprobar la conformidad de dichos sistemas con los requisitos establecidos en los artículos 8 a 15.
2. Los Estados miembros que opten por permitir las pruebas a que se refiere el apartado 1 adoptarán, individual o conjuntamente, marcos para la prueba en condiciones reales.
3. Cada Estado miembro notificará a la Comisión todo marco para la prueba en condiciones reales que adopte antes de ponerlo en práctica. Esto no afectará a las competencias de la Comisión en virtud de los actos legislativos de armonización de la Unión enumerados en el anexo I, sección B.
4. Los Estados miembros que hayan adoptado marcos para la prueba en condiciones reales se asegurarán de que las autoridades nacionales competentes pertinentes, las autoridades pertinentes y las autoridades públicas responsables de la gestión y el funcionamiento de infraestructuras y productos regulados por los actos legislativos de armonización de la Unión enumerados en el anexo I, sección B, cooperen estrechamente entre sí de buena fe y eliminen cualquier obstáculo práctico, incluidos aquellos que afecten a las normas de procedimiento que regulen el acceso a infraestructuras públicas físicas, cuando sea necesario, a fin de poner en práctica satisfactoriamente dichos marcos para la prueba en condiciones reales y probar los productos basados en la IA regulados por los actos legislativos de armonización de la Unión enumerados en el anexo I, sección B.
5. Los marcos para la prueba en condiciones reales establecerán los requisitos con arreglo a los cuales se realizará la prueba en condiciones reales. Dichos marcos:
   a) incluirán la presentación obligatoria de un plan de la prueba en condiciones reales, que deberá ser acordado entre el proveedor o proveedor potencial y la autoridad nacional competente o la autoridad pertinente de conformidad con los actos legislativos de armonización de la Unión enumerados en el anexo I, sección B;
   b) garantizarán el cumplimiento de los requisitos establecidos en el artículo 60, apartados 2 y 3, apartado 4, letras d) a j), y apartados 5 a 9, entendiéndose toda referencia hecha en dichas disposiciones a las autoridades de vigilancia del mercado como hecha a la autoridad nacional competente, o a la autoridad pertinente, según proceda, de conformidad con los actos legislativos de armonización de la Unión enumerados en el anexo I, sección B;
   c) incluirán mecanismos eficaces de gobernanza y rendición de cuentas;
   d) garantizarán un elevado nivel de protección de la salud, la seguridad y los derechos fundamentales.
6. La prueba en condiciones reales cumplirá las disposiciones aplicables establecidas en los actos legislativos de armonización de la Unión enumerados en el anexo I, sección B. Los requisitos establecidos en dichas disposiciones no afectarán a la aplicación del presente artículo en la medida necesaria para hacer posible las pruebas a que se refiere el apartado 1.

ARTÍCULO 61
CONSENTIMIENTO INFORMADO PARA PARTICIPAR EN PRUEBAS EN CONDICIONES REALES FUERA DE LOS ESPACIOS CONTROLADOS DE PRUEBAS PARA LA IA

1. A los efectos de las pruebas en condiciones reales con arreglo al artículo 60, se obtendrá de los sujetos de las pruebas un consentimiento informado dado libremente antes de participar en dichas pruebas y después de haber recibido información concisa, clara, pertinente y comprensible en relación con:
   a) la naturaleza y los objetivos de las pruebas en condiciones reales y los posibles inconvenientes asociados a su participación;
   b) las condiciones en las que se van a llevar a cabo las pruebas en condiciones reales, incluida la duración prevista de la participación del sujeto o los sujetos;
   c) sus derechos y las garantías relativas a su participación, en particular su derecho a negarse a participar y el derecho a abandonar las pruebas en condiciones reales en cualquier momento sin sufrir por ello perjuicio alguno y sin tener que proporcionar ninguna justificación;

d) las disposiciones para solicitar la reversión o el descarte de las predicciones, recomendaciones o decisiones del sistema de IA;

e) el número de identificación único para toda la Unión de la prueba en condiciones reales de conformidad con el artículo 60, apartado 4, letra c), y la información de contacto del proveedor o de su representante legal, de quien se puede obtener más información.

2. El consentimiento informado estará fechado y documentado, y se entregará una copia a los sujetos de la prueba o a sus representantes legales.

ARTÍCULO 62
MEDIDAS DIRIGIDAS A PROVEEDORES Y RESPONSABLES DEL DESPLIEGUE, EN PARTICULAR PYMES, INCLUIDAS LAS EMPRESAS EMERGENTES

1. Los Estados miembros adoptarán las medidas siguientes:

a) proporcionarán a las pymes, incluidas las empresas emergentes, que tengan un domicilio social o una sucursal en la Unión un acceso prioritario a los espacios controlados de pruebas para la IA, siempre que cumplan las condiciones de admisibilidad y los criterios de selección; el acceso prioritario no impedirá que otras pymes, incluidas las empresas emergentes, distintas de las mencionadas en el presente apartado accedan al espacio controlado de pruebas para la IA, siempre que también cumplan las condiciones de admisibilidad y los criterios de selección;

b) organizarán actividades de sensibilización y formación específicas sobre la aplicación del presente Reglamento adaptadas a las necesidades de las pymes, incluidas las empresas emergentes, los responsables del despliegue y, en su caso, las autoridades públicas locales;

c) utilizarán canales específicos existentes y establecerán, en su caso, nuevos canales para la comunicación con las pymes, incluidas las empresas emergentes, los responsables del despliegue y otros agentes innovadores, así como, en su caso, las autoridades públicas locales, a fin de proporcionar asesoramiento y responder a las dudas planteadas acerca de la aplicación del presente Reglamento, también en relación con la participación en los espacios controlados de pruebas para la IA;

d) fomentarán la participación de las pymes y otras partes interesadas pertinentes en el proceso de desarrollo de la normalización.

2. Se tendrán en cuenta los intereses y necesidades específicos de los proveedores que sean pymes, incluidas las empresas emergentes, a la hora de fijar las tasas para la evaluación de la conformidad en virtud del artículo 43, y se reducirán dichas tasas en proporción a su tamaño, al tamaño del mercado y a otros indicadores pertinentes.

3. La Oficina de IA adoptará las medidas siguientes:

a) proporcionará modelos normalizados para los ámbitos regulados por el presente Reglamento, tal como especifique el Consejo de IA en su solicitud;

b) desarrollará y mantendrá una plataforma única de información que proporcione información fácil de usar en relación con el presente Reglamento destinada a todos los operadores de la Unión;

c) organizará campañas de comunicación adecuadas para sensibilizar sobre las obligaciones derivadas del presente Reglamento;

d) evaluará y fomentará la convergencia de las mejores prácticas en los procedimientos de contratación pública en relación con los sistemas de IA.

ARTÍCULO 63
EXCEPCIONES PARA OPERADORES ESPECÍFICOS

1. Las pymes, incluidas las empresas emergentes, podrán cumplir determinados elementos del sistema de gestión de la calidad exigido por el artículo 17 del presente Reglamento de manera simplificada, siempre que no tengan empresas asociadas o empresas vinculadas en el sentido de la Recomendación 2003/361/CE. A tal fin, la Comisión elaborará directrices sobre los elementos del sistema de gestión de la calidad que puedan cumplirse de manera simplificada teniendo en cuenta las necesidades de las pymes sin que ello afecte al nivel de protección ni a la necesidad de cumplir los requisitos relativos a los sistemas de IA de alto riesgo.

2. El apartado 1 del presente artículo no se interpretará en el sentido de que exime a dichos operadores de cumplir cualquier otro requisito u obligación establecidos en el presente Reglamento, incluidos aquellos que figuran en los artículos 9, 10, 11, 12, 13, 14, 15, 72 y 73.

Fuente: Reglamento (UE) 2024/1689, texto consolidado a 27 de julio de 2026. Transcripción del PDF aportado; se han omitido las marcas editoriales de consolidación y las cabeceras de página.

Resumen del Capítulo VI — Medidas de apoyo a la innovación

Reglamento (UE) 2024/1689 · Texto consolidado a 27/07/2026 · Páginas 67–79 · Artículos 57 a 63, incluido el 60 bis

Este capítulo es especialmente interesante para las empresas tecnológicas, fabricantes de software, consultoras e integradores de inteligencia artificial.

Su objetivo es facilitar el desarrollo y la implantación de nuevas soluciones de IA, reduciendo las barreras regulatorias para innovar, especialmente para las pymes y las empresas emergentes.

El Reglamento reconoce que el cumplimiento normativo puede resultar complejo y costoso, por lo que establece mecanismos de apoyo, asesoramiento, experimentación y simplificación.

La principal novedad es la creación de **espacios controlados de pruebas de IA**, conocidos como *regulatory sandboxes*, donde las empresas pueden desarrollar y probar sistemas innovadores bajo supervisión de las autoridades.

1. Artículo 57. Espacios controlados de pruebas para IA

Páginas 67–70

Este artículo establece la creación de entornos supervisados que permiten desarrollar, entrenar, validar y probar sistemas innovadores de IA antes de comercializarlos.

Empresa desarrolla una solución innovadora de IA

Por ejemplo, un agente inteligente conectado a un ERP

Espacio controlado de pruebas

Desarrollo, experimentación y orientación de las autoridades competentes

Resultados y preparación para la comercialización

Informe de salida y documentación útil para acreditar el cumplimiento normativo

¿Qué ventajas ofrecen a las empresas?

Los participantes pueden recibir orientación sobre las obligaciones legales, identificar riesgos y probar las medidas destinadas a reducirlos.

Las autoridades facilitan además información sobre cómo cumplir los requisitos del Reglamento y pueden emitir documentación sobre las actividades realizadas y sus resultados.

Esa documentación puede utilizarse en los procedimientos posteriores de evaluación de conformidad, cuando corresponda.

¿Existen ventajas en materia de sanciones?

Sí, pero con condiciones importantes.

El artículo 57.12 establece que, si los proveedores potenciales respetan el plan de pruebas, cumplen las condiciones de participación y siguen de buena fe las orientaciones de las autoridades, no se impondrán multas administrativas por infracciones del Reglamento en esas circunstancias.

Sin embargo, esto **no elimina la responsabilidad por los daños causados a terceros** ni impide a las autoridades suspender las pruebas cuando existan riesgos importantes.

¿Cuándo deben estar disponibles?

02/08/2027

Fecha límite

Cada Estado miembro deberá asegurar la existencia de al menos un espacio controlado de pruebas de ámbito nacional, propio o compartido, con cobertura equivalente.

La modificación de 2026 también contempla la posibilidad de que la Oficina de IA establezca un espacio controlado a escala de la Unión para determinados sistemas, con acceso prioritario para pymes y empresas emergentes.

2. Artículo 58. Funcionamiento y acceso a los espacios controlados

Páginas 70–72

Este artículo regula cómo deben organizarse estos entornos de experimentación.

La Comisión Europea debe establecer criterios comunes para evitar diferencias innecesarias entre los Estados miembros.

Entre las condiciones que se recogen destacan:

Aspecto	Condición establecida
Acceso	Abierto a proveedores y proveedores potenciales que cumplan los requisitos.
Participación de pymes	Procedimientos simplificados y adaptados a su tamaño.
Coste	Acceso gratuito para pymes y empresas emergentes, salvo costes excepcionales recuperables de forma proporcionada.
Respuesta a solicitudes	Las autoridades deberán comunicar su decisión en un máximo de tres meses.
Duración	Limitada según la complejidad del proyecto, con posibilidad de prórroga.
Colaboración	Participación de empresas, universidades, laboratorios y otros agentes.
Supervisión	Orientación y vigilancia de las autoridades competentes.

Aplicación empresarial: una pequeña empresa de software podría solicitar participar para desarrollar una nueva aplicación de IA, comprobar sus requisitos regulatorios y preparar la documentación necesaria para comercializarla.

La participación no es automática: debe presentar una solicitud y cumplir los criterios establecidos.

3. Artículo 59. Utilización de datos personales en los espacios de pruebas

Páginas 72–74

Este artículo establece condiciones especiales para utilizar datos personales recogidos lícitamente con otros fines durante el desarrollo, entrenamiento y prueba de determinados sistemas de IA.

Es especialmente importante porque **no autoriza a las empresas a utilizar libremente cualquier base de datos para entrenar inteligencia artificial**.

El tratamiento excepcional solo se contempla cuando se cumplen todas las condiciones legales y el sistema pretende proteger un interés público esencial en alguno de los ámbitos establecidos.

Entre ellos se encuentran:

- Salud y seguridad públicas.
- Protección del medio ambiente y transición ecológica.
- Sostenibilidad energética.
- Seguridad del transporte, movilidad e infraestructuras críticas.
- Eficiencia y calidad de la Administración y los servicios públicos.

Además, deben garantizarse la necesidad del tratamiento, la protección de los datos, el aislamiento del entorno, la limitación de accesos, la eliminación de la información cuando corresponda y el respeto a los derechos de los interesados.

Ejemplo práctico

Una empresa que desarrolla IA para mejorar la detección de enfermedades podría, dentro de un espacio controlado y cumpliendo las condiciones del artículo, utilizar determinados datos personales que resulten imprescindibles para el proyecto.

En cambio, **una empresa que quiera utilizar toda la información personal de los clientes almacenada en su ERP para entrenar un asistente comercial no queda autorizada por este artículo**.

Para ello necesitaría cumplir las normas de protección de datos aplicables y disponer de una base jurídica válida.

4. Artículo 60. Pruebas de IA de alto riesgo en condiciones reales

Páginas 74–76

El Reglamento permite que determinados sistemas de IA de alto riesgo se prueben en entornos reales antes de su comercialización o puesta en servicio, incluso fuera de los espacios controlados.

Esto facilita verificar su funcionamiento en situaciones prácticas, más allá de los laboratorios o entornos simulados.

¿Qué condiciones deben cumplirse?

Requisito	Explicación
Plan de pruebas	Debe prepararse y presentarse a la autoridad competente.
Aprobación	Se requiere aprobación conforme al procedimiento previsto.
Registro	Deben cumplirse las obligaciones de registro aplicables.
Supervisión	La prueba debe contar con personas cualificadas y responsables.
Protección de datos	Deben respetarse las garantías legales pertinentes.
Consentimiento	Se requiere el consentimiento informado de los participantes, salvo la excepción legal específica.
Seguridad	Deben aplicarse medidas para evitar y reducir daños.
Gestión de incidentes	Es obligatorio comunicar incidentes graves y adoptar medidas correctoras.

Duración máxima de las pruebas

6 meses

Duración máxima inicial

+6 meses

Posible prórroga justificada

La duración deberá limitarse, en cualquier caso, a lo necesario para alcanzar los objetivos de la prueba.

Artículo 60 bis. Pruebas en sectores regulados

La modificación de 2026 incorpora este artículo.

Permite que los Estados miembros establezcan marcos para probar en condiciones reales determinados sistemas de IA de alto riesgo asociados a los productos regulados por la legislación sectorial enumerada en el anexo I, sección B.

Son pruebas sujetas a condiciones específicas, coordinación entre autoridades y garantías de protección de la salud, la seguridad y los derechos fundamentales.

5. Artículo 61. Consentimiento informado de los participantes

Páginas 77–78

Las personas que participan en las pruebas en condiciones reales del artículo 60 deben recibir información suficiente y prestar su consentimiento libre e informado, conforme a las reglas aplicables.

Deben conocer la finalidad de las pruebas, su duración, sus posibles inconvenientes y sus derechos.

El consentimiento debe estar documentado y fechado, y debe entregarse una copia a los participantes o a sus representantes legales.

También deben poder retirarse sin sufrir perjuicios y sin tener que justificar su decisión.

Aplicación empresarial: si una empresa prueba un sistema de IA de alto riesgo con personas reales, no basta con que el departamento técnico apruebe el proyecto. Deben cumplirse las garantías de participación y protección previstas.

6. Artículo 62. Medidas de apoyo para pymes y empresas emergentes

Páginas 78–79

Especialmente relevante para empresas de software

Este artículo establece medidas para que las pequeñas empresas puedan innovar sin soportar cargas regulatorias desproporcionadas.

Las principales son:

Medida	Beneficio para las empresas
Acceso prioritario a los espacios controlados	Facilita la experimentación y validación de soluciones innovadoras.
Formación específica	Ayuda a comprender las obligaciones legales de la IA.
Canales de asesoramiento	Permite plantear dudas a las autoridades competentes.
Participación en normalización	Favorece la intervención de pymes en el desarrollo de normas técnicas.
Reducción de tasas	Las tasas de evaluación de conformidad deben adaptarse proporcionalmente a las características de las pymes.
Plataforma informativa europea	Facilita el acceso a modelos, información y orientaciones sobre el Reglamento.

El apoyo no se limita exclusivamente a los fabricantes de modelos: también contempla medidas para los responsables del despliegue y otros agentes innovadores.

7. Artículo 63. Simplificación de obligaciones para determinados operadores

Página 79

Este artículo permite que determinadas pymes, incluidas empresas emergentes, cumplan de forma simplificada algunos elementos del sistema de gestión de calidad exigido por el artículo 17.

La redacción consolidada de 2026 establece condiciones, incluida la ausencia de empresas asociadas o vinculadas en el sentido de la normativa europea correspondiente.

¿Qué significa?

Una pyme que desarrolla sistemas de IA de alto riesgo puede beneficiarse de procedimientos de calidad menos complejos cuando cumpla los requisitos aplicables.

Sin embargo, **la simplificación no supone quedar exenta de cumplir las obligaciones esenciales**.

Se mantienen, entre otras, las exigencias sobre:

- Gestión de riesgos.
- Gobernanza de datos.
- Documentación técnica.
- Registros y trazabilidad.
- Transparencia y supervisión humana.
- Precisión, solidez y ciberseguridad.
- Vigilancia posterior e información sobre incidentes.

La intención es reducir la carga administrativa, no disminuir el nivel de protección.

8. ¿Qué oportunidades ofrece para la integración de IA en Sage 200?

El capítulo VI puede resultar especialmente interesante para empresas que desarrollen soluciones innovadoras alrededor de un ERP.

Proyecto de IA	Posible aplicación de las medidas
Asistente conectado a Sage 200 mediante API o MCP	Acceder a orientación regulatoria y, si cumple los criterios, participar en un espacio controlado.
IA para selección de personal	Probar un sistema potencialmente de alto riesgo con las garantías correspondientes.
Agente de IA para automatizar procesos empresariales	Recibir asesoramiento sobre la clasificación del sistema y sus obligaciones.
IA industrial conectada al ERP y a maquinaria	Evaluar los requisitos de seguridad y las posibilidades de pruebas supervisadas.
Sistema predictivo aplicado a servicios públicos	Valorar la participación en espacios controlados y las condiciones específicas sobre datos.
Desarrollo de soluciones verticales de IA por una pyme	Beneficiarse de las medidas de acceso, asesoramiento y simplificación previstas.

Son ejemplos de posibles aplicaciones, no una confirmación de admisión a un espacio controlado ni de la clasificación regulatoria de productos concretos.

Ejemplo: desarrollo de un agente conectado a Sage 200

Una empresa de software quiere desarrollar un agente que se conecte al ERP y permita consultar información, generar propuestas comerciales y ejecutar determinadas operaciones mediante APIs.

Podría analizar la posibilidad de participar en un espacio controlado para recibir orientación sobre las obligaciones del sistema, comprobar riesgos y documentar las medidas de control.

Si posteriormente ampliase la solución para evaluar candidatos o decidir promociones laborales, tendría que revisar su clasificación conforme al capítulo III.

El interés de los espacios controlados es precisamente ofrecer un entorno supervisado para analizar estas cuestiones antes de comercializar el sistema.

9. Calendario de aplicación

02/08/2026

Aplicable

Aplicación general del capítulo VI

Entrada en aplicación de sus disposiciones, con los plazos específicos establecidos.

02/08/2027

Previsto

Disponibilidad de espacios controlados nacionales

Fecha límite establecida en el artículo 57 para que los Estados miembros aseguren al menos un espacio controlado operativo de ámbito nacional.

10. Conclusión del capítulo VI

El capítulo VI demuestra que el Reglamento Europeo de Inteligencia Artificial no se centra únicamente en establecer restricciones y sanciones: también pretende facilitar el desarrollo tecnológico.

Sus principales aportaciones son **permitir la experimentación supervisada, ofrecer seguridad jurídica, facilitar las pruebas de sistemas innovadores y reducir las barreras para las pymes**.

Para el sector del software empresarial, el aspecto más interesante es que una empresa puede recibir orientación regulatoria durante el desarrollo de una solución de IA, antes de introducirla en el mercado.

Eso puede ser especialmente útil para proyectos de integración entre ERP, agentes inteligentes, aplicaciones de recursos humanos, software industrial y otros sistemas corporativos.

La conclusión esencial es que **la innovación y el cumplimiento normativo pueden desarrollarse conjuntamente**, aunque participar en un espacio controlado no equivale a obtener una autorización general para utilizar cualquier dato o tecnología.

Resumen basado en los artículos 57 a 63 del texto consolidado facilitado, incluida la modificación de 2026 y el nuevo artículo 60 bis.

CELEX_02024R1689-20260727_ES_TXT.pdf

TEXTO OFICIAL · CAPÍTULO VII

CAPÍTULO VII
GOBERNANZA

SECCIÓN 1
GOBERNANZA A ESCALA DE LA UNIÓN

ARTÍCULO 64
OFICINA DE IA

1. La Comisión desarrollará los conocimientos especializados y las capacidades de la Unión en el ámbito de la IA mediante la Oficina de IA.
2. Los Estados miembros facilitarán las tareas encomendadas a la Oficina de IA, que están reflejadas en el presente Reglamento.
3. Sin perjuicio del procedimiento presupuestario, se asignarán a la Oficina de IA los recursos adecuados para que pueda desempeñar eficazmente sus funciones y ejercer sus competencias en relación con ejecución del presente Reglamento.

ARTÍCULO 65
CREACIÓN Y ESTRUCTURA DEL CONSEJO EUROPEO DE INTELIGENCIA ARTIFICIAL

1. Se crea un Consejo Europeo de Inteligencia Artificial (en lo sucesivo, «Consejo de IA»).
2. El Consejo de IA estará compuesto de un representante por Estado miembro. El Supervisor Europeo de Protección de Datos participará en calidad de observador. La Oficina de IA también asistirá a las reuniones del Consejo de IA sin participar en las votaciones. El Consejo de IA podrá invitar a otras autoridades, organismos o expertos nacionales y de la Unión a las reuniones en función de cada situación concreta, cuando los temas tratados sean relevantes para ellos.
3. Cada representante será designado por su Estado miembro por un período de tres años, renovable una vez.
4. Los Estados miembros se asegurarán de que sus representantes en el Consejo de IA:
   a) tengan las competencias y los poderes pertinentes en su Estado miembro para poder contribuir activamente al cumplimiento de las funciones del Consejo de IA a que se refiere el artículo 66;
   b) sean designados como punto de contacto único respecto del Consejo de IA y, en su caso, teniendo en cuenta las necesidades de los Estados miembros, como punto de contacto único para las partes interesadas;
   c) estén facultados para facilitar la coherencia y la coordinación entre las autoridades nacionales competentes en su Estado miembro en relación con la aplicación del presente Reglamento, también mediante la recopilación de datos e información pertinentes para cumplir sus funciones en el Consejo de IA.
5. Los representantes designados de los Estados miembros adoptarán el Reglamento Interno del Consejo de IA por mayoría de dos tercios. El Reglamento Interno establecerá, en particular, los procedimientos para el proceso de selección, la duración del mandato y las especificaciones de las funciones de la presidencia, las modalidades de votación detalladas y la organización de las actividades del Consejo de IA y de sus subgrupos.
6. El Consejo de IA establecerá dos subgrupos permanentes a fin de proporcionar una plataforma de cooperación e intercambio entre las autoridades de vigilancia del mercado y de notificar a las autoridades cuestiones relacionadas con la vigilancia del mercado y los organismos notificados, respectivamente.

   El subgrupo permanente de vigilancia del mercado debe actuar como grupo de cooperación administrativa (ADCO) para el presente Reglamento en el sentido del artículo 30 del Reglamento (UE) 2019/1020.

   El Consejo de IA puede establecer otros subgrupos de carácter permanente o temporal, según proceda, para examinar asuntos específicos. Cuando proceda, se podrá invitar a representantes del foro consultivo a que se refiere el artículo 67 a dichos subgrupos o a reuniones específicas de dichos subgrupos en calidad de observadores.
7. El Consejo de IA se organizará y gestionará de manera que se preserve la objetividad e imparcialidad de sus actividades.
8. El Consejo de IA estará presidido por uno de los representantes de los Estados miembros. La Oficina de IA asumirá las labores de secretaría del Consejo de IA, convocará las reuniones a petición de la presidencia y elaborará el orden del día de conformidad con las funciones del Consejo de IA en virtud del presente Reglamento y de su Reglamento Interno.

ARTÍCULO 66
FUNCIONES DEL CONSEJO DE IA

El Consejo de IA prestará asesoramiento y asistencia a la Comisión y a los Estados miembros para facilitar la aplicación coherente y eficaz del presente Reglamento. A tal fin, el Consejo de IA podrá, en particular:

a) contribuir a la coordinación entre las autoridades nacionales competentes responsables de la aplicación del presente Reglamento y, en cooperación con las autoridades de vigilancia del mercado de que se trate y previo acuerdo de estas, apoyar las actividades conjuntas de las autoridades de vigilancia del mercado a que se refiere el artículo 74, apartado 11;

b) recopilar y compartir conocimientos técnicos y reglamentarios y mejores prácticas entre los Estados miembros;

c) ofrecer asesoramiento sobre la aplicación del presente Reglamento, en particular en lo relativo al cumplimiento de las normas sobre modelos de IA de uso general;

d) contribuir a la armonización de las prácticas administrativas en los Estados miembros, también en relación con la exención de los procedimientos de evaluación de la conformidad a que se refiere el artículo 46, el funcionamiento de los espacios controlados de pruebas para la IA y las pruebas en condiciones reales a que se refieren los artículos 57, 59 y 60;

e) previa solicitud de la Comisión o por iniciativa propia, emitir recomendaciones y dictámenes por escrito en relación con cualquier asunto pertinente relacionado con la ejecución del presente Reglamento y con su aplicación coherente y eficaz, por ejemplo:

   i) sobre la elaboración y aplicación de códigos de conducta y códigos de buenas prácticas con arreglo al presente Reglamento, así como de las directrices de la Comisión,

ii) sobre la evaluación y revisión del presente Reglamento con arreglo al artículo 112, también en lo que respecta a los informes de incidentes graves a que se refiere el artículo 73, y el funcionamiento de la base de datos de la UE a que se refiere el artículo 71, la preparación de los actos delegados o de ejecución, y en lo que respecta a las posibles adaptaciones del presente Reglamento a los actos legislativos de armonización de la Unión enumerados en el anexo I,

iii) sobre especificaciones técnicas o normas existentes relativas a los requisitos establecidos en el capítulo III, sección 2,

iv) sobre el uso de normas armonizadas o especificaciones comunes a que se refieren los artículos 40 y 41,

v) sobre tendencias, como la competitividad de Europa a escala mundial en materia de IA, la adopción de la IA en la Unión y el desarrollo de capacidades digitales,

vi) sobre tendencias en la tipología cambiante de las cadenas de valor de la IA, en particular sobre las implicaciones resultantes en términos de rendición de cuentas,

vii) sobre la posible necesidad de modificar el anexo III de conformidad con el artículo 7 y sobre la posible necesidad de revisar el artículo 5 con arreglo al artículo 112, teniendo en cuenta las pruebas disponibles pertinentes y los últimos avances tecnológicos;

f) apoyar a la Comisión en la promoción de la alfabetización en materia de IA, la sensibilización del público y la comprensión de las ventajas, los riesgos, las salvaguardias y los derechos y obligaciones en relación con la utilización de sistemas de IA;

g) facilitar el desarrollo de criterios comunes y la comprensión compartida entre los operadores del mercado y las autoridades competentes de los conceptos pertinentes previstos en el presente Reglamento, por ejemplo, contribuyendo al desarrollo de parámetros de referencia;

h) cooperar, en su caso, con otras instituciones, órganos y organismos de la Unión, así como con grupos de expertos y redes pertinentes de la Unión, en particular en los ámbitos de la seguridad de los productos, la ciberseguridad, la competencia, los servicios digitales y de medios de comunicación, los servicios financieros, la protección de los consumidores, y la protección de datos y de los derechos fundamentales;

i) contribuir a la cooperación efectiva con las autoridades competentes de terceros países y con organizaciones internacionales;

j) asistir a las autoridades nacionales competentes y a la Comisión en el desarrollo de los conocimientos técnicos y organizativos necesarios para la aplicación del presente Reglamento, por ejemplo, contribuyendo a la evaluación de las necesidades de formación del personal de los Estados miembros que participe en dicha aplicación;

k) asistir a la Oficina de IA en el apoyo a las autoridades nacionales competentes para el establecimiento y el desarrollo de espacios controlados de pruebas para la IA, y facilitar la cooperación y el intercambio de información entre espacios controlados de pruebas para la IA;

l) contribuir a la elaboración de documentos de orientación y proporcionar el asesoramiento pertinente al respecto;

m) proporcionar asesoramiento a la Comisión en relación con asuntos internacionales en materia de IA;

n) emitir dictámenes para la Comisión sobre las alertas cualificadas relativas a modelos de IA de uso general;

o) recibir dictámenes de los Estados miembros sobre alertas cualificadas relativas a modelos de IA de uso general y sobre las experiencias y prácticas nacionales en materia de supervisión y ejecución de los sistemas de IA, en particular los sistemas que integran los modelos de IA de uso general.

ARTÍCULO 67
FORO CONSULTIVO

1. Se creará un foro consultivo para proporcionar conocimientos técnicos y asesorar al Consejo de IA y a la Comisión, así como para contribuir a las funciones de estos en virtud del presente Reglamento.
2. La composición del foro consultivo representará una selección equilibrada de partes interesadas, incluidos la industria, las empresas emergentes, las pymes, la sociedad civil y el mundo académico. La composición del foro consultivo estará equilibrada en lo que respecta a los intereses comerciales y los no comerciales y, dentro de la categoría de los intereses comerciales, en lo que respecta a las pymes y otras empresas.
3. La Comisión nombrará a los miembros del foro consultivo, de conformidad con los criterios establecidos en el apartado 2, de entre las partes interesadas con conocimientos especializados reconocidos en el ámbito de la IA.
4. El mandato de los miembros del foro consultivo será de dos años y podrá prorrogarse hasta un máximo de cuatro años.
5. La Agencia de los Derechos Fundamentales de la Unión Europea, la Agencia de la Unión Europea para la Ciberseguridad, el Comité Europeo de Normalización (CEN), el Comité Europeo de Normalización Electrotécnica (Cenelec) y el Instituto Europeo de Normas de Telecomunicaciones (ETSI) serán miembros permanentes del foro consultivo.
6. El foro consultivo establecerá su reglamento interno. Elegirá dos copresidentes de entre sus miembros, de conformidad con los criterios establecidos en el apartado 2. El mandato de los copresidentes será de dos años, renovable una sola vez.
7. El foro consultivo celebrará reuniones al menos dos veces al año. Podrá invitar a expertos y otras partes interesadas a sus reuniones.
8. El foro consultivo podrá elaborar dictámenes, recomendaciones y contribuciones por escrito a petición del Consejo de IA o de la Comisión.
9. El foro consultivo podrá crear subgrupos permanentes o temporales, según proceda, para examinar cuestiones específicas relacionadas con los objetivos del presente Reglamento.
10. El foro consultivo redactará un informe anual de sus actividades. Dicho informe se pondrá a disposición del público.

ARTÍCULO 68
GRUPO DE EXPERTOS CIENTÍFICOS INDEPENDIENTES

1. La Comisión adoptará, mediante un acto de ejecución, disposiciones sobre la creación de un grupo de expertos científicos independientes (en lo sucesivo, «grupo de expertos científicos») destinado a apoyar las actividades de garantía del cumplimiento previstas en el presente Reglamento. Dicho acto de ejecución se adoptará de conformidad con el procedimiento de examen a que se refiere el artículo 98, apartado 2.
2. El grupo de expertos científicos estará compuesto por expertos seleccionados por la Comisión sobre la base de conocimientos científicos o técnicos actualizados en el ámbito de la IA necesarios para las funciones establecidas en el apartado 3, y será capaz de demostrar que cumple todas las condiciones siguientes:
   a) conocimientos especializados y competencias particulares, y conocimientos científicos o técnicos en el ámbito de la IA;
   b) independencia de cualquier proveedor de sistemas de IA o de modelos de IA de uso general;
   c) capacidad para llevar a cabo actividades con diligencia, precisión y objetividad.

   La Comisión, en consulta con el Consejo de IA, determinará el número de expertos del grupo de acuerdo con las necesidades requeridas y garantizará una representación geográfica y de género justa.
3. El grupo de expertos científicos asesorará y apoyará a la Oficina de IA, en particular en lo que respecta a las siguientes funciones:
   a) apoyar la aplicación y el cumplimiento del presente Reglamento en lo que respecta a los sistemas y modelos de IA de uso general, en particular:
      i) alertando a la Oficina de IA de los posibles riesgos sistémicos a escala de la Unión de modelos de IA de uso general, de conformidad con el artículo 90,
      ii) contribuyendo al desarrollo de herramientas y metodologías para evaluar las capacidades de los sistemas y modelos de IA de uso general, también a través de parámetros de referencia,
      iii) asesorando sobre la clasificación de modelos de IA de uso general con riesgo sistémico,
      iv) asesorando sobre la clasificación de diversos sistemas y modelos de IA de uso general,
      v) contribuyendo al desarrollo de herramientas y modelos;
   b) apoyar la labor de las autoridades de vigilancia del mercado, a petición de estas;
   c) apoyar las actividades transfronterizas de vigilancia del mercado a que se refiere el artículo 74, apartado 11, sin perjuicio de los poderes de las autoridades de vigilancia del mercado;
   d) apoyar a la Oficina de IA en el ejercicio de sus funciones en el contexto del procedimiento de salvaguardia de la Unión con arreglo al artículo 81.
4. Los expertos del grupo desempeñarán sus funciones con imparcialidad y objetividad y garantizarán la confidencialidad de la información y los datos obtenidos en el ejercicio de sus funciones y actividades. No solicitarán ni aceptarán instrucciones de nadie en el ejercicio de sus funciones previstas en el apartado 3. Cada experto cumplimentará una declaración de intereses que se hará pública. La Oficina de IA establecerá sistemas y procedimientos para gestionar y prevenir activamente los posibles conflictos de intereses.
5. El acto de ejecución a que se refiere el apartado 1 incluirá disposiciones sobre las condiciones, los procedimientos y las disposiciones detalladas para que el grupo de expertos científicos y sus miembros emitan alertas y soliciten la asistencia de la Oficina de IA para el desempeño de las funciones del grupo de expertos científicos.

ARTÍCULO 69
ACCESO A EXPERTOS POR PARTE DE LOS ESTADOS MIEMBROS

1. Los Estados miembros podrán recurrir a expertos del grupo de expertos científicos para que apoyen sus actividades de garantía del cumplimiento previstas en el presente Reglamento.
2. Se podrá exigir a los Estados miembros que paguen tasas por el asesoramiento y el apoyo prestado por los expertos, por un importe equivalente a los honorarios aplicables a la Comisión de conformidad con el acto de ejecución a que se refiere el artículo 68, apartado 1.
3. La Comisión facilitará el acceso oportuno de los Estados miembros a los expertos, según sea necesario, y garantizará que la combinación de las actividades de apoyo llevadas a cabo por las estructuras de apoyo a los ensayos de IA de la Unión con arreglo al artículo 84 y por expertos con arreglo al presente artículo se organice de manera eficiente y ofrezca el mayor valor añadido posible.

SECCIÓN 2
AUTORIDADES NACIONALES COMPETENTES

ARTÍCULO 70
DESIGNACIÓN DE LAS AUTORIDADES NACIONALES COMPETENTES Y DE LOS PUNTOS DE CONTACTO ÚNICO

1. Cada Estado miembro establecerá o designará al menos una autoridad notificante y al menos una autoridad de vigilancia del mercado como autoridades nacionales competentes a los efectos del presente Reglamento. Dichas autoridades nacionales competentes ejercerán sus poderes de manera independiente, imparcial y sin sesgos, a fin de preservar la objetividad de sus actividades y funciones y de garantizar la aplicación y ejecución del presente Reglamento. Los miembros de dichas autoridades se abstendrán de todo acto incompatible con sus funciones. Siempre que se respeten esos principios, tales actividades y funciones podrán ser realizadas por una o varias autoridades designadas, de conformidad con las necesidades organizativas del Estado miembro.
2. Los Estados miembros comunicarán a la Comisión la identidad de las autoridades notificantes y de las autoridades de vigilancia del mercado y las funciones de dichas autoridades, así como cualquier cambio posterior al respecto. Los Estados miembros pondrán a disposición del público, por medios de comunicación electrónica, información sobre la forma de contactar con las autoridades competentes y los puntos de contacto únicos a más tardar el 2 de agosto de 2025. Los Estados miembros designarán una autoridad de vigilancia del mercado que

actúe como punto de contacto único para el presente Reglamento y notificarán a la Comisión la identidad de dicho punto. La Comisión pondrá a disposición del público la lista de puntos de contacto únicos.

3. Los Estados miembros garantizarán que sus autoridades nacionales competentes dispongan de recursos técnicos, financieros y humanos adecuados, y de infraestructuras para el desempeño de sus funciones de manera efectiva con arreglo al presente Reglamento. En concreto, las autoridades nacionales competentes dispondrán permanentemente de suficiente personal cuyas competencias y conocimientos técnicos incluirán un conocimiento profundo de las tecnologías de IA, datos y computación de datos; la protección de los datos personales, la ciberseguridad, los riesgos para los derechos fundamentales, la salud y la seguridad, y conocimientos acerca de las normas y requisitos legales vigentes. Los Estados miembros evaluarán y, en caso necesario, actualizarán anualmente los requisitos en materia de competencias y recursos a que se refiere el presente apartado.
4. Las autoridades nacionales competentes adoptarán las medidas adecuadas para garantizar un nivel adecuado de ciberseguridad.
5. En el desempeño de sus funciones, las autoridades nacionales competentes actuarán de conformidad con las obligaciones de confidencialidad establecidas en el artículo 78.
6. A más tardar el 2 de agosto de 2025 y cada dos años a partir de entonces, los Estados miembros presentarán a la Comisión un informe acerca del estado de los recursos financieros y humanos de las autoridades nacionales competentes, que incluirá una evaluación de su idoneidad. La Comisión remitirá dicha información al Consejo de IA para que mantenga un debate sobre ella y, en su caso, formule recomendaciones.
7. La Comisión facilitará el intercambio de experiencias entre las autoridades nacionales competentes.
8. Las autoridades nacionales competentes podrán proporcionar orientaciones y asesoramiento sobre la aplicación del presente Reglamento, en particular a las pymes —incluidas las empresas emergentes— y las pequeñas empresas de mediana capitalización, teniendo en cuenta las orientaciones y el asesoramiento del Consejo de IA y de la Comisión, según proceda. Siempre que una autoridad nacional competente tenga la intención de proporcionar orientaciones y asesoramiento en relación con un sistema de IA en ámbitos regulados por otros actos del Derecho de la Unión, se consultará a las autoridades nacionales competentes con arreglo a lo dispuesto en dichos actos, según proceda.
9. Cuando las instituciones, órganos y organismos de la Unión entren en el ámbito de aplicación del presente Reglamento, el Supervisor Europeo de Protección de Datos actuará como autoridad competente para su supervisión.

Fuente: Reglamento (UE) 2024/1689, texto consolidado a 27 de julio de 2026. Transcripción del PDF aportado; se han omitido las marcas editoriales de consolidación y las cabeceras de página.

Resumen del Capítulo VII — Gobernanza de la inteligencia artificial

Reglamento (UE) 2024/1689 · Texto consolidado a 27/07/2026 · Páginas 79–86 · Artículos 64 a 70

Este capítulo establece **quién supervisa, coordina y controla la aplicación del Reglamento Europeo de Inteligencia Artificial**, tanto a escala de la Unión Europea como en cada Estado miembro.

Su objetivo es crear una estructura común que garantice que las normas sobre IA se apliquen de forma coherente en toda Europa.

Para las empresas, es importante porque identifica **qué organismos pueden supervisar sus sistemas, ofrecer orientación, comprobar el cumplimiento y participar en actuaciones de control**.

El capítulo se divide en dos secciones.

1. Estructura de gobernanza de la IA en Europa

Comisión Europea

Responsabilidad institucional de la aplicación del Reglamento

Oficina Europea de IA

Funciones técnicas, coordinación, seguimiento y competencias de supervisión atribuidas por el Reglamento

Consejo de IA

Coordinación de Estados

Foro consultivo

Industria y sociedad civil

Grupo científico

Expertos independientes

Autoridades nacionales competentes

Supervisión y vigilancia del mercado, con las competencias establecidas en el Reglamento

Esquema funcional simplificado. No representa una relación jerárquica entre todos los organismos: el Consejo, el Foro y el Grupo científico tienen funciones propias de asesoramiento y apoyo, mientras que las autoridades nacionales ejercen sus competencias con independencia.

2. Sección 1. Gobernanza a escala de la Unión Europea

Artículos 64 a 69 · Páginas 79–85

Artículo 64. Oficina Europea de Inteligencia Artificial

La Oficina de IA forma parte de la estructura de la Comisión Europea y contribuye al desarrollo de las capacidades de la Unión en materia de inteligencia artificial.

Desempeña las funciones que el Reglamento le atribuye, incluidas tareas de apoyo técnico y determinadas competencias de supervisión y ejecución desarrolladas en otros artículos.

La modificación de 2026 refuerza la previsión relativa a la asignación de recursos adecuados para que pueda desempeñar sus competencias.

Aplicación empresarial: la Oficina de IA es especialmente importante para proveedores de modelos de IA de uso general y en los supuestos en que el Reglamento le atribuye competencias directas de supervisión.

No significa que cualquier empresa que utilice IA tenga que registrarse directamente ante esta Oficina.

Artículo 65. Consejo Europeo de Inteligencia Artificial

El Consejo de IA es un organismo de coordinación compuesto por un representante de cada Estado miembro.

El Supervisor Europeo de Protección de Datos participa como observador y la Oficina de IA asiste a las reuniones sin voto.

Su finalidad es facilitar una aplicación homogénea del Reglamento en los distintos países.

Artículo 66. Funciones del Consejo de IA

El Consejo asesora a la Comisión y a los Estados miembros.

Sus principales funciones se pueden resumir así:

Función	Objetivo
Coordinación	Facilitar la colaboración entre autoridades nacionales.
Interpretación normativa	Favorecer una aplicación coherente del Reglamento.
Recomendaciones	Emitir dictámenes sobre la aplicación y revisión de las normas.
Supervisión técnica	Asesorar sobre requisitos, normas armonizadas y modelos de IA.
Apoyo a la innovación	Facilitar la coordinación de espacios controlados de pruebas.
Alfabetización	Apoyar la difusión de conocimientos sobre oportunidades, riesgos y obligaciones de IA.
Cooperación internacional	Facilitar relaciones con autoridades de terceros países y organizaciones internacionales.

Aplicación empresarial: el Consejo contribuye a que una empresa que comercializa una solución en España no se enfrente, en lo posible, a interpretaciones regulatorias radicalmente diferentes en otros Estados miembros.

El Consejo no sustituye a las autoridades nacionales en el ejercicio de sus competencias de inspección y supervisión.

Artículo 67. Foro consultivo

El Reglamento crea un foro consultivo destinado a aportar conocimientos especializados a la Comisión y al Consejo de IA.

Debe contar con una representación equilibrada de los distintos sectores implicados en el desarrollo y utilización de inteligencia artificial.

Participan representantes de la industria, pymes, empresas emergentes, sociedad civil y ámbito académico.

También se contemplan miembros permanentes de organismos europeos especializados en derechos fundamentales, ciberseguridad y normalización.

Aplicación empresarial: ofrece un mecanismo para que los intereses y necesidades de la industria y de las empresas pequeñas estén representados en las actividades de asesoramiento sobre el Reglamento.

No supone un derecho automático de participación individual de cualquier empresa.

Artículo 68. Grupo de expertos científicos independientes

La Comisión debe establecer un grupo de especialistas independientes para apoyar las actividades de cumplimiento del Reglamento.

Estos expertos deben reunir conocimientos científicos y técnicos actualizados, actuar objetivamente y mantener su independencia respecto de los proveedores de IA.

Entre sus funciones destacan la evaluación de las capacidades de los modelos, la identificación de riesgos sistémicos y el asesoramiento técnico a la Oficina de IA y a las autoridades competentes.

Ejemplo práctico: ante un modelo de IA especialmente avanzado que pueda presentar riesgos importantes, los expertos pueden contribuir a evaluar sus capacidades y detectar posibles riesgos sistémicos.

Artículo 69. Acceso a expertos por los Estados miembros

Los Estados miembros pueden recurrir a este grupo científico para apoyar sus actuaciones de aplicación y control del Reglamento.

La modificación de 2026 contempla expresamente la posibilidad de cobrar determinadas tasas por ese asesoramiento y apoyo.

Esto permite que las autoridades nacionales accedan a especialistas cuando necesiten conocimientos técnicos específicos para examinar un sistema de IA.

3. Sección 2. Autoridades nacionales competentes

Artículo 70 · Páginas 85–86

Este artículo tiene una repercusión directa en la supervisión empresarial.

Cada Estado miembro debe establecer o designar, como mínimo, una autoridad notificante y una autoridad de vigilancia del mercado.

Organismo	Responsabilidad
Autoridad notificante	Gestionar los procedimientos de evaluación, designación, notificación y supervisión de organismos de evaluación de conformidad.
Autoridad de vigilancia del mercado	Ejercer las funciones de vigilancia y control que le corresponden sobre los sistemas de IA.
Punto de contacto único	Facilitar un interlocutor nacional para las cuestiones relacionadas con el Reglamento.

Las autoridades deben actuar con independencia, imparcialidad y objetividad.

También deben contar con personal cualificado, recursos técnicos y económicos suficientes y conocimientos sobre IA, ciberseguridad, protección de datos y derechos fundamentales.

¿Qué significa para las empresas españolas?

Las empresas que desarrollen, distribuyan o utilicen sistemas de IA deberán atender, cuando corresponda, los requerimientos de las autoridades competentes.

Estas podrán ejercer las facultades de supervisión, investigación o control que se les atribuyan en las disposiciones aplicables.

Además, el artículo 70.8 contempla que las autoridades nacionales puedan ofrecer orientación y asesoramiento, especialmente a pymes y empresas emergentes.

Importante: el capítulo VII define la estructura de autoridades, pero no identifica por su nombre qué organismos concretos ejercen todas estas funciones en España. Esa designación debe verificarse en la normativa y los actos nacionales correspondientes.

4. ¿Cómo afecta este capítulo a las empresas?

A diferencia de los capítulos III, IV y V, el capítulo VII se centra fundamentalmente en organizar a las autoridades y los órganos de coordinación.

Sus implicaciones empresariales son sobre todo indirectas, aunque importantes.

Situación empresarial	Implicación
Desarrollar un sistema de IA de alto riesgo	Puede estar sujeto a supervisión y a los procedimientos de conformidad aplicables.
Comercializar IA en varios países europeos	Se busca una interpretación y supervisión coordinadas.
Utilizar un sistema de IA de alto riesgo	La empresa debe colaborar con las autoridades cuando lo exijan las normas aplicables.
Detectar un problema grave en una solución de IA	Deben seguirse los procedimientos de comunicación y corrección correspondientes.
Desarrollar una solución novedosa siendo pyme	Puede beneficiarse de orientación y asesoramiento de las autoridades competentes.

5. ¿Qué supone para Sage 200 y sus integraciones con IA?

En un proyecto de integración de IA con Sage 200 es importante identificar el papel que desempeña cada participante.

Empresa que desarrolla el conector o agente de IA

Debe analizar si actúa como proveedor de un sistema de IA, qué clasificación corresponde a la solución y qué obligaciones le resultan aplicables.

El capítulo VII identifica la estructura de supervisión con la que puede tener que relacionarse.

Empresa cliente que utiliza la solución

Si el sistema está sujeto a obligaciones específicas, deberá estar preparada para atender los requerimientos de información y colaborar con las autoridades cuando corresponda.

Autoridad competente

Ejerce las funciones que le atribuya la normativa, incluyendo, según el caso, vigilancia del mercado, comprobación del cumplimiento y actuaciones de supervisión.

Ejemplo práctico

Una empresa desarrolla un sistema de IA conectado a Sage 200 que evalúa automáticamente el rendimiento de los trabajadores y recomienda decisiones relacionadas con promociones laborales.

Si el sistema se clasifica como de alto riesgo, las obligaciones técnicas y de utilización se determinarán principalmente por el capítulo III.

El capítulo VII establece la estructura institucional para su supervisión, mientras que los poderes concretos de inspección, vigilancia y ejecución se desarrollan especialmente en el capítulo IX.

6. Calendario de aplicación

02/08/2025

Aplicable

El capítulo VII es aplicable desde el 2 de agosto de 2025, de conformidad con el artículo 113 del Reglamento.

Esta fecha no implica que todas las obligaciones correspondientes a los sistemas de IA de alto riesgo fueran exigibles desde ese momento. Esas obligaciones disponen de su propio calendario de aplicación.

7. Conclusión del capítulo VII

El capítulo VII crea el sistema de gobernanza de la inteligencia artificial en Europa.

Su finalidad es garantizar que el Reglamento no sea simplemente una declaración de principios, sino que exista una estructura institucional capaz de coordinar su aplicación, proporcionar conocimientos especializados y supervisar su cumplimiento.

Para las empresas, lo más importante es entender que **el cumplimiento de la normativa sobre IA puede ser supervisado por autoridades públicas competentes, con funciones y responsabilidades específicas**.

El capítulo no impone, por sí solo, una obligación general de registrar cualquier chatbot, automatización o integración con un ERP.

Su principal aportación es establecer quién coordina y supervisa el marco europeo de IA.

El siguiente capítulo, el VIII, desarrolla una cuestión especialmente relacionada: **la base de datos europea para registrar determinados sistemas de IA de alto riesgo**, que permitirá identificar y consultar información sobre esos sistemas.

Resumen elaborado a partir de los artículos 64 a 70 del texto consolidado aportado, incluida la modificación de 2026.

CELEX_02024R1689-20260727_ES_TXT.pdf

TEXTO OFICIAL · CAPÍTULO VIII

CAPÍTULO VIII
BASE DE DATOS DE LA UE PARA SISTEMAS DE IA DE ALTO RIESGO

ARTÍCULO 71
BASE DE DATOS DE LA UE PARA LOS SISTEMAS DE IA DE ALTO RIESGO ENUMERADOS EN EL ANEXO III

1. La Comisión, en colaboración con los Estados miembros, creará y mantendrá una base de datos de la UE que contendrá la información mencionada en los apartados 2 y 3 del presente artículo en relación con los sistemas de IA de alto riesgo a que se refiere el artículo 6, apartado 2, que estén registrados con arreglo a los artículos 49 y 60 y los sistemas de IA que no se consideren de alto riesgo en virtud del artículo 6, apartado 3, y que estén registrados con arreglo al artículo 6, apartado 4, y al artículo 49. La Comisión consultará a los expertos pertinentes a la hora de fijar las especificaciones funcionales de dicha base de datos y al Consejo de IA a la hora de actualizarlas.
2. Los datos enumerados en el anexo VIII, secciones A y B, serán introducidos en la base de datos de la UE por el proveedor o, en su caso, por el representante autorizado.
3. Los datos enumerados en el anexo VIII, sección C, serán introducidos en la base de datos de la UE por el responsable del despliegue que sea una autoridad pública, órgano u organismo, o actúe en su nombre, de conformidad con el artículo 49, apartados 3 y 4.
4. A excepción de la sección a que se refieren el artículo 49, apartado 4, y el artículo 60, apartado 4, letra c), la información presente en la base de datos de la UE y registrada de conformidad con lo dispuesto en el artículo 49 será accesible y estará a disposición del público de manera sencilla. Debe ser fácil navegar por la información y esta ha de ser legible por máquina. Únicamente podrán acceder a la información registrada de conformidad con el artículo 60 las autoridades de vigilancia de mercado y la Comisión, a menos que el proveedor potencial o el proveedor hayan dado su consentimiento a que la información también esté accesible para el público.
5. La base de datos de la UE únicamente contendrá datos personales en la medida en que sean necesarios para la recogida y el tratamiento de información de conformidad con el presente Reglamento. Dicha información incluirá los nombres y datos de contacto de las personas físicas responsables del registro de sistema y que cuenten con autoridad legal para representar al proveedor o al responsable del despliegue, según proceda.
6. La Comisión será la responsable del tratamiento de la base de datos de la UE, y proporcionará apoyo técnico y administrativo adecuado a los proveedores, proveedores potenciales y responsables del despliegue. La base de datos de la UE cumplirá los requisitos de accesibilidad aplicables.

Fuente: Reglamento (UE) 2024/1689, texto consolidado a 27 de julio de 2026. Transcripción del PDF aportado; se han omitido las marcas editoriales de consolidación y las cabeceras de página.

Resumen del Capítulo VIII — Base de datos europea de sistemas de IA de alto riesgo

Reglamento (UE) 2024/1689 · Texto consolidado a 27/07/2026 · Páginas 86–87 · Artículo 71

Este capítulo establece la creación de una **base de datos oficial de la Unión Europea para registrar determinados sistemas de inteligencia artificial de alto riesgo**.

Su finalidad es mejorar la transparencia, facilitar la supervisión por las autoridades y permitir que ciudadanos y empresas puedan consultar información sobre determinados sistemas de IA comercializados o utilizados en Europa.

La idea principal: no todas las herramientas de inteligencia artificial deben registrarse. La obligación afecta a las categorías y operadores expresamente previstos en el Reglamento.

El capítulo contiene un único artículo: el **artículo 71**.

1. Artículo 71. Base de datos europea de sistemas de IA de alto riesgo

La Comisión Europea, en colaboración con los Estados miembros, es responsable de crear y mantener esta base de datos.

El registro está vinculado principalmente a los sistemas identificados en el **anexo III**, entre los que se encuentran determinadas aplicaciones de IA para recursos humanos, educación, biometría, servicios esenciales y otras actividades especialmente sensibles.

Su objetivo no es recopilar todos los programas que incorporan IA, sino disponer de información identificativa y de supervisión sobre los sistemas sujetos a registro.

2. ¿Qué sistemas deben registrarse?

Categoría	¿Qué establece el Reglamento?
Sistemas de alto riesgo del anexo III	Registro europeo conforme al artículo 49, con las excepciones establecidas.
Sistemas del anexo III que el proveedor considera no sujetos a la clasificación de alto riesgo por el artículo 6.3	También deben registrarse, indicando la justificación correspondiente.
Sistemas de alto riesgo de infraestructuras críticas del anexo III, punto 2	Registro a nivel nacional, conforme al artículo 49.5.
Determinados sistemas policiales, migratorios o de control fronterizo	Registro en una sección segura no pública.
Determinadas pruebas de sistemas de alto riesgo en condiciones reales	Registro de la información correspondiente, con acceso restringido como regla general.

¿Por qué se registran sistemas que no se consideran de alto riesgo?

El artículo 6 permite que ciertos sistemas incluidos inicialmente en los ámbitos del anexo III no se clasifiquen como de alto riesgo cuando cumplen condiciones específicas.

Sin embargo, el proveedor debe documentar esa evaluación y registrar el sistema.

De esta manera, las autoridades pueden conocer qué sistemas se han acogido a esa excepción y comprobar, cuando proceda, si la clasificación está justificada.

3. ¿Quién tiene que realizar el registro?

El Reglamento distingue entre proveedores y responsables del despliegue.

Responsable	Obligación
Proveedor del sistema de IA	Registrar el sistema y sus datos identificativos cuando corresponda.
Representante autorizado	Puede efectuar el registro en los supuestos previstos.
Administración pública que utiliza un sistema de alto riesgo del anexo III	Registrar su condición de responsable del despliegue y la utilización del sistema, con las excepciones legales.
Empresa privada que utiliza un sistema de alto riesgo	No queda obligada automáticamente a efectuar el registro como responsable del despliegue por el mero hecho de utilizarlo.

Ejemplo empresarial

Una empresa desarrolla y comercializa una solución de IA para seleccionar candidatos en procesos de contratación.

Si la solución se clasifica como sistema de alto riesgo del anexo III, su proveedor deberá cumplir la obligación de registro correspondiente.

Si una empresa privada compra y utiliza esa solución, no tendrá necesariamente que realizar una inscripción adicional como responsable del despliegue, aunque sí estará sujeta a las obligaciones de uso que le correspondan conforme al capítulo III.

4. ¿Qué información debe incluir el registro?

El artículo 71 remite al **anexo VIII**, que establece los datos que deben facilitar los participantes.

Entre ellos se encuentran:

Información	Contenido
Identificación del proveedor	Nombre, dirección y datos de contacto.
Identificación del sistema	Nombre comercial y referencias que permitan reconocerlo.
Finalidad prevista	Para qué se ha diseñado el sistema y qué funciones realiza.
Funcionamiento general	Descripción de los datos utilizados y de su lógica de funcionamiento, cuando corresponda.
Estado del sistema	Si está comercializado, en servicio, retirado o ha dejado de utilizarse.
Certificados	Información sobre los certificados de conformidad, cuando proceda.
Declaración UE de conformidad	Copia de la declaración exigida al proveedor.
Instrucciones de uso	Documentación electrónica, con las excepciones establecidas.
Países de comercialización	Estados miembros en los que se ha introducido o comercializado el sistema.

Para determinados responsables públicos del despliegue, el anexo VIII también contempla información sobre la utilización del sistema y, cuando proceda, resúmenes de evaluaciones de impacto.

Importante: el registro no implica publicar todo el código fuente, todos los datos de entrenamiento ni los secretos comerciales de cada sistema.

5. ¿La base de datos será pública?

Punto fundamental

El artículo 71 establece que gran parte de la información registrada será pública y deberá poder consultarse fácilmente, con datos accesibles y legibles por máquina.

Pero existen excepciones.

Información pública

Los registros ordinarios a los que se refiere el artículo 49 estarán disponibles públicamente, salvo las excepciones establecidas.

Información restringida

Los registros correspondientes a determinados sistemas de seguridad, garantía del cumplimiento del Derecho, migración, asilo y control fronterizo se incorporan a una sección protegida, accesible únicamente a las autoridades autorizadas.

Pruebas en condiciones reales

La información registrada conforme al artículo 60 está reservada a las autoridades de vigilancia del mercado y a la Comisión, salvo que el proveedor consienta su acceso público.

La Comisión será responsable del tratamiento de los datos de la base europea, que deberá cumplir los requisitos de accesibilidad y limitar los datos personales a los necesarios para sus finalidades.

6. ¿Qué supone este capítulo para Sage 200 y otros ERP?

La clave está en distinguir entre una funcionalidad ordinaria de IA y un sistema sujeto a registro conforme al anexo III.

Aplicación de IA	¿Registro europeo obligatorio?
OCR inteligente de facturas	No por esta funcionalidad ordinaria.
Conciliación bancaria mediante IA	No por su mera utilización.
Previsión de tesorería y ventas	No por estas funciones.
Asistente de IA conectado a Sage 200 por API o MCP	No por el simple hecho de realizar consultas al ERP.
IA para selección y evaluación de candidatos	Potencialmente sí, si se clasifica como sistema de alto riesgo del anexo III.
IA para evaluar el rendimiento y las promociones de trabajadores	Potencialmente sí, según su finalidad y clasificación.
IA para evaluar la solvencia de personas físicas	Potencialmente sí, conforme a la categoría del anexo III y sus excepciones.

La clasificación definitiva requiere analizar la funcionalidad concreta y las condiciones del artículo 6. Estos ejemplos no representan una evaluación oficial de productos Sage.

Ejemplo práctico

Imaginemos que se desarrollan dos soluciones conectadas a Sage 200.

Solución A: agente financiero. Consulta saldos, identifica facturas vencidas y genera previsiones de cobro. Por estas funciones, no se identifica una obligación de registro en la base europea del artículo 71.

Solución B: agente de recursos humanos. Analiza datos de candidatos y recomienda a quién contratar. Dependiendo de su clasificación, podría estar sujeto a las obligaciones de los sistemas de alto riesgo, incluido su registro.

La diferencia no está en la tecnología empleada, sino en **la finalidad y el impacto del sistema sobre las personas**.

7. ¿Cuándo es aplicable?

02/08/2026

Aplicable

El capítulo VIII se encuentra dentro de las disposiciones de aplicación general desde el 2 de agosto de 2026, conforme al artículo 113 del texto consolidado.

Debe tenerse en cuenta que el calendario de las obligaciones materiales de los sistemas de alto riesgo es distinto según su categoría, y existen disposiciones transitorias para determinados sistemas.

8. Conclusión del capítulo VIII

El capítulo VIII establece un mecanismo de identificación y transparencia de determinados sistemas de IA de alto riesgo.

Para las empresas, sus principales consecuencias son conocer qué aplicaciones están sujetas a inscripción, distinguir las obligaciones del proveedor y de los responsables públicos del despliegue, y facilitar que las autoridades y, en ciertos casos, los ciudadanos puedan consultar información sobre esos sistemas.

Lo más importante para el entorno ERP: una empresa no tiene que registrar todas sus automatizaciones, asistentes de IA ni funcionalidades inteligentes por el mero hecho de incorporarlas a su software.

El registro se exige cuando concurren las condiciones previstas en el Reglamento, especialmente en relación con los sistemas del anexo III.

El siguiente capítulo, el IX, desarrolla una cuestión directamente relacionada: **qué controles deben realizarse después de comercializar los sistemas de IA, cómo se comunican los incidentes graves y qué facultades tienen las autoridades para supervisar el mercado**.

TEXTO OFICIAL · CAPÍTULO IX

CAPÍTULO IX
VIGILANCIA POSCOMERCIALIZACIÓN, INTERCAMBIO DE INFORMACIÓN Y VIGILANCIA DEL MERCADO

SECCIÓN 1
VIGILANCIA POSCOMERCIALIZACIÓN

ARTÍCULO 72
VIGILANCIA POSCOMERCIALIZACIÓN POR PARTE DE LOS PROVEEDORES Y PLAN DE VIGILANCIA POSCOMERCIALIZACIÓN PARA SISTEMAS DE IA DE ALTO RIESGO

1. Los proveedores establecerán y documentarán un sistema de vigilancia poscomercialización de forma proporcionada a la naturaleza de las tecnologías de IA y a los riesgos de los sistemas de IA de alto riesgo.
2. El sistema de vigilancia poscomercialización recopilará, documentará y analizará de manera activa y sistemática los datos pertinentes que pueden facilitar los responsables del despliegue o que pueden recopilarse a través de otras fuentes sobre el funcionamiento de los sistemas de IA de alto riesgo durante toda su vida útil, y que permiten al proveedor evaluar el cumplimiento permanente de los requisitos establecidos en el capítulo III, sección 2, por parte de los sistemas de IA. Cuando proceda, la vigilancia poscomercialización incluirá un análisis de la interacción con otros sistemas de IA. Esta obligación no comprenderá los datos operativos sensibles de los responsables del despliegue que sean autoridades garantes del cumplimiento del Derecho.
3. El sistema de vigilancia poscomercialización se basará en un plan de vigilancia poscomercialización. El plan de vigilancia poscomercialización formará parte de la documentación técnica a que se refiere el anexo IV. La Comisión, teniendo en cuenta en la mayor medida posible el dictamen del Consejo de IA, adoptará orientaciones —que incluirán un modelo— sobre el plan de seguimiento poscomercialización a más tardar el 2 de septiembre de 2027.
4. En el caso de los sistemas de IA de alto riesgo regulados por los actos legislativos de armonización de la Unión enumerados en el anexo I, sección A, cuando ya se hayan establecido un sistema y un plan de vigilancia poscomercialización con arreglo a dichos actos, con el fin de garantizar la coherencia, evitar duplicidades y reducir al mínimo las cargas adicionales, los proveedores podrán optar por integrar, según proceda, los elementos necesarios descritos en los apartados 1, 2 y 3, utilizando el modelo a que se refiere el apartado 3, en los sistemas y planes que ya existan en virtud de dicha legislación, siempre que alcance un nivel de protección equivalente.

El párrafo primero del presente apartado también se aplicará a los sistemas de IA de alto riesgo a que se refiere el anexo III, punto 5, introducidos en el mercado o puestos en servicio por entidades financieras sujetas a requisitos relativos a su gobernanza, sus sistemas o sus procesos internos en virtud del Derecho de la Unión en materia de servicios financieros.

SECCIÓN 2
INTERCAMBIO DE INFORMACIÓN SOBRE INCIDENTES GRAVES

ARTÍCULO 73
NOTIFICACIÓN DE INCIDENTES GRAVES

1. Los proveedores de sistemas de IA de alto riesgo introducidos en el mercado de la Unión notificarán cualquier incidente grave a las autoridades de vigilancia del mercado de los Estados miembros en los que se haya producido dicho incidente.
2. La notificación a que se refiere el apartado 1 se efectuará inmediatamente después de que el proveedor haya establecido un vínculo causal entre el sistema de IA y el incidente grave o la probabilidad razonable de que exista dicho vínculo y, en cualquier caso, a más tardar quince días después de que el proveedor o, en su caso, el responsable del despliegue, tengan conocimiento del incidente grave.

El plazo para la notificación a que se refiere el párrafo primero tendrá en cuenta la magnitud del incidente grave.

3. No obstante lo dispuesto en el apartado 2 del presente artículo, en caso de una infracción generalizada o de un incidente grave tal como se define en el artículo 3, punto 49, letra b), la notificación a que se refiere el apartado 1 del presente artículo se realizará de manera inmediata y a más tardar dos días después de que el proveedor o, en su caso, el responsable del despliegue tenga conocimiento del incidente.
4. No obstante lo dispuesto en el apartado 2, en caso de fallecimiento de una persona, la notificación se efectuará de manera inmediata después de que el proveedor o el responsable del despliegue haya establecido —o tan pronto como sospeche— una relación causal entre el sistema de IA de alto riesgo y el incidente grave, en un plazo no superior a diez días a contar de la fecha en la que el proveedor o, en su caso, el responsable del despliegue tenga conocimiento del incidente grave.
5. Cuando sea necesario para garantizar la notificación en tiempo oportuno, el proveedor o, en su caso, el responsable del despliegue podrá presentar inicialmente una notificación incompleta, seguida de una notificación completa.
6. Después de notificar un incidente grave con arreglo al apartado 1, el proveedor realizará sin demora las investigaciones necesarias en relación con el incidente grave y el sistema de IA afectado. Esto incluirá una evaluación de riesgos del incidente y las medidas correctoras.

El proveedor cooperará con las autoridades competentes y, en su caso, con el organismo notificado afectado durante las investigaciones a que se refiere el párrafo primero, y no emprenderá acción alguna que suponga la modificación del sistema de IA afectado de un modo que pueda repercutir en cualquier evaluación posterior de las causas del incidente sin haber informado antes de dicha acción a las autoridades competentes.

7. Tras la recepción de una notificación relativa a un incidente grave a que se refiere el artículo 3, punto 49, letra c), la autoridad de vigilancia del mercado pertinente informará a las autoridades u organismos públicos nacionales a que se refiere el artículo 77, apartado 1. La Comisión elaborará orientaciones específicas para facilitar el cumplimiento de

las obligaciones establecidas en el apartado 1 del presente artículo. Dichas orientaciones se publicarán a más tardar el 2 de agosto de 2025 y se evaluarán periódicamente.

8. La autoridad de vigilancia del mercado adoptará medidas adecuadas tal como se establece en el artículo 19 del Reglamento (UE) 2019/1020, en un plazo de siete días a partir de la fecha en que reciba la notificación a que se refiere el apartado 1 del presente artículo, y seguirá los procedimientos de notificación previstos en dicho Reglamento.

9. En el caso de los sistemas de IA de alto riesgo a que se refiere el anexo III, introducidos en el mercado o puestos en servicio por proveedores que estén sujetos a instrumentos legislativos de la Unión por los que se establezcan obligaciones de información equivalentes a las establecidas en el presente Reglamento, la notificación de incidentes graves se limitará a los mencionados en el artículo 3, punto 49, letra c).

10. En el caso de los sistemas de IA de alto riesgo que sean componentes de seguridad de dispositivos, o que en sí mismos sean dispositivos, regulados por los Reglamento (UE) 2017/745 y (UE) 2017/746, la notificación de incidentes graves se limitará a los mencionados en el artículo 3, punto 49, letra c), del presente Reglamento, y se hará a la autoridad nacional competente elegida para tal fin por los Estados miembros en los que se haya producido el incidente.

11. Las autoridades nacionales competentes informarán de inmediato a la Comisión de todo incidente grave, independientemente de han adoptado medidas al respecto, de conformidad con el artículo 20 del Reglamento (UE) 2019/1020.

SECCIÓN 3
GARANTÍA DEL CUMPLIMIENTO

ARTÍCULO 74
VIGILANCIA DEL MERCADO Y CONTROL DE LOS SISTEMAS DE IA EN EL MERCADO DE LA UNIÓN

1. El Reglamento (UE) 2019/1020 se aplicará a los sistemas de IA regulados por el presente Reglamento. A efectos de garantía del cumplimiento efectivo del presente Reglamento:

   a) se entenderá que toda referencia a un operador económico con arreglo al Reglamento (UE) 2019/1020 incluye a todos los operadores mencionados en el artículo 2, apartado 1, del presente Reglamento;

   b) se entenderá que toda referencia a un producto con arreglo al Reglamento (UE) 2019/1020 incluye todos los sistemas de IA que estén comprendidos en el ámbito de aplicación del presente Reglamento.

2. Como parte de sus obligaciones de presentación de información en virtud del artículo 34, apartado 4, del Reglamento (UE) 2019/1020, las autoridades de vigilancia del mercado informarán anualmente a la Comisión y a las autoridades nacionales de competencia pertinentes de cualquier información recabada en el transcurso de las actividades de vigilancia del mercado que pueda ser de interés potencial para la aplicación del Derecho de la Unión en materia de normas de competencia. Asimismo, informarán anualmente a la Comisión sobre el recurso a prácticas prohibidas que se hayan producido durante ese año y sobre las medidas adoptadas.

3. En el caso de los sistemas de IA de alto riesgo asociados a productos regulados por los actos legislativos de armonización de la Unión enumerados en el anexo I, sección A, la autoridad de vigilancia del mercado a efectos del presente Reglamento será la autoridad responsable de las actividades de vigilancia del mercado designada en virtud de dichos actos legislativos.

Como excepción a lo dispuesto en el párrafo primero, en circunstancias adecuadas, los Estados miembros podrán designar otra autoridad pertinente como autoridad de vigilancia del mercado, siempre que se garantice la coordinación con las autoridades sectoriales de vigilancia del mercado pertinentes responsables de la ejecución de los actos legislativos de armonización de la Unión enumerados en el anexo I.

4. Los procedimientos a que se refieren los artículos 79 a 83 del presente Reglamento no se aplicarán a los sistemas de IA asociados a productos regulados por los actos legislativos de armonización de la Unión enumerados en el anexo I, sección A, cuando dichos actos legislativos ya prevean procedimientos que garanticen un nivel equivalente de protección que tengan el mismo objetivo. En dichos casos, se aplicarán los procedimientos sectoriales pertinentes.

5. Sin perjuicio de los poderes de las autoridades de vigilancia del mercado en virtud del artículo 14 del Reglamento (UE) 2019/1020, a efectos de garantizar la ejecución efectiva del presente Reglamento, las autoridades de vigilancia del mercado podrán ejercer a distancia los poderes a que se refiere el artículo 14, apartado 4, letras d) y j), de dicho Reglamento, según proceda.

6. En el caso de los sistemas de IA de alto riesgo introducidos en el mercado, puestos en servicio o utilizados por entidades financieras reguladas por el Derecho de la Unión en materia de servicios financieros, la autoridad de vigilancia del mercado a efectos del presente Reglamento será la autoridad nacional pertinente responsable de la supervisión financiera de dichas entidades con arreglo a la mencionada legislación, en la medida en que la introducción en el mercado, la puesta en servicio o la utilización del sistema de IA esté directamente relacionada con la prestación de dichos servicios financieros.

7. Como excepción a lo dispuesto en el apartado 6, en las circunstancias apropiadas y siempre que se garantice la coordinación, el Estado miembro podrá designar otra autoridad pertinente como autoridad de vigilancia del mercado a efectos del presente Reglamento.

Las autoridades nacionales de vigilancia del mercado que supervisen las entidades de crédito reguladas por la Directiva 2013/36/UE y que participen en el Mecanismo Único de Supervisión establecido por el Reglamento (UE) n. o 1024/2013 deberán comunicar sin demora al Banco Central Europeo toda información obtenida en el transcurso de sus actividades de vigilancia del mercado que pueda ser de interés para las funciones de supervisión prudencial del Banco Central Europeo especificadas en dicho Reglamento.

8. En el caso de los sistemas de IA de alto riesgo enumerados en el anexo III del presente Reglamento, punto 1, en la medida en que los sistemas se utilicen a los efectos de la garantía del cumplimiento del Derecho, la gestión de fronteras y la justicia y la democracia, y en el caso de los sistemas de IA de alto riesgo enumerados en el anexo III, puntos 6, 7 y 8, del presente Reglamento, los Estados

miembros designarán como autoridades de vigilancia del mercado a efectos del presente Reglamento bien a las autoridades de control encargadas de la protección de datos competentes con arreglo al Reglamento (UE) 2016/679 o a la Directiva (UE) 2016/680, bien a cualquier otra autoridad designada con arreglo a las mismas condiciones establecidas en los artículos 41 a 44 de la Directiva (UE) 2016/680. Las actividades de vigilancia del mercado no afectarán en modo alguno a la independencia de las autoridades judiciales ni interferirán de otro modo en sus actividades en el ejercicio de su función judicial.

9. Cuando las instituciones, órganos y organismos de la Unión entren en el ámbito de aplicación del presente Reglamento, el Supervisor Europeo de Protección de Datos actuará como su autoridad de vigilancia del mercado, salvo en relación con el Tribunal de Justicia de la Unión Europea cuando actúe en el ejercicio de su función judicial.

10. Los Estados miembros facilitarán la coordinación entre las autoridades de vigilancia del mercado designadas con arreglo al presente Reglamento y otras autoridades u organismos nacionales pertinentes responsables de supervisar la aplicación de la legislación de armonización de la Unión indicada en el anexo I o en otras disposiciones de Derecho de la Unión que pudieran resultar pertinente para los sistemas de IA de alto riesgo a que se refiere el anexo III.

11. Las autoridades de vigilancia del mercado y la Comisión podrán proponer actividades conjuntas, incluidas investigaciones conjuntas, que deben llevar a cabo bien las autoridades de vigilancia del mercado, bien las autoridades de vigilancia del mercado junto con la Comisión, con el objetivo de fomentar el cumplimiento, detectar incumplimientos, sensibilizar u ofrecer orientaciones en relación con el presente Reglamento con respecto a las categorías específicas de sistemas de IA de alto riesgo que presentan un riesgo grave en dos o más Estados miembros de conformidad con el artículo 9 del Reglamento (UE) 2019/1020. La Oficina de IA prestará apoyo de coordinación a las investigaciones conjuntas.

12. Sin perjuicio de los poderes previstos en el Reglamento (UE) 2019/1020, y cuando proceda y se limite a lo necesario para el desempeño de sus funciones, los proveedores concederán a las autoridades de vigilancia del mercado pleno acceso a la documentación, así como a los conjuntos de datos de entrenamiento, validación y prueba utilizados para el desarrollo de los sistemas de IA de alto riesgo, también, cuando proceda y con sujeción a garantías de seguridad, a través de interfaces de programación de aplicaciones (API) o de otras herramientas y medios técnicos pertinentes que permitan el acceso a distancia.

13. Se concederá a las autoridades de vigilancia del mercado acceso al código fuente del sistema de IA de alto riesgo, previa solicitud motivada y solo si se cumplen las dos siguientes condiciones:

    a) el acceso al código fuente es necesario para evaluar la conformidad de un sistema de IA de alto riesgo con los requisitos establecidos en el capítulo III, sección 2, y

    b) se han agotado todos los procedimientos de prueba o auditoría y todas las comprobaciones basadas en los datos y la documentación facilitados por el proveedor, o han resultado insuficientes.

14. Cualesquiera información o documentación obtenidas por las autoridades de vigilancia del mercado se tratarán de conformidad con las obligaciones de confidencialidad establecidas en el artículo 78.

ARTÍCULO 75
VIGILANCIA DEL MERCADO Y CONTROL DE LOS SISTEMAS DE IA Y ASISTENCIA MUTUA

1. La Oficina de IA tendrá competencia exclusiva para supervisar y garantizar el cumplimiento de las obligaciones derivadas del presente Reglamento en relación con los sistemas de IA siguientes:

    a) sistemas de IA basados en modelos de IA de uso general en los que el modelo y el sistema sean desarrollados por el mismo proveedor o por proveedores que formen parte de una misma empresa, con excepción de:

        i) los sistemas de IA relacionados con productos regulados por los actos legislativos de armonización de la Unión enumerados en el anexo I,

        ii) los sistemas de IA a que se refiere el anexo III, punto 2,

        iii) los sistemas de IA proporcionados por autoridades garantes del cumplimiento del Derecho, autoridades de gestión de fronteras y entidades financieras, en la medida en que dichos sistemas de IA entren en el ámbito de aplicación del artículo 74, apartado 6, y

        iv) los sistemas de IA a que se refiere el anexo III, punto 8, en lo que respecta a la administración de justicia;

    b) sistemas de IA que constituyan o estén integrados en una plataforma en línea de muy gran tamaño o un motor de búsqueda en línea de muy gran tamaño designados de conformidad con el Reglamento (UE) 2022/2065.

La competencia exclusiva a que se refiere el párrafo primero se aplicará a los proveedores de dichos sistemas. Únicamente se aplicará a los responsables del despliegue de dichos sistemas cuando sean también el proveedor o formen parte de la misma empresa que el proveedor.

1 bis. Como excepción a lo dispuesto en el artículo 73, los proveedores de sistemas de IA de alto riesgo sujetos a la competencia de la Oficina de IA en virtud del apartado 1 del presente artículo notificarán cualquier incidente grave a la Oficina de IA. Será aplicable por analogía el artículo 73, apartados 2 a 9. La Oficina de IA transmitirá sin demora la información pertinente a la autoridad de vigilancia del mercado del Estado miembro en cuyo territorio esté situado el proveedor o su representante legal.

1 ter. Las autoridades que participen en la aplicación del presente Reglamento cooperarán activamente con la Oficina de IA y le prestarán la asistencia necesaria para el ejercicio de sus competencias, incluido, cuando sea necesario, en relación con las inspecciones u otras medidas de garantía del cumplimiento llevadas a cabo en el territorio de un Estado miembro. A tal fin, dichas autoridades gozarán de los poderes establecidos en virtud del presente Reglamento y del Reglamento (UE) 2019/1020 y, cuando proceda y de modo limitado a lo necesario para desempeñar sus funciones con arreglo al presente apartado, de conformidad con los procedimientos nacionales aplicables.

1 quater. Cuando adopte medidas de investigación o de garantía del cumplimiento en el territorio de un Estado miembro que impliquen el acceso a los datos o al sistema de IA de una autoridad pública, la Oficina de IA estará

asistida por la autoridad de vigilancia del mercado pertinente.

1 quinquies. Antes de adoptar una decisión que tenga por efecto prohibir o restringir la comercialización o puesta en servicio del sistema de IA en un mercado nacional, o una decisión de retirar o recuperar el sistema de IA de dicho mercado, la Oficina de IA notificará, sin demora indebida, a la autoridad de vigilancia del mercado competente para dicho mercado su intención de adoptar tal decisión. La Oficina de IA consultará a las autoridades que participen en la aplicación del presente Reglamento, cuando proceda, sobre cualquier asunto relacionado con la aplicación y ejecución del presente Reglamento.

1 sexies. La Oficina de IA será responsable de las evaluaciones de la conformidad y las pruebas de los sistemas de IA a que se refiere el apartado 1 del presente artículo clasificados como de alto riesgo y sujetos a una evaluación de la conformidad de terceros en virtud del artículo 43 antes de su introducción en el mercado o su puesta en servicio. Dichas pruebas y evaluaciones comprobarán que los sistemas cumplen los requisitos pertinentes del presente Reglamento y pueden introducirse en el mercado o ponerse en servicio en la Unión de conformidad con el presente Reglamento. La Comisión encomendará la realización de estas pruebas o evaluaciones a organismos notificados designados de conformidad con el presente Reglamento, en cuyo caso el organismo notificado actuará en nombre de la Comisión. Si un organismo notificado al que la Comisión haya encomendado tareas en virtud del presente apartado no las realiza adecuadamente, la Comisión podrá retirar la delegación con efecto inmediato.

Las tasas por las actividades de prueba y evaluación se cobrarán a los proveedores de sistemas de IA de alto riesgo que hayan solicitado a la Comisión la evaluación de la conformidad de terceros. El proveedor abonará directamente al organismo notificado los costes relacionados con los servicios encomendados por la Comisión a los organismos notificados de conformidad con el presente artículo.

2. Cuando las autoridades de vigilancia del mercado pertinentes tengan motivos suficientes para considerar que los sistemas de IA de uso general que pueden ser utilizados directamente por los responsables del despliegue al menos para una de las finalidades clasificadas como de alto riesgo con arreglo al presente Reglamento no cumplen los requisitos establecidos en el presente Reglamento, cooperarán con la Oficina de IA para llevar a cabo evaluaciones del cumplimiento e informarán al respecto al Consejo de IA y las demás autoridades de vigilancia del mercado.

2 bis. Cuando una autoridad de vigilancia del mercado tenga motivos fundados y suficientes para sospechar que un proveedor o un responsable del despliegue de un sistema de IA a que se refiere el apartado 1 del presente artículo ha infringido el presente Reglamento, podrá solicitar a la Oficina de IA, a través del punto de contacto único pertinente designado de conformidad con el artículo 70, apartado 2, que evalúe la cuestión con el fin de adoptar las medidas de supervisión y de garantía del cumplimiento necesarias para garantizar el rápido cumplimiento del presente Reglamento. Tal solicitud deberá motivarse debidamente e indicar, como mínimo:

a) el nombre del proveedor o del responsable del despliegue de que se trate;

b) una descripción de los hechos pertinentes, las disposiciones del presente Reglamento presuntamente infringidas y cualquier motivo fundado y suficiente para sospechar una infracción, incluida, en su caso, la descripción de los efectos negativos de la presunta infracción, y

c) la autoridad de vigilancia del mercado que presenta la solicitud.

La Oficina de IA tendrá en cuenta la solicitud en la mayor medida posible, y la autoridad de vigilancia del mercado cooperará activamente y proporcionará a la Oficina de IA la asistencia necesaria para el ejercicio de sus competencias de conformidad con el apartado 1 bis.

La Oficina de IA, sin demora indebida y, en cualquier caso, a más tardar cuatro meses después de la recepción de la solicitud, informará al punto de contacto único de su intención de ejercer sus competencias de conformidad con el artículo 75 bis o de sus motivos para no ejercer dichas competencias. Si la Oficina de IA decide ejercer sus competencias de conformidad con el artículo 75 bis, informará periódicamente a dicho punto de contacto único sobre cualquier novedad destacada en el procedimiento y sobre el resultado de este, sin revelar ninguna información confidencial.

3. Cuando una autoridad de vigilancia del mercado no pueda concluir su investigación sobre el sistema de IA de alto riesgo por no poder acceder a determinada información relativa al modelo de IA de uso general, a pesar de haber realizado todos los esfuerzos adecuados para obtener esa información, podrá presentar una solicitud motivada a la Oficina de IA para que se imponga el acceso a dicha información. En tal caso, la Oficina de IA facilitará a la autoridad solicitante sin demora y, en cualquier caso en un plazo de treinta días, toda la información que la Oficina de IA considere pertinente para determinar si un sistema de IA de alto riesgo no es conforme. Las autoridades de vigilancia del mercado preservarán la confidencialidad de la información obtenida de conformidad con lo dispuesto en el artículo 78 del presente Reglamento. Se aplicará mutatis mutandis el procedimiento previsto en el capítulo VI del Reglamento (UE) 2019/1020.

ARTÍCULO 75 BIS
COMPETENCIAS DE SUPERVISIÓN Y DE GARANTÍA DEL CUMPLIMIENTO DE LA OFICINA DE IA

1. Para llevar a cabo las tareas de supervisión y de garantía del cumplimiento establecidas en el artículo 75, apartado 1 del presente Reglamento, la Oficina de IA tendrá todos los poderes de una autoridad de vigilancia del mercado previstos en la presente sección y en el artículo 14, apartado 4, y el artículo 16, apartado 3, del Reglamento (UE) 2019/1020. La Oficina de IA estará autorizada a reclamar al operador pertinente la totalidad de los costes derivados de sus actividades de supervisión y de garantía del cumplimiento en casos de incumplimiento, incluidos los costes de recursos humanos y técnicos, de conformidad con el artículo 15 del Reglamento (UE) 2019/1020. El artículo 17 del Reglamento (UE) 2019/1020 se aplicará mutatis mutandis.

2. Cuando la Oficina de IA tenga motivos razonables para sospechar que un proveedor o un responsable del despliegue de un sistema de IA a que se refiere el artículo 75, apartado 1 del presente Reglamento, incumple el

presente Reglamento, podrá adoptar una decisión de iniciar una investigación sobre dicho incumplimiento de conformidad con el artículo 14, apartado 4, letra f), del Reglamento (UE) 2019/1020. Al iniciar dicha investigación, la Oficina de IA lo notificará al operador del sistema de IA de que se trate. La Oficina de IA podrá ejercer los poderes a que se refiere el apartado 1 del presente artículo por iniciativa propia o a raíz de una reclamación recibida en virtud del artículo 85 del presente Reglamento, incluso antes de iniciar una investigación en virtud del artículo 14, apartado 4, letra f), del Reglamento (UE) 2019/1020.

Cuando una autoridad de vigilancia del mercado tenga motivos para sospechar que un proveedor o un responsable del despliegue de un sistema de IA a que se refiere el artículo 75, apartado 1, incumple el presente Reglamento, podrá enviar una solicitud a la Oficina de IA para que evalúe el asunto.

3. La Oficina de IA podrá ejercer los poderes enumerados en el artículo 14, apartado 4, letras a), b) y c), del Reglamento (UE) 2019/1020 y en el artículo 74, apartados 12 y 13, del presente Reglamento mediante simple solicitud o mediante una decisión.

Al solicitar información, la Oficina de IA indicará la base jurídica y la finalidad de la solicitud, especificará qué información se requiere y fijará el plazo en el que debe proporcionarse la información. Cuando se trate de una simple solicitud, la Oficina de IA indicará asimismo que, aunque no exista obligación de proporcionar la información solicitada, toda respuesta voluntaria deberá ser correcta y no engañosa, e indicará las posibles multas previstas en el artículo 99, apartado 5, por proporcionar información inexacta o engañosa. Cuando la solicitud se presente mediante decisión, la Oficina de IA indicará además las multas previstas en el artículo 99, apartado 5, por proporcionar información inexacta, incompleta o engañosa, e indicará el derecho a recurrir la decisión ante el Tribunal de Justicia de la Unión Europea. La Oficina de IA enviará una copia de la solicitud a la autoridad de vigilancia del mercado del Estado miembro en cuyo territorio esté situado el operador o su representante legal.

4. A fin de desempeñar las funciones que se le asignan en virtud de la presente sección, la Oficina de IA podrá llevar a cabo todas las inspecciones a distancia o in situ necesarias en virtud de los poderes establecidos en el artículo 14, apartado 4, letras d) y e), del Reglamento (UE) 2019/1020 y en el artículo 74, apartado 5, del presente Reglamento. Al llevar a cabo una inspección, la Oficina de IA informará al proveedor de que se trate del objeto y la finalidad de la investigación, de las multas pertinentes a que se refiere el artículo 99, apartado 5, del presente Reglamento y del derecho a recurrir la decisión ante el Tribunal de Justicia de la Unión Europea. Antes de llevar a cabo una inspección, la Oficina de IA informará a la autoridad de vigilancia del mercado del Estado miembro en cuyo territorio esté situado el operador o su representante legal.

Durante dicha inspección, los agentes de la Oficina de IA estarán facultados para:

a) acceder a cualquiera de los locales, terrenos o propiedades de uso profesional situados en la Unión del operador de que se trate;

b) examinar los libros, datos y demás documentación pertinentes para el desempeño de sus funciones, independientemente del medio utilizado para almacenarlos;

c) tomar u obtener, en cualquier formato, copias o extractos de libros, datos y otros registros;

d) pedir a toda persona objeto de la inspección, o a sus representantes o a miembros de su personal, que den explicaciones orales o escritas sobre los factores o documentos que guarden relación con el objeto y el propósito de la inspección, y registrar las respuestas, o

e) precintar todos los locales y libros o documentos de la empresa mientras dure la inspección y en la medida en que sea necesario para esta.

Cuando la Oficina de IA constate que una persona física o jurídica se opone a una inspección o la obstaculiza, la autoridad nacional competente del Estado miembro de que se trate le prestará la asistencia necesaria, solicitando, cuando proceda, la asistencia de la policía o de una autoridad de garantía del cumplimiento equivalente, para poder llevar a cabo la inspección in situ.

Cuando una inspección in situ de locales, terrenos o propiedades de uso profesional requiera la autorización de una autoridad judicial de conformidad con el Derecho nacional, la Oficina de IA solicitará dicha autorización. También podrá solicitarla como medida cautelar. Cuando se solicite dicha autorización, la autoridad judicial nacional comprobará sin demora que las medidas coercitivas previstas no sean arbitrarias ni desproporcionadas, teniendo en cuenta el objeto de la investigación o inspección y los documentos facilitados por la Oficina de IA junto con la decisión. Al comprobar la proporcionalidad de las medidas coercitivas, la autoridad judicial nacional podrá solicitar a la Oficina de IA explicaciones detalladas, en particular sobre los motivos por los que la Oficina de IA sospecha que se ha infringido el presente Reglamento, así como sobre la gravedad de la presunta infracción y, en su caso, la naturaleza de la implicación de la persona sujeta a las medidas coercitivas. La autoridad judicial nacional no revisará la necesidad de la investigación o inspección ni exigirá información del expediente de la Oficina de IA. De conformidad con los Tratados, la legalidad de la decisión de la Oficina de IA solo está sujeta al examen del Tribunal de Justicia de la Unión Europea.

5. A petición de la Oficina de IA, la autoridad de vigilancia del mercado competente de un Estado miembro podrá llevar a cabo en su propio territorio cualquier investigación, inspección u otra medida de investigación en nombre y por cuenta de la Oficina de IA con el fin de determinar si se ha infringido el presente Reglamento. Los agentes de las autoridades competentes de los Estados miembros que sean responsables de llevar a cabo tales investigaciones, inspecciones o medidas de investigación, así como las personas autorizadas o designadas por ellos, ejercerán sus facultades de conformidad con su Derecho nacional.

6. Además de los poderes establecidos en el apartado 1 del presente artículo, la Oficina de IA, en el ejercicio de sus competencias a que se refiere el artículo 75, apartado 1, podrá:

a) ordenar a los operadores que proporcionen acceso a sus sistemas de IA y explicaciones al respecto;

b) imponer a un operador la obligación de conservar todos los datos y documentos que se consideren necesarios para evaluar la aplicación y el cumplimiento de las obligaciones derivadas del presente Reglamento.

7. Con el fin de ayudarla a supervisar la aplicación y el cumplimiento efectivos de las disposiciones pertinentes del presente Reglamento y de proporcionarle conocimientos especializados o específicos en el ejercicio de sus poderes con arreglo al artículo 75, apartado 1, la Oficina de IA podrá nombrar a expertos y auditores externos independientes, así como a expertos, equipos de investigación y auditores de las autoridades competentes de los Estados miembros, con el acuerdo de la autoridad de que se trate. La información obtenida como resultado de dichas medidas de seguimiento se compartirá con las autoridades competentes pertinentes de los Estados miembros.
8. La información recopilada en virtud del presente artículo se utilizará únicamente a efectos del presente Reglamento.

ARTÍCULO 75 TER
COMPROMISOS

Si, durante uno de los procedimientos previstos en el artículo 75 bis, apartado 2, el operador de que se trate ofrece compromisos para garantizar el cumplimiento de las disposiciones pertinentes del presente Reglamento, la Oficina de IA podrá, mediante decisión, hacer que dichos compromisos sean vinculantes para el operador de que se trate y declarar que no existen motivos adicionales para actuar. La Oficina de IA podrá, previa solicitud o por iniciativa propia, reabrir el procedimiento cuando:

a) se haya producido una modificación significativa de los hechos den los que se haya basado la decisión;
b) el operador actúe en contra de sus compromisos, o
c) la decisión se haya basado en informaciones incompletas, inexactas o engañosas proporcionadas por el operador de que se trate.

Cuando la Oficina de IA considere que los compromisos ofrecidos por el operador afectado no pueden garantizar el cumplimiento efectivo de las disposiciones pertinentes del presente Reglamento, rechazará dichos compromisos en una decisión motivada al finalizar el procedimiento.

ARTÍCULO 75 QUATER
INCUMPLIMIENTO, MULTAS SANCIONADORAS Y MULTAS COERCITIVAS

1. Cuando la Oficina de IA constate que un operador que se regule en el artículo 75, apartado 1, incumple las disposiciones pertinentes del presente Reglamento o los compromisos convertidos en vinculantes en virtud del artículo 75 ter, adoptará una decisión por la que se declare dicho incumplimiento.
2. Antes de adoptar una decisión en virtud del apartado 1, la Oficina de IA comunicará sus conclusiones preliminares al operador de que se trate. En dichas conclusiones, la Oficina de IA explicará las medidas que esté considerando adoptar, o que considere que el operador de que se trate debe adoptar a fin de atender de manera efectiva a las conclusiones preliminares.
3. En la decisión adoptada en virtud del apartado 1 del presente artículo, la Oficina de IA ordenará, cuando proceda, al operador de que se trate que adopte, en un plazo razonable especificado en dicha decisión, las medidas necesarias para garantizar el cumplimiento de las disposiciones pertinentes del presente Reglamento y que proporcione información sobre las medidas que tenga intención de adoptar para dar cumplimiento a la decisión. El operador de que se trate aportará a la Oficina de IA una descripción de las medidas que haya adoptado para garantizar el cumplimiento de la decisión tras su aplicación. Antes de solicitar cualquier medida, la Oficina de IA podrá entablar un diálogo estructurado con el operador del sistema de IA en cuestión. Durante este diálogo, el operador podrá proponer compromisos de conformidad con el artículo 75 ter.
4. Una decisión adoptada en virtud del apartado 1 del presente artículo podrá ir acompañada de la imposición de sanciones de conformidad con el artículo 99, apartados 3 a 7, cuyas disposiciones se aplicarán, mutatis mutandis, a la Oficina de IA en el ejercicio de las tareas de supervisión y de garantía del cumplimiento a que se refiere el artículo 75, apartado 1.

En particular, estarán sujetos a las multas administrativas a que se refiere el artículo 99, apartado 4:

a) las infracciones de cualquier disposición aplicable del presente Reglamento, incluidas las no enumeradas en el artículo 99, apartado 4;
b) el incumplimiento de las decisiones o medidas adoptadas en virtud de los poderes enumerados en el artículo 14, apartado 4, o en el artículo 16, apartado 3, del Reglamento (UE) 2019/1020, así como los especificados en el artículo 75 bis del presente Reglamento;
c) el incumplimiento de un compromiso que se haya declarado vinculante por medio de una decisión adoptada en virtud del artículo 75 ter.

El suministro de información inexacta, incompleta o engañosa a la Oficina de IA en respuesta a una solicitud estará sujeta a las multas administrativas a que se refiere el artículo 99, apartado 5.

5. La Oficina de IA podrá adoptar una decisión por la que se impongan multas coercitivas para obligar a los operadores sujetos a sus poderes en virtud del artículo 75, apartado 1, a:

a) someterse a una investigación;
b) atender una solicitud de información ordenada mediante una decisión adoptada en virtud del artículo 75 bis, apartado 3;
c) someterse a una inspección ordenada mediante una decisión adoptada en virtud del artículo 75 bis, apartado 4;
d) proporcionar respuestas o explicaciones correctas o completas en el contexto de una inspección ordenada mediante una decisión adoptada en virtud del artículo 75 bis, apartado 4;
e) cumplir las medidas correctoras ordenadas en virtud de los poderes enumerados en el artículo 16 del Reglamento (UE) 2019/1020;
f) cumplir los compromisos que se hayan hecho jurídicamente vinculantes mediante una decisión adoptada en virtud del artículo 75 ter, o
g) cumplir una decisión adoptada en virtud del apartado 1 del presente artículo.

Dichas multas coercitivas serán efectivas y proporcionadas y, cuando proceda, no excederán, por día y a partir de la fecha fijada en la decisión, del 5 % de los ingresos diarios medios o del volumen de negocios anual mundial del ejercicio financiero anterior.

6. El Tribunal de Justicia de la Unión Europea tendrá plena competencia jurisdiccional para examinar las decisiones de

la Oficina de IA por las que se fije una multa sancionadora o una multa coercitiva en virtud del presente artículo. Podrá anular, reducir o incrementar la multa sancionadora o la multa coercitiva impuesta.

7. Los fondos recaudados mediante la imposición de multas sancionadoras o multas coercitivas impuestas en virtud del presente artículo contribuirán al presupuesto general de la Unión.

8. Los poderes otorgados a la Oficina de IA por el presente artículo estarán sujetos a un plazo de prescripción de cinco años. El plazo de prescripción comenzará a contar a partir del día en que se haya cometido la infracción. No obstante, en el caso de infracciones continuadas o reiteradas, el plazo de prescripción comenzará a contarse el día en que cese la infracción.

Los poderes de la Oficina de IA para hacer cumplir las decisiones adoptadas en virtud del presente artículo estarán sujetos a un plazo de prescripción de cinco años. El plazo de prescripción comenzará a contar a partir del día en que la decisión sea firme.

El acto de ejecución a que se refiere el artículo 75 quinquies, apartado 3, especificará los párrafos primero y segundo del presente apartado, incluidas las circunstancias en las que se interrumpirán los plazos de prescripción.

9. Cuando la Oficina de IA determine que no existen motivos para adoptar una decisión de incumplimiento, pondrá fin al procedimiento mediante una decisión. Dicha decisión se aplicará con efectos inmediatos.

ARTÍCULO 75 QUINQUIES
SALVAGUARDIAS Y ESPECIFICACIONES ADICIONALES

1. El artículo 18 del Reglamento (UE) 2019/1020 se aplicará, mutatis mutandis, a los operadores sujetos a la competencia de la Oficina de IA en virtud del artículo 75, apartado 1, del presente Reglamento, sin perjuicio de los derechos procedimentales más específicos previstos en el presente Reglamento.

2. Los derechos de defensa y de acceso al expediente de los operadores comprendidos en el ámbito de aplicación del artículo 75, apartado 1, se respetarán plenamente en los procedimientos. Habida cuenta de la posible adopción de decisiones con arreglo al artículo 75 quater, apartado 1, dichos operadores tendrán derecho de acceso al expediente de la Oficina de IA en las condiciones de una divulgación negociada, sin perjuicio del interés legítimo del operador u otra persona afectada en la protección de sus secretos comerciales. La Oficina de IA estará facultada para adoptar decisiones en las que se establezcan dichas condiciones de divulgación en caso de desacuerdo entre las partes. El derecho de acceso al expediente no se extenderá a la información confidencial ni a los documentos internos de la Oficina de IA, el Consejo de IA, las autoridades competentes de vigilancia del mercado u otras autoridades públicas de los Estados miembros. En particular, el derecho de acceso no se extenderá a la correspondencia entre la Oficina de IA y dichas autoridades. Nada de lo dispuesto en el presente apartado impedirá que la Oficina de IA revele y utilice la información necesaria para demostrar una infracción.

3. La Comisión estará facultada para adoptar actos de ejecución relativos a las modalidades prácticas de acceso al expediente y a la divulgación negociada de información prevista en el apartado 2.

4. La Oficina de IA publicará las decisiones que adopte en virtud de los artículos 75 ter y 75 quater. Dicha publicación mencionará los nombres de las partes y el contenido principal de la decisión, incluidas las sanciones impuestas. La publicación tendrá en cuenta los derechos e intereses legítimos de cualquier persona interesada en la protección de su información confidencial.

ARTÍCULO 76
SUPERVISIÓN DE LAS PRUEBAS EN CONDICIONES REALES POR LAS AUTORIDADES DE VIGILANCIA DEL MERCADO

1. Las autoridades de vigilancia del mercado tendrán las competencias y los poderes necesarios para garantizar que las pruebas en condiciones reales se ajusten a lo dispuesto en el presente Reglamento.

Cuando la prueba en condiciones reales se base en el artículo 60 bis, toda referencia a una autoridad de vigilancia del mercado en el presente artículo se interpretará como una referencia a la autoridad nacional competente o a la autoridad apropiada con arreglo a los actos legislativos de armonización de la Unión enumerados en el anexo I, sección B, y las referencias al artículo 60 se interpretarán como referencias al artículo 60 bis, según proceda.

2. Cuando se realicen pruebas en condiciones reales de sistemas de IA supervisadas dentro de un espacio controlado de pruebas para la IA con arreglo al artículo 58, las autoridades de vigilancia del mercado verificarán el cumplimiento de del artículo 60 como parte de su función supervisora en el espacio controlado de pruebas para la IA. Dichas autoridades podrán permitir, según proceda, que el proveedor o proveedor potencial lleve a cabo pruebas en condiciones reales, como excepción a las condiciones establecidas en el artículo 60, apartado 4, letras f) y g).

3. Cuando una autoridad de vigilancia del mercado haya sido informada por el proveedor potencial, el proveedor o un tercero de un incidente grave o tenga otros motivos para pensar que no se cumplen las condiciones establecidas en los artículos 60 y 61, podrá adoptar una de las decisiones siguientes en su territorio, según proceda:

a) suspender o poner fin a las pruebas en condiciones reales;

b) exigir al proveedor o proveedor potencial y al responsable del despliegue o responsable del despliegue potencial que modifiquen cualquier aspecto de las pruebas en condiciones reales.

4. Cuando una autoridad de vigilancia del mercado haya adoptado una decisión mencionada en el apartado 3 del presente artículo o haya formulado una objeción en el sentido del artículo 60, apartado 4, letra b), la decisión o la objeción deberá estar motivada e indicar las vías de que dispone el proveedor o proveedor potencial para poder impugnar la decisión o la objeción.

5. En su caso, cuando una autoridad de vigilancia del mercado haya adoptado una decisión mencionada en el apartado 3, comunicará los motivos de dicha decisión a las autoridades de vigilancia del mercado de los demás Estados miembros en que se haya probado el sistema de IA de conformidad con el plan de la prueba.

ARTÍCULO 77
PODERES DE LAS AUTORIDADES ENCARGADAS DE PROTEGER LOS DERECHOS FUNDAMENTALES Y COOPERACIÓN CON LAS AUTORIDADES DE VIGILANCIA DEL MERCADO

1. Las autoridades u organismos públicos nacionales encargados de supervisar o hacer respetar las obligaciones contempladas en el Derecho de la Unión en materia de protección de los derechos fundamentales, incluido el derecho a la no discriminación, tendrán el poder de solicitar cualquier información o documentación creada o conservada por la autoridad de vigilancia del mercado pertinente en virtud del presente Reglamento y de acceder a ella, en un lenguaje accesible y en un formato legible por máquina por medios electrónicos, en caso de que el acceso a dicha información o documentación sea necesario para el cumplimiento efectivo de sus mandatos, dentro de los límites de su jurisdicción. Este artículo se entiende sin perjuicio de las competencias, tareas, poderes e independencia de las autoridades u organismos públicos nacionales pertinentes en el marco de sus mandatos.

1 bis. En las condiciones especificadas en el presente artículo, la autoridad de vigilancia del mercado concederá a la autoridad u organismo público pertinente a que se refiere el apartado 1 acceso a esa información o documentación, incluso solicitando dicha información o documentación al proveedor o al responsable del despliegue, cuando sea necesario y sin demora indebida.

1 ter. Las autoridades de vigilancia del mercado y las autoridades u organismos públicos a que se refiere el apartado 1 cooperarán estrechamente y se prestarán la asistencia mutua necesaria para el cumplimiento de sus respectivos mandatos, con miras a garantizar una aplicación coherente del presente Reglamento y del Derecho de la Unión en materia de protección de los derechos fundamentales y racionalizar los procedimientos, respetando al mismo tiempo sus respectivas competencias, tareas, poderes e independencia. Esto incluirá, en particular, el intercambio de información cuando sea necesario para ejercer de manera eficaz la supervisión o la garantía del cumplimiento de lo establecido en el presente Reglamento y otra normativa de la Unión pertinente.

2. A más tardar el 2 de noviembre de 2024, cada Estado miembro designará las autoridades u organismos públicos a que se refiere el apartado 1 y los incluirá en una lista que pondrá a disposición del público. Los Estados miembros notificarán dicha lista a la Comisión y a los demás Estados miembros y la mantendrán actualizada.

3. Cuando la documentación mencionada en el apartado 1 no baste para determinar si se ha producido un incumplimiento de las obligaciones previstas en el Derecho de la Unión en materia de protección de los derechos fundamentales, la autoridad u organismo público a que se refiere el apartado 1 podrá presentar una solicitud motivada a la autoridad de vigilancia del mercado para organizar pruebas del sistema de IA de alto riesgo a través de medios técnicos. La autoridad de vigilancia del mercado organizará las pruebas con la estrecha colaboración de la autoridad u organismo público solicitante en un plazo razonable tras la presentación de la solicitud.

4. Cualquier información o documentación obtenidas por las autoridades u organismos públicos nacionales a que se refiere el apartado 1 del presente artículo con arreglo al presente artículo se tratará de conformidad con las obligaciones de confidencialidad dispuestas en el artículo 78.

ARTÍCULO 78
CONFIDENCIALIDAD

1. La Comisión, las autoridades de vigilancia del mercado, los organismos notificados y cualquier otra persona física o jurídica que participe en la aplicación del presente Reglamento, de conformidad con el Derecho de la Unión o nacional, respetarán la confidencialidad de la información y los datos obtenidos en el ejercicio de sus funciones y actividades de modo que se protejan, en particular:
   a) los derechos de propiedad intelectual e industrial y la información empresarial confidencial o los secretos comerciales de una persona física o jurídica, incluido el código fuente, salvo en los casos mencionados en el artículo 5 de la Directiva (UE) 2016/943 del Parlamento Europeo y del Consejo (1);
   b) la aplicación eficaz del presente Reglamento, en particular a efectos de investigaciones, inspecciones o auditorías;
   c) los intereses de seguridad pública y nacional;
   d) el desarrollo de las causas penales o los procedimientos administrativos;
   e) la información clasificada con arreglo al Derecho de la Unión o nacional.

2. Las autoridades involucradas en la aplicación del presente Reglamento de conformidad con el apartado 1 solo solicitarán los datos que sean estrictamente necesarios para la evaluación del riesgo que presentan los sistemas de IA y para el ejercicio de sus competencias de conformidad con el presente Reglamento y con el Reglamento (UE) 2019/1020. Establecerán medidas adecuadas y eficaces en materia de ciberseguridad a fin de proteger la seguridad y la confidencialidad de la información y los datos obtenidos, y suprimirán los datos recopilados tan pronto como dejen de ser necesarios para los fines para los que se obtuvieron, de conformidad con el Derecho de la Unión y nacional aplicable.

(1) Directiva (UE) 2016/943 del Parlamento Europeo y del Consejo, de 8 de junio de 2016, relativa a la protección de los conocimientos técnicos y la información empresarial no divulgados (secretos comerciales) contra su obtención, utilización y revelación ilícitas (DO L 157 de 15.6.2016, p. 1).

3. Sin perjuicio de lo dispuesto en los apartados 1 y 2, la información intercambiada de forma confidencial entre las autoridades nacionales competentes o entre estas y la Comisión no se revelará sin consultar previamente a la autoridad nacional competente de origen y al responsable del despliegue cuando las autoridades garantes del cumplimiento del Derecho, del control de fronteras, de la inmigración o del asilo utilicen los sistemas de IA de alto riesgo a que se refiere el anexo III, puntos 1, 6 o 7, y dicha divulgación comprometería los intereses de seguridad pública y nacional. Este intercambio de información no comprenderá los datos operativos sensibles relativos a las actividades de las autoridades garantes del cumplimiento del Derecho, del control de fronteras, de la inmigración o del asilo.

Cuando las autoridades garantes del cumplimiento del Derecho, de la inmigración o del asilo sean proveedores de

sistemas de IA de alto riesgo a que se refiere el anexo III, puntos 1, 6 o 7, la documentación técnica mencionada en el anexo IV permanecerá dentro de las instalaciones de dichas autoridades. Dichas autoridades velarán por que las autoridades de vigilancia del mercado a que se refiere el artículo 74, apartados 8 y 9, según proceda, puedan, previa solicitud, acceder inmediatamente a la documentación u obtener una copia de esta. Tan solo se permitirá acceder a dicha documentación o a cualquier copia de esta al personal de la autoridad de vigilancia del mercado que disponga de una habilitación de seguridad del nivel adecuado.

4. Los apartados 1, 2 y 3 no afectarán a los derechos u obligaciones de la Comisión, los Estados miembros y sus autoridades pertinentes, ni a los derechos u obligaciones de los organismos notificados en lo que se refiere al intercambio de información y la difusión de advertencias, también en el contexto de la cooperación transfronteriza, ni a las obligaciones de facilitar información en virtud del Derecho penal de los Estados miembros que incumban a las partes interesadas.
5. Cuando sea necesario y con arreglo a las disposiciones pertinentes de los acuerdos internacionales y comerciales, la Comisión y los Estados miembros podrán intercambiar información confidencial con autoridades reguladoras de terceros países con las que hayan celebrado acuerdos de confidencialidad bilaterales o multilaterales que garanticen un nivel de confidencialidad adecuado.

ARTÍCULO 79
PROCEDIMIENTO APLICABLE A ESCALA NACIONAL A LOS SISTEMAS DE IA QUE PRESENTEN UN RIESGO

1. Los sistemas de IA que presentan un riesgo se entenderán como «productos que presentan un riesgo» tal como se definen en el artículo 3, punto 19, del Reglamento (UE) 2019/1020, en la medida en que presenten riegos que afecten a la salud, la seguridad o los derechos fundamentales de las personas.
2. Cuando la autoridad de vigilancia del mercado de un Estado miembro tenga motivos suficientes para considerar que un sistema de IA presenta un riesgo mencionado en el apartado 1 del presente artículo, efectuará una evaluación del sistema de IA de que se trate para verificar su cumplimiento de todos los requisitos y obligaciones establecidos en el presente Reglamento. Debe prestarse una especial atención a los sistemas de IA que presenten un riesgo para los colectivos vulnerables. Cuando se detecten riesgos para los derechos fundamentales, la autoridad de vigilancia del mercado informará también a las autoridades u organismos públicos nacionales pertinentes a que se refiere el artículo 77, apartado 1, y cooperará plenamente con ellos. Los operadores pertinentes cooperarán en lo necesario con la autoridad de vigilancia del mercado y con las demás autoridades u organismos públicos nacionales a que se refiere el artículo 77, apartado 1.

Cuando, en el transcurso de tal evaluación, la autoridad de vigilancia del mercado o, cuando proceda, la autoridad de vigilancia del mercado en cooperación con la autoridad nacional pública a que se refiere el artículo 77, apartado 1, constate que el sistema de IA no cumple los requisitos y obligaciones establecidos en el presente Reglamento, exigirá sin demora indebida al operador pertinente que adopte todas las medidas correctoras oportunas para adaptar el sistema de IA a los citados requisitos y obligaciones, retirarlo del mercado o recuperarlo, dentro de un plazo que dicha autoridad podrá determinar y, en cualquier caso, en un plazo de quince días hábiles a más tardar o en el plazo que prevean los actos legislativos de armonización de la Unión pertinentes según corresponda.

La autoridad de vigilancia del mercado informará al organismo notificado correspondiente en consecuencia. El artículo 18 del Reglamento (UE) 2019/1020 será de aplicación a las medidas mencionadas en el párrafo segundo del presente apartado.

3. Cuando la autoridad de vigilancia del mercado considere que el incumplimiento no se limita a su territorio nacional, informará a la Comisión y a los demás Estados miembros sin demora indebida de los resultados de la evaluación y de las medidas que haya instado al operador a adoptar.
4. El operador se asegurará de que se adopten todas las medidas correctoras adecuadas en relación con todos los sistemas de IA afectados que haya comercializado en la Unión.
5. Si el operador de un sistema de IA no adopta las medidas correctoras adecuadas en el plazo a que hace referencia el apartado 2, la autoridad de vigilancia del mercado adoptará todas las medidas provisionales adecuadas para prohibir o restringir la comercialización del sistema de IA en su mercado nacional o su puesta en servicio, para retirar el producto o el sistema de IA independiente de dicho mercado o recuperarlo. Dicha autoridad notificará estas medidas sin demora indebida a la Comisión y a los demás Estados miembros.
6. La notificación a que se refiere el apartado 5 incluirá todos los detalles disponibles, en particular la información necesaria para la identificación del sistema de IA no conforme, el origen del sistema de IA y la cadena de suministro, la naturaleza de la presunta no conformidad y el riesgo planteado, la naturaleza y duración de las medidas nacionales adoptadas y los argumentos expresados por el operador correspondiente. En concreto, las autoridades de vigilancia del mercado indicarán si la no conformidad se debe a uno o varios de los motivos siguientes:
   a) el no respeto de la prohibición de las prácticas de IA a que se refiere el artículo 5;
   b) el incumplimiento de los requisitos establecidos en el capítulo III, sección 2, por parte de un sistema de IA de alto riesgo;
   c) deficiencias en las normas armonizadas o especificaciones comunes mencionadas en los artículos 40 y 41 que confieren la presunción de conformidad;
   d) el incumplimiento del artículo 50.
7. Las autoridades de vigilancia del mercado distintas de la autoridad de vigilancia del mercado del Estado miembro que inició el procedimiento comunicarán sin demora indebida a la Comisión y a los demás Estados miembros toda medida que adopten y cualquier información adicional de que dispongan en relación con la no conformidad del sistema de IA de que se trate y, en caso de desacuerdo con la medida nacional notificada, sus objeciones al respecto.
8. Si, en el plazo de tres meses desde la recepción de la notificación mencionada en el apartado 5 del presente artículo, ninguna autoridad de vigilancia del mercado de un Estado miembro ni la Comisión presentan objeción

alguna sobre una medida provisional adoptada por una autoridad de vigilancia del mercado de otro Estado miembro, la medida se considerará justificada. Esto se entiende sin perjuicio de los derechos procedimentales del operador correspondiente con arreglo al artículo 18 del Reglamento (UE) 2019/1020. El plazo de tres meses a que se refiere el presente apartado se reducirá a treinta días en caso de no respeto de la prohibición de las prácticas de IA a que se refiere el artículo 5 del presente Reglamento.

9. Las autoridades de vigilancia del mercado velarán por que se adopten sin demora indebida las medidas restrictivas adecuadas respecto del producto o del sistema de IA de que se trate, tales como la retirada del producto o del sistema de IA de su mercado.

ARTÍCULO 80
PROCEDIMIENTO APLICABLE A LOS SISTEMAS DE IA CLASIFICADOS POR EL PROVEEDOR COMO NO DE ALTO RIESGO EN APLICACIÓN DEL ANEXO III

1. Cuando una autoridad de vigilancia del mercado tenga motivos suficientes para considerar que un sistema de IA que el proveedor haya clasificado como no de alto riesgo con arreglo al artículo 6, apartado 3, sí lo es, dicha autoridad realizará una evaluación del sistema de IA de que se trate por cuanto se refiere a su clasificación como sistema de IA de alto riesgo en función de las condiciones establecidas en el artículo 6, apartado 3, y las directrices de la Comisión.
2. Cuando, al realizar dicha evaluación, la autoridad de vigilancia del mercado constate que el sistema de IA afectado es de alto riesgo, pedirá sin demora indebida al proveedor correspondiente que adopte todas las medidas necesarias para que el sistema de IA cumpla los requisitos y obligaciones establecidos en el presente Reglamento, así como que adopte las medidas correctoras adecuadas en el plazo que la autoridad de vigilancia del mercado podrá determinar.
3. Cuando la autoridad de vigilancia del mercado considere que la utilización del sistema de IA afectado no se circunscribe a su territorio nacional, informará a la Comisión y a los demás Estados miembros sin demora indebida de los resultados de la evaluación y de las medidas que haya exigido al proveedor que adopte.
4. El proveedor se asegurará de que se adopten todas las medidas necesarias para que el sistema de IA cumpla los requisitos y obligaciones que se establecen en el presente Reglamento. Cuando el proveedor de un sistema de IA afectado no haga lo necesario para que cumpla dichos requisitos y obligaciones en el plazo a que se refiere el apartado 2 del presente artículo, se le impondrán multas de conformidad con el artículo 99.
5. El proveedor se asegurará de que se adopten todas las medidas correctoras adecuadas para todos los sistemas de IA afectados que haya comercializado en toda la Unión.
6. Cuando el proveedor del sistema de IA afectado no adopte las medidas correctoras adecuadas en el plazo a que se refiere el apartado 2 del presente artículo, se aplicará el artículo 79, apartados 5 a 9.
7. Cuando, al realizar la evaluación con arreglo al apartado 1 del presente artículo, la autoridad de vigilancia del mercado determine que el proveedor había clasificado erróneamente el sistema de IA como de no alto riesgo con el fin de eludir la aplicación de los requisitos establecidos en el capítulo III, sección 2, se impondrán multas al proveedor de conformidad con el artículo 99.
8. En el ejercicio de su facultad de supervisión de la aplicación del presente artículo, y de conformidad con el artículo 11 del Reglamento (UE) 2019/1020, las autoridades de vigilancia del mercado podrán realizar los controles pertinentes, teniendo en cuenta, en particular, la información almacenada en la base de datos de la UE a que se refiere el artículo 71 del presente Reglamento.

ARTÍCULO 81
PROCEDIMIENTO DE SALVAGUARDIA DE LA UNIÓN

1. Cuando, en el plazo de tres meses desde la recepción de la notificación a que se refiere el artículo 79, apartado 5, o en el plazo de treinta días en caso de que no se respete la prohibición de las prácticas de IA a que se refiere el artículo 5, la autoridad de vigilancia del mercado de un Estado miembro formule objeciones sobre una medida adoptada por otra autoridad de vigilancia del mercado, o cuando la Comisión considere que la medida es contraria al Derecho de la Unión, la Comisión entablará consultas sin demora indebida con la autoridad de vigilancia del mercado del Estado miembro pertinente y el operador u operadores, y evaluará la medida nacional. Basándose en los resultados de la mencionada evaluación, la Comisión decidirá, en un plazo de seis meses a partir de la notificación a que se refiere el artículo 79, apartado 5, o de sesenta días en caso de que no se respete la prohibición de las prácticas de IA a que se refiere el artículo 5, si la medida nacional está justificada y notificará su decisión a la autoridad de vigilancia del mercado del Estado miembro interesado. La Comisión informará también a las demás autoridades de vigilancia del mercado de su decisión.
2. Cuando la Comisión considere que la medida adoptada por el Estado miembro correspondiente está justificada, todos los Estados miembros se asegurarán de adoptar las medidas restrictivas adecuadas con respecto al sistema de IA de que se trate, como exigir la retirada del sistema de IA de su mercado sin demora indebida, e informarán de ello a la Comisión. Cuando la Comisión considere que la medida nacional no está justificada, el Estado miembro correspondiente retirará la medida e informará de ello a la Comisión.
3. Cuando se considere que la medida nacional está justificada y la no conformidad del sistema de IA se atribuya a deficiencias de las normas armonizadas o especificaciones comunes a las que se refieren los artículos 40 y 41 del presente Reglamento, la Comisión aplicará el procedimiento previsto en el artículo 11 del Reglamento (UE) n. o 1025/2012.

ARTÍCULO 82
SISTEMAS DE IA CONFORMES QUE PRESENTEN UN RIESGO

1. Si, tras efectuar una evaluación con arreglo a lo dispuesto en el artículo 79 y consultar a la autoridad pública nacional a que se refiere el artículo 77, apartado 1, la autoridad de vigilancia del mercado de un Estado miembro concluye que un sistema de IA de alto riesgo, a pesar de cumplir con el presente Reglamento, presenta sin embargo un riesgo para la salud o la seguridad de las personas, para los derechos fundamentales o para otros aspectos de

protección del interés público, pedirá al operador interesado que adopte todas las medidas adecuadas para garantizar que el sistema de IA de que se trate ya no presente ese riesgo cuando se introduzca en el mercado o se ponga en servicio sin demora indebida, dentro de un plazo que dicha autoridad podrá determinar.

2. El proveedor u otro operador pertinente se asegurará de que se adoptan medidas correctoras con respecto a todos los sistemas de IA afectados que haya comercializado en el mercado de la Unión en el plazo determinado por la autoridad de vigilancia del mercado del Estado miembro a que se refiere el apartado 1.

3. Los Estados miembros informarán inmediatamente a la Comisión y a los demás Estados miembros cuando se llegue a una conclusión en virtud del apartado 1. La información facilitada incluirá todos los detalles disponibles, en particular los datos necesarios para detectar el sistema de IA afectado y para determinar su origen y cadena de suministro, la naturaleza del riesgo planteado y la naturaleza y duración de las medidas nacionales adoptadas.

4. La Comisión entablará sin demora indebida consultas con los Estados miembros afectados y los operadores pertinentes y evaluará las medidas nacionales adoptadas. Basándose en los resultados de esta evaluación, la Comisión decidirá si la medida está justificada y, en su caso, propondrá otras medidas adecuadas.

5. La Comisión comunicará inmediatamente su decisión a los Estados miembros afectados y a los operadores pertinentes. Informará asimismo a los demás Estados miembros.

ARTÍCULO 83
INCUMPLIMIENTO FORMAL

1. Cuando la autoridad de vigilancia del mercado de un Estado miembro constate una de las situaciones indicadas a continuación, exigirá al proveedor correspondiente que subsane el incumplimiento de que se trate, dentro de un plazo que dicha autoridad podrá determinar:

   a) se ha colocado el marcado CE contraviniendo el artículo 48;

   b) no se ha colocado el marcado CE;

   c) no se ha elaborado la declaración UE de conformidad con el artículo 47;

   d) no se ha elaborado correctamente la declaración UE de conformidad con el artículo 47;

   e) no se ha efectuado el registro en la base de datos de la UE de conformidad con el artículo 71;

   f) cuando proceda, no se ha designado a un representante autorizado;

   g) no se dispone de documentación técnica.

2. Si el incumplimiento a que se refiere el apartado 1 persiste, la autoridad de vigilancia del mercado del Estado miembro de que se trate adoptará medidas adecuadas y proporcionadas para restringir o prohibir la comercialización del sistema de IA de alto riesgo o para asegurarse de que se recupera o retira del mercado sin demora.

ARTÍCULO 84
ESTRUCTURAS DE APOYO A LOS ENSAYOS DE IA DE LA UNIÓN

1. La Comisión designará una o varias estructuras de apoyo a los ensayos de IA de la Unión para realizar las actividades enumeradas en el artículo 21, apartado 6, del Reglamento (UE) 2019/1020 en el ámbito de la IA.

2. Sin perjuicio de las actividades a que se refiere el apartado 1, las estructuras de apoyo a los ensayos de IA de la Unión también proporcionarán asesoramiento técnico o científico independiente a petición del Consejo de IA, la Comisión o de las autoridades de vigilancia del mercado.

SECCIÓN 4
VÍAS DE RECURSO

ARTÍCULO 85
DERECHO A PRESENTAR UNA RECLAMACIÓN ANTE UNA AUTORIDAD DE VIGILANCIA DEL MERCADO

Sin perjuicio de otras vías administrativas o judiciales de recurso, toda persona física o jurídica que tenga motivos para considerar que se ha infringido lo dispuesto en el presente Reglamento podrá presentar reclamaciones ante la autoridad de vigilancia del mercado pertinente.

De conformidad con el Reglamento (UE) 2019/1020, tales reclamaciones se tendrán en cuenta a la hora de llevar a cabo actividades de vigilancia del mercado y se tramitarán de conformidad con los procedimientos específicos establecidos con este fin por las autoridades de vigilancia del mercado.

ARTÍCULO 86
DERECHO A EXPLICACIÓN DE DECISIONES TOMADAS INDIVIDUALMENTE

1. Toda persona que se vea afectada por una decisión que el responsable del despliegue adopte basándose en los resultados de salida de un sistema de IA de alto riesgo que figure en el anexo III, con excepción de los sistemas enumerados en su punto 2, y que produzca efectos jurídicos o le afecte considerablemente del mismo modo, de manera que considere que tiene un efecto perjudicial para su salud, su seguridad o sus derechos fundamentales, tendrá derecho a obtener del responsable del despliegue explicaciones claras y significativas acerca del papel que el sistema de IA ha tenido en el proceso de toma de decisiones y los principales elementos de la decisión adoptada.

2. No se aplicará el apartado 1 a la utilización de sistemas de IA para los que existan excepciones o restricciones a la obligación prevista en dicho apartado derivadas del Derecho de la Unión o nacional de conformidad con el Derecho de la Unión.

3. El presente artículo se aplicará únicamente en la medida en que el derecho a que se refiere el apartado 1 no esté previsto de otro modo en el Derecho de la Unión.

ARTÍCULO 87
DENUNCIA DE INFRACCIONES Y PROTECCIÓN DE LOS DENUNCIANTES

La Directiva (UE) 2019/1937 se aplicará a la denuncia de infracciones del presente Reglamento y a la protección de las personas que denuncien tales infracciones.

SECCIÓN 5
SUPERVISIÓN, INVESTIGACIÓN, CUMPLIMIENTO Y SEGUIMIENTO RESPECTO DE PROVEEDORES DE MODELOS DE IA DE USO GENERAL

ARTÍCULO 88
CUMPLIMIENTO DE LAS OBLIGACIONES DE LOS PROVEEDORES DE MODELOS DE IA DE USO GENERAL

1. La Comisión tendrá competencias exclusivas para supervisar y hacer cumplir el capítulo V, teniendo en cuenta las garantías procedimentales previstas en el artículo 94. La Comisión debe confiar la ejecución de estas tareas a la Oficina de IA, sin perjuicio de las competencias de organización de la Comisión y del reparto de competencias entre los Estados miembros y la Unión en virtud de los Tratados.
2. Sin perjuicio de lo dispuesto en el artículo 75, apartado 3, las autoridades de vigilancia del mercado podrán solicitar a la Comisión que ejerza las facultades previstas en la presente sección, cuando resulte necesario y proporcionado para ayudar a que se lleven a cabo las actividades de su competencia en virtud del presente Reglamento.

ARTÍCULO 89
MEDIDAS DE SEGUIMIENTO

1. Con el fin de llevar a cabo los cometidos que se le atribuyen en la presente sección, la Oficina de IA podrá tomar las medidas necesarias para supervisar la aplicación y cumplimiento efectivos del presente Reglamento por parte de los proveedores de modelos de IA de uso general, incluida su observancia de los códigos de buenas prácticas aprobados.
2. Los proveedores posteriores tendrán derecho a presentar reclamaciones alegando infracciones del presente Reglamento. Las reclamaciones deberán motivarse debidamente e indicar, como mínimo:
   a) el punto de contacto del proveedor del modelo de IA de uso general de que se trate;
   b) una descripción de los hechos, las disposiciones del presente Reglamento afectadas y los motivos por los que el proveedor posterior considera que el proveedor del modelo de IA de uso general de que se trate ha infringido el presente Reglamento;
   c) cualquier otra información que el proveedor posterior que presente la reclamación considere pertinente, como, por ejemplo, en su caso, información que haya recopilado por iniciativa propia.

ARTÍCULO 90
ALERTAS DEL GRUPO DE EXPERTOS CIENTÍFICOS SOBRE RIESGOS SISTÉMICOS

1. El grupo de expertos científicos podrá proporcionar alertas cualificadas a la Oficina de IA cuando tenga motivos para sospechar que:
   a) un modelo de IA de uso general plantea un riesgo concreto reconocible a escala de la Unión, o
   b) un modelo de IA de uso general reúne las condiciones a que se refiere el artículo 51.
2. Tras recibir dicha alerta cualificada, la Comisión podrá ejercer, a través de la Oficina de IA y tras haber informado al Consejo de IA, las facultades previstas en la presente sección con el fin de evaluar la cuestión. La Oficina de IA informará al Consejo de IA de cualquier medida que se adopte de conformidad con los artículos 91 a 94.
3. Las alertas cualificadas deberán motivarse debidamente e indicar, como mínimo:
   a) el punto de contacto del proveedor del modelo de IA de uso general con riesgo sistémico de que se trate;
   b) una descripción de los hechos y los motivos por los que el grupo de expertos científicos proporciona la alerta;
   c) cualquier otra información que el grupo de expertos científicos considere pertinente, como, por ejemplo, en su caso, información que haya recopilado por iniciativa propia.

ARTÍCULO 91
PODERES PARA SOLICITAR DOCUMENTACIÓN E INFORMACIÓN

1. La Comisión podrá solicitar al proveedor del modelo de IA de uso general interesado que facilite la documentación preparada por el proveedor de conformidad con los artículos 53 y 55, o cualquier otra información que sea necesaria para evaluar el cumplimiento del presente Reglamento por parte del proveedor.
2. Antes de enviar la solicitud de información, la Oficina de IA podrá entablar un diálogo estructurado con el proveedor del modelo de IA de uso general.
3. Cuando el grupo de expertos científicos presente la correspondiente solicitud debidamente motivada, la Comisión podrá dirigir al proveedor de un modelo de IA de uso general una solicitud de información si el acceso a dicha información resulta necesario y proporcionado para que el grupo de expertos científicos pueda llevar a cabo sus cometidos en virtud del artículo 68, apartado 2.
4. La solicitud de información indicará la base jurídica y la finalidad de la solicitud, precisará qué información se requiere, fijará el plazo en el que deberá facilitarse la información e indicará las multas que se establecen en el artículo 101 por facilitar información incorrecta, incompleta o engañosa.
5. El proveedor del modelo de IA de uso general interesado, o su representante, facilitará la información solicitada. De tratarse de personas jurídicas, sociedades o empresas, o cuando el proveedor carezca de personalidad jurídica, las personas habilitadas por ley o por sus estatutos para representarlas facilitarán la información solicitada en nombre del proveedor del modelo de IA de uso general interesado. Los abogados debidamente habilitados podrán facilitar la información en nombre de sus representados. Los representados seguirán siendo, no obstante, plenamente responsables, si la información facilitada es incompleta, incorrecta o engañosa.

ARTÍCULO 92
PODERES PARA REALIZAR EVALUACIONES

1. La Oficina de IA, previa consulta al Consejo de IA, podrá realizar evaluaciones del modelo de IA de uso general de que se trate con el fin de:
   a) evaluar si el proveedor cumple sus obligaciones en virtud del presente Reglamento, cuando la información recabada con arreglo al artículo 91 resulte insuficiente, o

b) investigar riesgos sistémicos a escala de la Unión de modelos de IA de uso general con riesgo sistémico, en particular a raíz de una alerta cualificada del grupo de expertos científicos de conformidad con el artículo 90, apartado 1, letra a).

2. La Comisión podrá decidir nombrar a expertos independientes para que realicen las evaluaciones en su nombre, también expertos científicos del grupo establecido de conformidad con el artículo 68. Los expertos independientes que se nombren para realizar estas tareas cumplirán los criterios establecidos en el artículo 68, apartado 2.

3. A los efectos del apartado 1, la Comisión podrá solicitar el acceso al modelo de IA de uso general de que se trate a través de API o de otros medios y herramientas técnicos adecuados, como, por ejemplo, el código fuente.

4. La solicitud de acceso indicará la base jurídica, la finalidad y los motivos de la solicitud, y fijará el plazo durante el que deberá facilitarse el acceso y las multas que se establecen en el artículo 101 por no facilitarlo.

5. Los proveedores del modelo de IA de uso general interesados o su representante facilitarán la información solicitada. En caso de que se trate de personas jurídicas, sociedades o empresas, o cuando el proveedor carezca de personalidad jurídica, las personas habilitadas por ley o por sus estatutos para representarlas, facilitarán el acceso solicitado en nombre del proveedor del modelo de IA de uso general interesado.

6. La Comisión adoptará actos de ejecución en los que se establezcan las modalidades detalladas y las condiciones de las evaluaciones, incluidas las disposiciones detalladas para la participación de expertos independientes y el procedimiento para su selección. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 98, apartado 2.

7. Antes de solicitar el acceso al modelo de IA de uso general de que se trate, la Oficina de IA podrá entablar un diálogo estructurado con el proveedor del modelo de IA de uso general para recabar más información sobre los ensayos internos del modelo, las salvaguardias internas para prevenir los riesgos sistémicos y otros procedimientos y medidas internos que el proveedor haya adoptado para mitigar tales riesgos.

ARTÍCULO 93
PODERES PARA SOLICITAR LA ADOPCIÓN DE MEDIDAS

1. Cuando resulte necesario y conveniente, la Comisión podrá solicitar a los proveedores que:

a) adopten las medidas oportunas para cumplir las obligaciones establecidas en los artículos 53 y 54;

b) apliquen medidas de reducción de riesgos cuando la evaluación realizada de conformidad con el artículo 92 apunte a que existen motivos serios y fundados de preocupación por la existencia de un riesgo sistémico a escala de la Unión;

c) restrinjan la comercialización del modelo, lo retiren o lo recuperen.

2. Antes de solicitar que se adopten medidas, la Oficina de IA podrá entablar un diálogo estructurado con el proveedor del modelo de IA de uso general.

3. Si, durante el diálogo estructurado a que se refiere el apartado 2, el proveedor del modelo de IA de uso general con riesgo sistémico se compromete a adoptar medidas de reducción para hacer frente a un riesgo sistémico a escala de la Unión, la Comisión podrá, mediante una decisión, hacer dichos compromisos vinculantes y declarar que no hay ya motivos para actuar.

ARTÍCULO 94
GARANTÍAS PROCESALES DE LOS OPERADORES ECONÓMICOS DEL MODELO DE IA DE USO GENERAL

El artículo 18 del Reglamento (UE) 2019/1020 se aplicará mutatis mutandis a los proveedores del modelo de IA de uso general, sin perjuicio de las garantías procesales más específicas previstas en el presente Reglamento.

Fuente: Reglamento (UE) 2024/1689, texto consolidado a 27 de julio de 2026. Transcripción del PDF aportado; se han omitido las marcas editoriales de consolidación y las cabeceras de página.

Resumen del Capítulo IX — Vigilancia, control e incumplimientos de los sistemas de IA

Reglamento (UE) 2024/1689 · Texto consolidado a 27/07/2026 · Páginas 87–112 · Artículos 72 a 94, incluidos los nuevos artículos 75 bis a 75 quinquies

Este es uno de los capítulos más importantes del Reglamento para comprender **qué ocurre cuando una empresa ya ha comercializado o puesto en funcionamiento un sistema de inteligencia artificial**.

Mientras que el capítulo III establece las obligaciones que deben cumplir determinados sistemas de alto riesgo, el capítulo IX explica cómo se supervisa su cumplimiento, cómo se investigan los incidentes y qué medidas pueden adoptar las autoridades.

Además, regula los derechos de las personas afectadas y las facultades de control sobre los proveedores de modelos de IA de uso general.

Idea principal: cumplir la normativa en el momento de instalar una IA no es suficiente. Cuando corresponda, debe vigilarse su funcionamiento durante toda su vida útil y corregirse cualquier riesgo que pueda aparecer.

El capítulo está dividido en cinco secciones.

1. Sección 1 — Vigilancia posterior a la comercialización

Artículo 72 · Páginas 87–88

Artículo 72. Vigilancia poscomercialización de sistemas de alto riesgo

Los proveedores de sistemas de IA de alto riesgo deben establecer un sistema de vigilancia que permita comprobar que sus productos siguen cumpliendo los requisitos después de su comercialización.

Este sistema debe recopilar, documentar y analizar información sobre su funcionamiento durante toda su vida útil.

¿Qué supone en la práctica?

Obligación	Aplicación empresarial
Seguimiento continuo	Controlar cómo funciona la solución una vez implantada.
Recopilación de información	Recibir información relevante de clientes y otras fuentes.
Análisis de incidencias	Identificar errores, desviaciones y riesgos.
Revisión de cumplimiento	Comprobar que siguen cumpliéndose los requisitos legales.
Plan documentado	Mantener un plan de vigilancia como parte de la documentación técnica.

Ejemplo en un ERP

Una empresa desarrolla un sistema de IA de alto riesgo para evaluar candidatos a puestos de trabajo y lo integra con una solución de recursos humanos.

Después de comercializarlo, el proveedor debe seguir comprobando si el sistema genera resultados incorrectos, presenta sesgos discriminatorios o incumple los requisitos establecidos.

No basta con haberlo probado antes de la implantación.

Importante: la obligación de implantar este sistema de vigilancia corresponde al proveedor del sistema de alto riesgo. La empresa cliente también puede tener obligaciones propias de seguimiento y comunicación conforme al artículo 26.

La versión consolidada de 2026 establece que la Comisión deberá adoptar orientaciones, incluido un modelo para el plan de vigilancia, a más tardar el **2 de septiembre de 2027**.

2. Sección 2 — Comunicación de incidentes graves

Artículo 73 · Páginas 88–89

Artículo 73. Notificación de incidentes graves

Los proveedores de sistemas de IA de alto riesgo deben comunicar los incidentes graves a las autoridades competentes, conforme a las condiciones previstas en el Reglamento.

Un incidente grave puede comprender situaciones como fallecimientos, daños graves a la salud, alteraciones graves de infraestructuras críticas o determinadas vulneraciones de derechos fundamentales.

Plazos para comunicar incidentes

Plazo máximo	Incidente	Actuación
15 días	Incidentes graves con carácter general	Comunicación inmediata una vez establecido el vínculo causal o su probabilidad razonable, y dentro del plazo máximo aplicable.
2 días	Infracciones generalizadas o determinados incidentes graves	Notificación inmediata y, como máximo, dentro de los dos días desde que se tenga conocimiento.
10 días	Fallecimiento de una persona	Notificación inmediata cuando se establezca o sospeche la relación causal, con el límite máximo específico de diez días.

Los plazos se calculan según los supuestos y puntos de partida concretos del artículo 73. No representan períodos de espera: la obligación es actuar inmediatamente cuando corresponda.

¿Qué debe hacerse después de comunicar un incidente?

El proveedor tiene que investigar lo ocurrido, evaluar los riesgos, adoptar las medidas correctoras necesarias y colaborar con las autoridades.

También se permite presentar inicialmente una comunicación incompleta cuando sea necesario para respetar los plazos, seguida posteriormente de una notificación completa.

Ejemplo empresarial

Un sistema de IA de alto riesgo empleado para tomar decisiones sobre personas provoca un incidente que puede encajar en la definición legal de incidente grave.

El proveedor debe investigar y comunicarlo cuando concurran los requisitos del artículo 73.

La empresa que utiliza la solución, por su parte, debe cumplir las obligaciones de aviso y actuación que le correspondan, incluidas las del artículo 26.

Punto importante: no cualquier error de una IA constituye automáticamente un incidente grave notificable. Debe analizarse la definición del Reglamento y las circunstancias del caso.

3. Sección 3 — Vigilancia del mercado y garantía del cumplimiento

Artículos 74 a 84 · Páginas 90–108

Esta es la sección más extensa del capítulo y una de las que más consecuencias prácticas tiene para los proveedores de IA.

Establece las facultades de las autoridades para comprobar el cumplimiento, investigar posibles infracciones, exigir correcciones y adoptar medidas sobre los sistemas que presenten riesgos.

Artículo 74. Vigilancia del mercado

Las autoridades de vigilancia pueden supervisar los sistemas de IA comercializados en la Unión Europea.

El Reglamento establece mecanismos de coordinación con las autoridades sectoriales y con otras instituciones competentes.

Entre las actuaciones posibles, conforme a las facultades legales aplicables, se encuentran las investigaciones, las solicitudes de documentación y la adopción de medidas correctoras.

Ejemplo: una autoridad recibe información sobre un sistema de IA de alto riesgo que podría estar incumpliendo los requisitos de supervisión humana o de calidad de los datos. Puede iniciar las comprobaciones correspondientes.

Artículo 75. Supervisión de determinados sistemas por la Oficina Europea de IA

Modificado sustancialmente en 2026

La versión consolidada amplía las competencias de la Oficina de IA.

Se le atribuye supervisión exclusiva de determinados sistemas, principalmente:

- Sistemas basados en modelos de IA de uso general cuando el modelo y el sistema son desarrollados por el mismo proveedor o por empresas del mismo grupo, con las excepciones legales.
- Sistemas de IA que constituyan o estén integrados en plataformas en línea o motores de búsqueda de muy gran tamaño designados conforme a la normativa europea.

Existen excepciones para determinadas aplicaciones sectoriales, de infraestructuras críticas, autoridades públicas, entidades financieras y administración de justicia.

También se regulan mecanismos de cooperación y asistencia entre la Oficina de IA y las autoridades nacionales.

Aplicación empresarial: utilizar un modelo GPT, Claude o Llama en un ERP no significa automáticamente que la Oficina Europea de IA tenga competencia exclusiva sobre toda esa integración. Es necesario determinar quién ha desarrollado el modelo y el sistema, así como su finalidad y las excepciones aplicables.

Nuevos artículos 75 bis a 75 quinquies

La modificación de 2026 desarrolla de forma más detallada las facultades de supervisión y ejecución de la Oficina Europea de IA.

Artículo	Contenido	Consecuencia
75 bis	Facultades de investigación y supervisión	Solicitar documentación, acceder a sistemas, investigar e inspeccionar, con las garantías establecidas.
75 ter	Compromisos de cumplimiento	Permitir que los operadores ofrezcan compromisos que pueden convertirse en jurídicamente vinculantes.
75 quater	Incumplimientos y sanciones	Declarar infracciones, ordenar medidas correctoras e imponer multas en los supuestos previstos.
75 quinquies	Salvaguardias y derechos de defensa	Garantizar los derechos procesales, el acceso al expediente y las garantías de confidencialidad.

Estas disposiciones son importantes porque refuerzan los mecanismos de control sobre los sistemas sujetos a competencia de la Oficina de IA.

Por ejemplo, el artículo 75 bis contempla inspecciones presenciales o a distancia y solicitudes de acceso a sistemas de IA.

El artículo 75 quater permite imponer multas sancionadoras y coercitivas dentro de su ámbito de aplicación, conforme a las condiciones establecidas.

Importante: estas competencias no permiten inspecciones arbitrarias. Deben respetarse los requisitos procedimentales, los derechos de defensa y, cuando corresponda, las autorizaciones judiciales.

Artículo 76. Supervisión de pruebas en condiciones reales

Las autoridades pueden controlar las pruebas de sistemas de IA realizadas en entornos reales.

Cuando detecten riesgos o incumplimientos, pueden ordenar modificaciones, suspender las pruebas o ponerles fin.

Este artículo conecta directamente con el capítulo VI, relativo al apoyo a la innovación.

Artículo 77. Protección de los derechos fundamentales

Establece la cooperación entre las autoridades de vigilancia del mercado y los organismos públicos responsables de proteger los derechos fundamentales, incluido el derecho a la no discriminación.

La modificación de 2026 refuerza los mecanismos de intercambio de información y asistencia mutua.

Ejemplo: si una IA utilizada en la selección de personal presenta indicios de discriminación, las autoridades competentes pueden colaborar dentro de sus respectivas atribuciones.

Artículo 78. Confidencialidad

Las autoridades y demás participantes en la aplicación del Reglamento deben proteger la información confidencial obtenida durante sus actuaciones.

Esto comprende, entre otros aspectos, la protección de los secretos comerciales, la propiedad intelectual y la información cuya divulgación pueda comprometer determinados intereses protegidos.

Aplicación empresarial: la existencia de una investigación no significa que toda la información técnica o comercial de una empresa deba hacerse pública.

Artículos 79 a 84. Medidas ante riesgos e incumplimientos

Artículo	Situación regulada	Medida prevista
79	Sistemas de IA que presentan riesgos	Evaluación y exigencia de medidas correctoras o restrictivas.
80	Sistemas clasificados incorrectamente como no de alto riesgo	Revisión de la clasificación, exigencia de cumplimiento y posibles sanciones.
81	Desacuerdos entre Estados miembros sobre medidas nacionales	Procedimiento de salvaguardia y decisión de la Comisión.
82	Sistemas que cumplen formalmente la normativa, pero presentan riesgos	Exigencia de medidas para eliminar o reducir esos riesgos.
83	Incumplimientos formales	Corrección de deficiencias documentales, de registro o de marcado CE, entre otras.
84	Estructuras europeas de apoyo a los ensayos	Apoyo técnico y científico para las actividades de evaluación y control.

Dos aspectos especialmente importantes

Primero: clasificar incorrectamente un sistema no evita la regulación.

El artículo 80 permite que una autoridad revise un sistema que el proveedor haya considerado no sujeto a la categoría de alto riesgo.

Si comprueba que sí lo es, puede exigir su adaptación y adoptar las medidas legalmente previstas.

Segundo: cumplir formalmente la normativa no garantiza que un sistema pueda continuar utilizándose sin cambios.

El artículo 82 permite actuar cuando un sistema de alto riesgo presenta riesgos relevantes, aunque cumpla los requisitos formales.

Esto significa que el cumplimiento debe mantenerse durante toda su utilización.

4. Sección 4 — Derechos de reclamación y explicación

Artículos 85 a 87 · Páginas 108–109

Especialmente importante para empresas y trabajadores

Esta sección reconoce mecanismos de protección para las personas afectadas por sistemas de IA.

Artículo 85. Derecho a presentar reclamaciones

Cualquier persona física o jurídica que tenga motivos para considerar que se ha infringido el Reglamento puede presentar una reclamación ante la autoridad de vigilancia del mercado correspondiente.

Las reclamaciones deben tramitarse conforme a los procedimientos establecidos.

Artículo 86. Derecho a recibir explicaciones sobre determinadas decisiones

Este artículo reconoce un derecho especialmente relevante.

Cuando una persona resulta afectada por una decisión adoptada basándose en los resultados de un sistema de IA de alto riesgo del anexo III, en las condiciones establecidas, puede solicitar explicaciones claras y significativas sobre:

- El papel que tuvo la IA en el proceso de decisión.
- Los principales elementos de la decisión adoptada.

Este derecho está sujeto a las condiciones y excepciones del artículo, entre ellas que la decisión produzca efectos jurídicos o afecte significativamente a la persona en los términos previstos.

Ejemplo empresarial

Una empresa utiliza una IA de alto riesgo para evaluar candidatos y toma una decisión de contratación basándose en sus resultados.

Cuando concurran las condiciones del artículo 86, la persona afectada puede tener derecho a conocer qué papel desempeñó el sistema y los elementos principales de la decisión.

Por ello, **las empresas deben prestar especial atención a la trazabilidad y explicabilidad de los sistemas de IA que intervienen en decisiones sobre personas**.

Artículo 87. Protección de denunciantes

Este artículo establece que la Directiva europea sobre protección de las personas que informan de infracciones se aplica a las denuncias de incumplimientos del Reglamento de IA.

Conecta la normativa de inteligencia artificial con los mecanismos de protección de denunciantes.

5. Sección 5 — Supervisión de los proveedores de modelos de IA de uso general

Artículos 88 a 94 · Páginas 109–112

Esta sección desarrolla cómo se controla el cumplimiento de las obligaciones del capítulo V, relativas a los modelos de IA de uso general.

Artículos 88 y 89. Supervisión y seguimiento

La Comisión Europea tiene competencias exclusivas para supervisar y hacer cumplir las obligaciones del capítulo V, mediante la Oficina de IA en los términos del Reglamento.

Además, se contemplan mecanismos de seguimiento y reclamación por parte de proveedores posteriores que integran modelos de IA de uso general en sus sistemas.

Artículo 90. Alertas sobre riesgos sistémicos

Los expertos científicos independientes pueden emitir alertas cuando detecten indicios de riesgos sistémicos o de que un modelo cumple las condiciones para ser clasificado como tal.

Estas alertas pueden dar lugar a actuaciones de evaluación e investigación.

Artículo 91. Solicitud de información

La Comisión puede requerir a los proveedores documentación técnica e información necesaria para comprobar el cumplimiento de las obligaciones aplicables.

Artículo 92. Evaluaciones de modelos

La Oficina de IA puede realizar evaluaciones en los supuestos establecidos y, cuando corresponda, solicitar acceso técnico al modelo, incluso mediante APIs u otros medios adecuados.

Artículo 93. Medidas correctoras

La Comisión puede exigir a los proveedores de modelos de uso general que adopten las medidas previstas en el artículo.

Entre ellas figuran las necesarias para cumplir determinadas obligaciones, mitigar riesgos sistémicos y, cuando resulte necesario, restringir la comercialización o retirar el modelo.

Artículo 94. Garantías procesales

Establece garantías procedimentales para los proveedores de modelos de IA de uso general.

Su finalidad es asegurar que las actuaciones de supervisión respeten los derechos reconocidos por la normativa aplicable.

6. ¿Cómo afecta el capítulo IX a las empresas?

La repercusión depende de si una empresa desarrolla un sistema, lo comercializa o simplemente lo utiliza.

Perfil empresarial	Responsabilidades especialmente relevantes
Fabricante de sistemas de IA de alto riesgo	Vigilancia posterior, gestión de incidentes y adopción de medidas correctoras.
Integrador de IA	Determinar si asume obligaciones de proveedor y asegurar el cumplimiento que le corresponda.
Empresa usuaria de IA de alto riesgo	Supervisión del uso, comunicación de riesgos y colaboración con las autoridades cuando proceda.
Proveedor de modelos de uso general	Documentación, cooperación y sometimiento a los mecanismos de supervisión aplicables.
Empresa que toma decisiones sobre personas con IA de alto riesgo	Atención a los derechos de información y explicación, cuando concurran los requisitos legales.

7. Aplicación práctica a Sage 200 y sus integraciones

Veamos cómo se traduciría este capítulo a distintos usos de IA en un ERP.

Aplicación	Principal aspecto que debe analizarse
IA para contabilización automática de facturas	Calidad de resultados, control de errores y obligaciones generales aplicables, sin presumir que sea de alto riesgo.
Agente conectado a Sage 200 mediante MCP	Permisos de acceso, trazabilidad y responsabilidades según la clasificación del sistema.
IA para evaluación de candidatos	Seguimiento de riesgos, prevención de sesgos y derechos de los afectados si es de alto riesgo.
IA para valorar el rendimiento de trabajadores	Supervisión, medidas correctoras y posibles derechos de explicación.
IA industrial conectada al ERP y a maquinaria	Vigilancia de los riesgos para la seguridad y coordinación con la normativa sectorial.
Modelo de IA de uso general integrado en un ERP	Diferenciación entre las obligaciones del fabricante del modelo y las del proveedor del sistema integrado.

Ejemplo: un agente de IA conectado a Sage 200

Imaginemos un agente que consulta saldos, prepara propuestas comerciales y puede ejecutar determinadas operaciones autorizadas en el ERP.

La integración no se considera automáticamente de alto riesgo.

Sin embargo, desde el punto de vista de una implantación responsable, convendría mantener controles sobre los permisos, el registro de operaciones, la revisión de resultados y la gestión de incidencias.

Estas son recomendaciones prácticas. **No todas constituyen obligaciones específicas impuestas por el capítulo IX a cualquier asistente de IA**.

Si posteriormente la solución se amplía para tomar o apoyar decisiones clasificadas como de alto riesgo, habrá que revisar las obligaciones legales correspondientes.

8. Calendario de aplicación

El capítulo IX se aplica con carácter general desde el **2 de agosto de 2026**, según el artículo 113 del texto consolidado.

Existen particularidades importantes: el artículo 78, relativo a confidencialidad, es aplicable desde el 2 de agosto de 2025, y la exigibilidad de determinadas obligaciones vinculadas a sistemas de alto riesgo debe interpretarse conjuntamente con las fechas del capítulo III y las disposiciones transitorias.

Por tanto, no todas las obligaciones de vigilancia relacionadas con sistemas de alto riesgo tienen necesariamente la misma fecha efectiva.

9. Conclusión del capítulo IX

El capítulo IX establece que la vigilancia de la inteligencia artificial **no termina cuando se vende, certifica o instala una solución**.

Sus principales consecuencias son:

- Los proveedores de sistemas de alto riesgo deben realizar un seguimiento de su funcionamiento durante su vida útil.
- Los incidentes graves deben comunicarse conforme a las condiciones y plazos legales.
- Las autoridades pueden investigar incumplimientos, requerir información y exigir medidas correctoras.

- Una clasificación incorrecta como sistema no sujeto a alto riesgo puede ser revisada.
- Los sistemas que presentan riesgos pueden ser objeto de medidas incluso aunque cumplan formalmente determinados requisitos.
- Las personas afectadas disponen de mecanismos de reclamación y, en determinados casos, de un derecho a recibir explicaciones.
- Los proveedores de modelos de IA de uso general están sometidos a mecanismos específicos de supervisión europea.

La conclusión más relevante para el mundo empresarial y los ERP es que la IA debe seguir siendo controlable, supervisable y corregible después de su implantación.

En las integraciones de IA con Sage 200, esto cobra especial importancia cuando las herramientas dejan de limitarse a consultar información y pasan a intervenir en procesos sensibles, decisiones sobre personas o funciones que puedan afectar a su seguridad o sus derechos.

Resumen basado en los artículos 72 a 94 del documento consolidado aportado, incluidas las modificaciones de 2026.

TEXTO OFICIAL · CAPÍTULO X

CAPÍTULO X
CÓDIGOS DE CONDUCTA Y DIRECTRICES

ARTÍCULO 95
CÓDIGOS DE CONDUCTA PARA LA APLICACIÓN VOLUNTARIA DE REQUISITOS ESPECÍFICOS

1. La Oficina de IA y los Estados miembros fomentarán y facilitarán la elaboración de códigos de conducta, con los correspondientes mecanismos de gobernanza, destinados a fomentar la aplicación voluntaria de alguno o de todos los requisitos establecidos en el capítulo III, sección 2, a los sistemas de IA que no sean de alto riesgo, teniendo en cuenta las soluciones técnicas disponibles y las mejores prácticas del sector que permitan la aplicación de dichos requisitos.
2. La Oficina de IA y los Estados miembros facilitarán la elaboración de códigos de conducta relativos a la aplicación voluntaria, también por parte de los responsables del despliegue, de requisitos específicos para todos los sistemas de IA, sobre la base de objetivos claros e indicadores clave de resultados para medir la consecución de dichos objetivos, incluidos, entre otros pero no exclusivamente, elementos como:
   a) los elementos aplicables establecidos en las Directrices éticas de la Unión para una IA fiable;
   b) la evaluación y reducción al mínimo de las repercusiones de los sistemas de IA en la sostenibilidad medioambiental, también por cuanto se refiere a la programación eficiente desde el punto de vista energético y las técnicas para diseñar, entrenar y utilizar la IA de manera eficiente;
   c) la promoción de la alfabetización en materia de IA, en particular en el caso de las personas que se ocupan del desarrollo, funcionamiento y utilización de la IA;
   d) la facilitación de un diseño inclusivo y diverso de los sistemas de IA, por ejemplo mediante la creación de equipos de desarrollo inclusivos y diversos y la promoción de la participación de las partes interesadas en dicho proceso;
   e) la evaluación y prevención de los perjuicios de los sistemas de IA para las personas vulnerables o los colectivos de personas vulnerables, también por cuanto se refiere a accesibilidad para las personas con discapacidad, así como para la igualdad de género.
3. Los códigos de conducta podrán ser elaborados por proveedores o responsables del despliegue de sistemas de IA particulares, por las organizaciones que los representen o por ambos, también con la participación de cualquier parte interesada y sus organizaciones representativas, como, por ejemplo, las organizaciones de la sociedad civil y el mundo académico. Los códigos de conducta podrán comprender uno o varios sistemas de IA en función de la similitud de la finalidad prevista de los distintos sistemas.
4. La Oficina de IA y los Estados miembros tendrán en cuenta los intereses y necesidades específicos de las pymes, incluidas las empresas emergentes y las pequeñas empresas de mediana capitalización, a la hora de fomentar y facilitar la elaboración de códigos de conducta.

ARTÍCULO 96
DIRECTRICES DE LA COMISIÓN SOBRE LA APLICACIÓN DEL PRESENTE REGLAMENTO

1. La Comisión elaborará directrices sobre la aplicación práctica del presente Reglamento y, en particular, sobre:
   a) la aplicación de los requisitos y obligaciones a que se refieren los artículos 8 a 15 y los artículos 25 y 26;
   b) las prácticas prohibidas a que se refiere el artículo 5;
   c) la aplicación práctica de las disposiciones relacionadas con modificaciones sustanciales;
   d) la aplicación práctica de las obligaciones de transparencia establecidas en el artículo 50;
   e) información detallada sobre la relación entre el presente Reglamento y la lista de actos legislativos de armonización de la Unión enumerados en el anexo I, así como otras disposiciones de Derecho de la Unión pertinentes, también por cuanto se refiere a la coherencia en su aplicación;
   f) la aplicación de la definición de sistema de IA que figura en el artículo 3, punto 1 ;
   g) la aplicación práctica del artículo 8, apartado 2, el artículo 9, apartado 10, y el artículo 17, apartado 3, de conformidad con los principios de complementariedad y proporcionalidad, con vistas a garantizar la coherencia, evitar duplicaciones y reducir al mínimo las cargas adicionales a la hora de cumplir los requisitos del presente Reglamento y los requisitos de los actos legislativos de armonización de la Unión enumerados en el anexo I, sección A; dichas directrices se publicarán a más tardar el 1 de agosto de 2027.

   Al publicar estas directrices, la Comisión implicará al Consejo de IA y prestará especial atención a las necesidades de las pymes, incluidas las empresas emergentes y las pequeñas empresas de mediana capitalización, de las autoridades públicas locales y de los sectores que tengan más probabilidades de verse afectados por el presente Reglamento.

   Las directrices a que se refiere el párrafo primero del presente apartado tendrán debidamente en cuenta el estado de la técnica generalmente reconocido en materia de IA, así como las normas armonizadas y especificaciones comunes pertinentes a que se refieren los artículos 40 y 41, o las normas armonizadas o especificaciones técnicas que se establezcan con arreglo al Derecho de armonización de la Unión.
2. A petición de los Estados miembros o de la Oficina de IA, o por propia iniciativa, la Comisión actualizará las directrices anteriormente adoptadas cuando se considere necesario.

Fuente: Reglamento (UE) 2024/1689, texto consolidado a 27 de julio de 2026. Transcripción del PDF aportado; se han omitido las marcas editoriales de consolidación y las cabeceras de página.

Resumen del Capítulo X — Códigos de conducta y directrices

Reglamento (UE) 2024/1689 · Texto consolidado a 27/07/2026 · Páginas 112–114 · Artículos 95 y 96

Este capítulo establece mecanismos para **facilitar que las empresas adopten buenas prácticas de inteligencia artificial y comprendan cómo cumplir correctamente el Reglamento europeo**.

Es especialmente interesante para las empresas que utilizan IA de riesgo limitado o mínimo, porque fomenta la aplicación voluntaria de medidas de seguridad, transparencia, supervisión humana y buenas prácticas.

La idea fundamental es que una empresa puede adoptar estándares de IA responsable incluso cuando su sistema no está clasificado como de alto riesgo.

El capítulo contiene dos artículos.

1. Artículo 95. Códigos de conducta para la aplicación voluntaria de requisitos específicos

Páginas 112–113

Este artículo establece que la Oficina Europea de IA y los Estados miembros fomentarán la elaboración de códigos de conducta voluntarios.

Su finalidad es promover que los proveedores y usuarios de sistemas de IA que no son de alto riesgo adopten parte o la totalidad de los requisitos técnicos y organizativos establecidos para los sistemas de alto riesgo en el capítulo III.

¿Qué medidas pueden adoptar voluntariamente las empresas?

Ámbito	Aplicación empresarial
Gestión de riesgos	Identificar posibles perjuicios derivados de la utilización de IA.
Calidad de los datos	Comprobar la fiabilidad y pertinencia de la información utilizada.
Transparencia	Informar claramente sobre las capacidades y limitaciones de la IA.
Supervisión humana	Establecer mecanismos de revisión e intervención.
Trazabilidad	Registrar operaciones y decisiones relevantes.
Ciberseguridad	Proteger el sistema frente a accesos indebidos y manipulaciones.

Estas son medidas asociadas a los requisitos del capítulo III que pueden incorporarse voluntariamente mediante códigos de conducta.

Importante: un código voluntario no convierte automáticamente un sistema ordinario en uno de alto riesgo, ni elimina las obligaciones legales que ya sean exigibles.

Otros ámbitos de buenas prácticas

El artículo 95.2 contempla además códigos aplicables voluntariamente a todos los sistemas de IA, con objetivos e indicadores que permitan medir sus resultados.

Ética e IA fiable

Promover el desarrollo y uso de sistemas respetuosos con los principios europeos de inteligencia artificial fiable.

Sostenibilidad medioambiental

Evaluar y reducir el consumo energético y otros impactos ambientales del diseño, entrenamiento y utilización de IA.

Formación y alfabetización

Mejorar los conocimientos sobre IA de las personas que desarrollan, operan y utilizan los sistemas.

Diseño inclusivo y diverso

Fomentar la diversidad de los equipos y la participación de las partes interesadas en el desarrollo de sistemas.

Protección de personas vulnerables

Prevenir perjuicios, facilitar la accesibilidad y promover la igualdad de género.

¿Quién puede elaborar estos códigos?

Los códigos de conducta pueden ser desarrollados por proveedores de IA, responsables del despliegue, asociaciones empresariales y otras organizaciones interesadas, con participación de entidades de la sociedad civil y del ámbito académico.

La modificación de 2026 establece expresamente que, al fomentar estos códigos, deben considerarse las necesidades de las pymes, las empresas emergentes y las pequeñas empresas de mediana capitalización.

2. Artículo 96. Directrices de la Comisión Europea

Páginas 113–114

Este artículo establece que la Comisión Europea elaborará directrices para facilitar la aplicación práctica del Reglamento.

Su finalidad es ayudar a las empresas, desarrolladores, proveedores y autoridades a interpretar correctamente las obligaciones legales.

¿Sobre qué cuestiones deben elaborarse directrices?

Ámbito	Qué deben aclarar
Sistemas de IA de alto riesgo	Aplicación de los requisitos técnicos de los artículos 8–15 y de determinadas obligaciones de los artículos 25 y 26.
Prácticas prohibidas	Interpretación práctica de las prohibiciones del artículo 5.
Modificaciones sustanciales	Cuándo un cambio en un sistema tiene consecuencias regulatorias.
Transparencia	Aplicación de las obligaciones del artículo 50.
Normativa sectorial	Relación entre el Reglamento de IA y otras normas europeas aplicables.
Definición de sistema de IA	Criterios para determinar qué tecnologías entran en el ámbito del Reglamento.
Cumplimiento conjunto	Cómo evitar duplicidades con requisitos de otras normas europeas sobre productos.

Novedad de la modificación de 2026

El texto consolidado incorpora una previsión específica para las directrices destinadas a facilitar el cumplimiento conjunto del Reglamento de IA y determinada legislación europea sectorial.

01/08/2027 — Fecha límite

Publicación de las directrices específicas previstas en el artículo 96.1.g para evitar duplicidades y reducir las cargas de cumplimiento entre el Reglamento de IA y determinadas normas europeas sobre productos.

Las directrices deben tener en cuenta la evolución tecnológica, las normas armonizadas y las necesidades de las pymes.

La Comisión también puede actualizarlas cuando resulte necesario.

¿Son obligatorias las directrices?

Es importante distinguir entre el Reglamento y las directrices interpretativas.

El Reglamento establece obligaciones jurídicamente vinculantes.

Las directrices de la Comisión sirven para explicar y facilitar su aplicación, pero no deben confundirse con una modificación del propio Reglamento.

En determinadas materias pueden existir además normas armonizadas, especificaciones comunes u otros instrumentos con efectos jurídicos específicos.

3. Diferencia entre códigos de conducta y directrices

Aspecto	Códigos de conducta	Directrices
Artículo	95	96
Finalidad	Fomentar buenas prácticas de IA responsable.	Facilitar la interpretación y aplicación del Reglamento.
Elaboración	Proveedores, usuarios y organizaciones, con apoyo institucional.	Comisión Europea.
Carácter	Voluntario en los supuestos del artículo 95.	Orientativo e interpretativo.
Destinatarios	Empresas y demás operadores de IA.	Empresas, proveedores, usuarios y autoridades.
Objetivo práctico	Mejorar voluntariamente la calidad y seguridad de los sistemas.	Reducir incertidumbres sobre el cumplimiento normativo.

4. ¿Cómo afecta a Sage 200 y otros ERP?

Este capítulo resulta interesante porque muchas aplicaciones de IA empresarial no se clasifican como de alto riesgo, pero eso no impide adoptar medidas para mejorar su fiabilidad y seguridad.

Aplicación de IA	Buena práctica que podría adoptarse
OCR inteligente de facturas	Validación de los datos extraídos y control de errores.
Conciliación bancaria con IA	Revisión de movimientos excepcionales o discrepancias.
Asistente conectado a Sage 200	Control de permisos, transparencia y registro de acciones.
Generación automática de informes	Verificación de los datos y las conclusiones.
Agente que realiza operaciones mediante API	Supervisión humana y controles antes de ejecutar acciones sensibles.
Predicciones comerciales	Seguimiento de la precisión y revisión de los resultados.

Estos ejemplos son recomendaciones de aplicación empresarial inspiradas en el artículo 95, no nuevas obligaciones legales específicas impuestas por el capítulo X.

Ejemplo: un agente inteligente conectado a Sage 200

Imaginemos que una empresa desarrolla un agente de IA que permite consultar facturas, comprobar existencias, preparar presupuestos y registrar operaciones en el ERP.

Aunque la solución no esté clasificada como de alto riesgo, podría aplicar voluntariamente un código de conducta con controles como los siguientes:

Permisos delimitados: el agente solo accede a las empresas, módulos y operaciones autorizadas.

Validación humana: determinadas operaciones, como emitir documentos o modificar datos críticos, requieren confirmación.

Trazabilidad: se registra qué operaciones solicita el usuario y cuáles ejecuta realmente el sistema.

Control de resultados: se establecen mecanismos para revisar errores, respuestas incorrectas o acciones no previstas.

Estas medidas pueden mejorar la seguridad y la confianza en la solución, además de facilitar su mantenimiento y posterior evolución.

5. ¿Cuándo es aplicable este capítulo?

02/08/2026 — Aplicable

El capítulo X es aplicable desde el 2 de agosto de 2026, conforme al calendario general del artículo 113.

La fecha de aplicación del capítulo no supone que todas las medidas voluntarias de sus códigos de conducta pasen a ser obligatorias.

6. Conclusión del capítulo X

El capítulo X tiene un enfoque distinto al de los capítulos dedicados a las prohibiciones, los sistemas de alto riesgo y las sanciones.

Su finalidad es **mejorar la calidad, seguridad y confianza en la inteligencia artificial mediante buenas prácticas voluntarias y orientaciones que faciliten el cumplimiento normativo**.

Para las empresas, destacan tres conclusiones: los sistemas que no son de alto riesgo también pueden incorporar controles voluntarios; las orientaciones de la Comisión pueden ayudar a interpretar obligaciones complejas; y las pymes deben ser tenidas en cuenta en la elaboración de estos instrumentos.

En el ámbito de Sage 200, este capítulo tiene especial interés para los desarrollos con agentes, APIs, automatizaciones inteligentes y conexiones entre diferentes aplicaciones empresariales.

La conclusión fundamental: aunque una integración de IA no esté legalmente clasificada como de alto riesgo, es recomendable diseñarla con transparencia, controles de seguridad, supervisión humana y trazabilidad.

Estas buenas prácticas permiten innovar con mayor confianza sin confundir las recomendaciones voluntarias con las obligaciones legales.

Resumen elaborado a partir de los artículos 95 y 96 del texto consolidado del Reglamento facilitado.

TEXTO OFICIAL · CAPÍTULO XI

CAPÍTULO XI
DELEGACIÓN DE PODERES Y PROCEDIMIENTO DE COMITÉ

ARTÍCULO 97
EJERCICIO DE LA DELEGACIÓN

1. Se otorgan a la Comisión los poderes para adoptar actos delegados en las condiciones establecidas en el presente artículo.
2. Los poderes para adoptar actos delegados mencionados en el artículo 6, apartado 6 y 7, el artículo 7, apartados 1 y 3, el artículo 11, apartado 3, el artículo 43, apartados 5 y 6, el artículo 47, apartado 5, el artículo 51, apartado 3, el artículo 52, apartado 4, y el artículo 53, apartados 5 y 6, se otorgan a la Comisión por un período de cinco años a partir del 1 de agosto de 2024. Los poderes para adoptar actos delegados mencionados en el artículo 2, apartado 13 y el artículo 30, apartado 2, se otorgan a la Comisión por un periodo de cinco años a partir del 27 de julio de 2026. La Comisión elaborará un informe sobre la delegación de poderes a más tardar nueve meses antes de que finalice el período de cinco años. La delegación de poderes se prorrogará tácitamente por períodos de idéntica duración, excepto si el Parlamento Europeo o el Consejo se oponen a dicha prórroga a más tardar tres meses antes del final de cada período.
3. La delegación de poderes mencionada en el artículo 2, apartado 13, en el artículo 6, apartados 6 y 7, el artículo 7, apartados 1 y 3, el artículo 11, apartado 3, el artículo 30, apartado 2, el artículo 43, apartados 5 y 6, el artículo 47, apartado 5, el artículo 51, apartado 3, el artículo 52, apartado 4, y el artículo 53, apartados 5 y 6, podrá ser revocada en cualquier momento por el Parlamento Europeo o por el Consejo. La decisión de revocación pondrá término a la delegación de los poderes que en ella se especifiquen. La decisión surtirá efecto el día siguiente al de su publicación en el Diario Oficial de la Unión Europea o en una fecha posterior indicada ella. No afectará a la validez de los actos delegados que ya estén en vigor.
4. Antes de la adopción de un acto delegado, la Comisión consultará a los expertos designados por cada Estado miembro de conformidad con los principios establecidos en el Acuerdo interinstitucional de 13 de abril de 2016 sobre la mejora de la legislación.
5. Tan pronto como la Comisión adopte un acto delegado lo notificará simultáneamente al Parlamento Europeo y al Consejo.
6. Los actos delegados adoptados en virtud del artículo 2, apartado 13, el artículo 6, apartados 6 o 7, el artículo 7, apartados 1 o 3, el artículo 11, apartado 3, el artículo 30, apartado 2, el artículo 43, apartados 5 o 6, el artículo 47, apartado 5, el artículo 51, apartado 3, el artículo 52, apartado 4, o el artículo 53, apartados 5 o 6, entrarán en vigor únicamente si, en un plazo de tres meses a partir de su notificación al Parlamento Europeo y al Consejo, ninguna de estas instituciones formula objeciones o si, antes del vencimiento de dicho plazo, ambas informan a la Comisión de que no las formularán. El plazo se prorrogará tres meses a iniciativa del Parlamento Europeo o del Consejo.

ARTÍCULO 98
PROCEDIMIENTO DE COMITÉ

1. La Comisión estará asistida por un comité. Dicho comité será un comité en el sentido del Reglamento (UE) n. o 182/2011.
2. En los casos en que se haga referencia al presente apartado, se aplicará el artículo 5 del Reglamento (UE) n. o 182/2011.

Fuente: Reglamento (UE) 2024/1689, texto consolidado a 27 de julio de 2026. Transcripción del PDF aportado; se han omitido las marcas editoriales de consolidación y las cabeceras de página.

Resumen del Capítulo XI — Delegación de poderes y procedimiento de comité

Reglamento (UE) 2024/1689 · Texto consolidado a 27/07/2026 · Páginas 114–115 · Artículos 97 y 98

Este capítulo establece **cómo puede la Comisión Europea desarrollar y actualizar determinados aspectos del Reglamento de Inteligencia Artificial sin tener que aprobar un nuevo reglamento completo cada vez**.

Es un capítulo de carácter principalmente institucional y jurídico, pero importante para las empresas porque permite adaptar determinadas disposiciones a los avances tecnológicos.

La idea fundamental: la normativa europea de IA puede evolucionar mediante actos jurídicos posteriores, dentro de los límites y procedimientos establecidos.

El capítulo contiene dos artículos.

1. Artículo 97. Ejercicio de la delegación de poderes

El artículo 97 permite que la Comisión Europea adopte **actos delegados** en determinadas materias expresamente previstas por el Reglamento.

Estos actos permiten modificar o completar determinados elementos normativos, pero no conceden a la Comisión libertad para cambiar cualquier disposición.

¿Qué aspectos pueden actualizarse?

Ámbito	Posibles modificaciones previstas
Clasificación de alto riesgo	Ajustar determinadas condiciones para clasificar sistemas de IA y modificar los casos de uso del anexo III.
Documentación técnica	Actualizar ciertos requisitos documentales.
Evaluación de conformidad	Modificar determinados procedimientos de evaluación.
Declaración UE de conformidad	Actualizar su contenido.
Modelos de IA de uso general	Adaptar determinados umbrales y criterios de clasificación.
Documentación de modelos de uso general	Actualizar los anexos y metodologías correspondientes.
Otras materias incorporadas en 2026	Ejercer las facultades específicas previstas en los artículos 2.13 y 30.2.

Por tanto, el Reglamento contempla mecanismos para adaptarse a la evolución tecnológica y a la experiencia adquirida durante su aplicación.

¿Quién controla a la Comisión Europea?

La Comisión no puede utilizar estos poderes sin límites.

El artículo 97 establece mecanismos de control por parte del Parlamento Europeo y del Consejo de la Unión Europea.

1. La Comisión prepara un acto delegado

Dentro de las competencias expresamente previstas en el Reglamento

2. Consulta a expertos nacionales

Conforme al procedimiento interinstitucional aplicable

3. Notificación al Parlamento y al Consejo

Ambas instituciones pueden formular objeciones

4. Entrada en vigor si se cumplen las condiciones

El acto no entra en vigor si el Parlamento o el Consejo formulan una objeción dentro del plazo establecido

Plazos establecidos

5 años

Duración inicial de las delegaciones, con posibles prórrogas automáticas.

3 meses

Plazo general para formular objeciones a los actos delegados, prorrogable otros tres meses.

El Parlamento Europeo o el Consejo también pueden revocar la delegación de poderes.

La versión consolidada establece dos fechas de inicio para los períodos de delegación de cinco años: el **1 de agosto de 2024** para las facultades originales enumeradas y el **27 de julio de 2026** para las nuevas facultades de los artículos 2.13 y 30.2.

2. Artículo 98. Procedimiento de comité

Este artículo regula cómo debe actuar la Comisión cuando el Reglamento exige la adopción de determinados **actos de ejecución**.

La Comisión estará asistida por un comité conforme al Reglamento (UE) 182/2011.

Cuando se remite al artículo 98.2, se aplica el procedimiento de examen previsto en el artículo 5 de dicho Reglamento.

¿Qué diferencia hay entre un acto delegado y un acto de ejecución?

Característica	Acto delegado	Acto de ejecución
Finalidad	Completar o modificar determinados elementos no esenciales de la norma.	Establecer condiciones uniformes para aplicar la norma.
Base en este capítulo	Artículo 97	Artículo 98
Control principal	Parlamento Europeo y Consejo.	Procedimiento de comité conforme a la normativa europea.
Ejemplo relacionado con IA	Actualizar determinados criterios de clasificación de sistemas de alto riesgo.	Establecer especificaciones comunes o modalidades prácticas cuando el Reglamento lo permita.

La diferencia es importante porque cada instrumento tiene límites y procedimientos distintos.

3. ¿Cómo afecta a las empresas?

Este capítulo no establece, por sí mismo, obligaciones directas como formar trabajadores, registrar un sistema o comunicar incidentes.

Su relevancia empresarial es que **determinados requisitos del Reglamento pueden evolucionar sin necesidad de sustituirlo por completo**.

Por ejemplo, pueden producirse cambios en los criterios para clasificar sistemas de IA, en determinadas obligaciones documentales o en procedimientos de conformidad.

Por eso, una empresa no debería limitar su seguimiento normativo al texto del Reglamento original de 2024.

También debe prestar atención a los actos jurídicos posteriores que puedan resultar aplicables.

4. ¿Cómo afecta a Sage 200 y sus integraciones con IA?

Imaginemos que una empresa desarrolla un agente inteligente conectado a Sage 200.

Inicialmente, el agente se limita a consultar información contable, analizar existencias y generar informes.

La empresa determina que, por esas funciones, no está incluido en una categoría de alto riesgo.

Sin embargo, el Reglamento permite que determinadas condiciones de clasificación y casos de uso del anexo III sean modificados mediante actos delegados, dentro de los límites establecidos.

Por tanto, conviene revisar periódicamente si las reglas aplicables a una solución concreta han cambiado.

Situación	Consecuencia práctica
Se actualizan determinados criterios de alto riesgo	Revisar si cambia la clasificación de alguna solución.
Se modifican requisitos de documentación	Comprobar si debe actualizarse la documentación del sistema.
Cambian procedimientos de evaluación	Adaptar los procesos correspondientes a nuevas versiones o comercializaciones.
Se actualizan criterios sobre modelos de IA de uso general	Comprobar las obligaciones del proveedor del modelo, cuando corresponda.

Estos cambios no se producen automáticamente: requieren la aprobación de los actos jurídicos correspondientes y deben analizarse sus fechas de aplicación y disposiciones transitorias.

5. ¿Cuándo es aplicable este capítulo?

02/08/2026 — Aplicable

El capítulo XI es aplicable con carácter general desde el 2 de agosto de 2026, conforme al artículo 113, sin perjuicio de las fechas específicas previstas para el ejercicio de las delegaciones.

6. Conclusión del capítulo XI

El capítulo XI establece los mecanismos institucionales necesarios para que el Reglamento Europeo de Inteligencia Artificial pueda adaptarse a una tecnología que evoluciona rápidamente.

Sus principales consecuencias son que la Comisión puede actualizar determinados aspectos del Reglamento mediante actos delegados, que estos actos están sometidos a controles institucionales y que existen procedimientos específicos para adoptar normas de ejecución.

Para las empresas, la conclusión es que el cumplimiento normativo de la IA debe mantenerse actualizado.

En proyectos de integración de IA con ERP, especialmente cuando se desarrollan soluciones para terceros, resulta recomendable incorporar un procedimiento de seguimiento de cambios regulatorios que puedan afectar a la clasificación, documentación o evaluación de los sistemas.

El capítulo XII, que viene a continuación, es especialmente relevante para empresarios y proveedores porque establece **el régimen de sanciones y las multas que pueden imponerse por incumplir el Reglamento**.

Resumen basado en los artículos 97 y 98 del texto consolidado que has facilitado, incluidas las modificaciones de 2026.

TEXTO OFICIAL · CAPÍTULO XII

CAPÍTULO XII
SANCIONES

ARTÍCULO 99
SANCIONES

1. De conformidad con las condiciones previstas en el presente Reglamento, los Estados miembros establecerán el régimen de sanciones y otras medidas de garantía del cumplimiento, como multas administrativas, advertencias o medidas no pecuniarias, aplicable a cualquier infracción del presente Reglamento que cometan los operadores y adoptarán todas las medidas necesarias para garantizar que se aplican de forma adecuada y efectiva y teniendo así en cuenta las directrices emitidas por la Comisión en virtud del artículo 96. Tales sanciones establecidas serán efectivas, proporcionadas y disuasorias. A la hora de imponer sanciones, los Estados miembros tendrán en cuenta los intereses de las pymes, incluidas las empresas emergentes y las pequeñas empresas de mediana capitalización, así como su viabilidad económica.
2. Los Estados miembros comunicarán a la Comisión, sin demora y, como muy tarde, en la fecha de aplicación las normas referentes a las sanciones y otras medidas de ejecución mencionadas en el apartado 1 y la informará, sin demora, de toda modificación de dichas normas.
3. El no respeto de la prohibición de las prácticas de IA a que se refiere el artículo 5 estará sujeto a multas administrativas de hasta 35 000 000 EUR o, si el infractor es una empresa, de hasta el 7 % de su volumen de negocios mundial total correspondiente al ejercicio financiero anterior, si esta cuantía fuese superior.
4. El incumplimiento de cualquiera de las disposiciones que figuran a continuación en relación con los operadores o los organismos notificados, distintas de los mencionados en el artículo 5, estará sujeto a multas administrativas de hasta 15 000 000 EUR o, si el infractor es una empresa, de hasta el 3 % de su volumen de negocios mundial total correspondiente al ejercicio financiero anterior, si esta cuantía fuese superior:
   a) las obligaciones de los proveedores con arreglo al artículo 16;
   b) las obligaciones de los representantes autorizados con arreglo al artículo 22;
   c) las obligaciones de los importadores con arreglo al artículo 23;
   d) las obligaciones de los distribuidores con arreglo al artículo 24;
   d bis) las obligaciones de los proveedores y operadores en virtud del artículo 25, apartados 2 y 4;
   e) las obligaciones de los responsables del despliegue con arreglo al artículo 26;
   f) los requisitos y obligaciones de los organismos notificados con arreglo al artículo 31, al artículo 33, apartados 1, 3 y 4, o al artículo 34;
   g) las obligaciones de transparencia de los proveedores y responsables del despliegue con arreglo al artículo 50.
5. La presentación de información inexacta, incompleta o engañosa a organismos notificados o a las autoridades nacionales competentes en respuesta a una solicitud estará sujeta a multas administrativas de hasta 7 500 000 EUR o, si el infractor es una empresa, de hasta el 1 % del volumen de negocios mundial total correspondiente al ejercicio financiero anterior, si esta cuantía fuese superior.
6. En el caso de las pymes, incluidas las empresas emergentes, cada una de las multas a que se refiere el presente artículo podrá ser por el porcentaje o el importe a que se refieren los apartados 3, 4 y 5, según cuál de ellos sea menor.

6 bis. En el caso de las pequeñas empresas de mediana capitalización, cada multa a que se refieren los apartados 4 y 5 no excederá de los porcentajes o importes mencionados en dichos apartados, aplicándose el menor de ellos.

7. Al decidir la imposición de una multa administrativa y su cuantía en cada caso concreto se tomarán en consideración todas las circunstancias pertinentes de la situación de que se trate y, en su caso, se tendrá en cuenta lo siguiente:
   a) la naturaleza, la gravedad y la duración de la infracción y de sus consecuencias, teniendo en cuenta la finalidad del sistema de IA y, cuando proceda, el número de personas afectadas y el nivel de los daños que hayan sufrido;
   b) si otras autoridades de vigilancia del mercado han impuesto ya multas administrativas al mismo operador por la misma infracción;
   c) si otras autoridades han impuesto ya multas administrativas al mismo operador por infracciones de otros actos legislativos nacionales o de la Unión, cuando dichas infracciones se deriven de la misma actividad u omisión que constituya una infracción pertinente del presente Reglamento;
   d) el tamaño, el volumen de negocios anual y la cuota de mercado del operador que comete la infracción;
   e) cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso, como los beneficios financieros obtenidos o las pérdidas evitadas, directa o indirectamente, a través de la infracción;
   f) el grado de cooperación con las autoridades nacionales competentes con el fin de subsanar la infracción y mitigar sus posibles efectos adversos;
   g) el grado de responsabilidad del operador, teniendo en cuenta las medidas técnicas y organizativas aplicadas por este;
   h) la forma en que las autoridades nacionales competentes tuvieron conocimiento de la infracción, en particular si el operador notificó la infracción y, en tal caso, en qué medida;
   i) la intencionalidad o negligencia en la infracción;
   j) las acciones emprendidas por el operador para mitigar los perjuicios sufridos por las personas afectadas.
8. Cada Estado miembro establecerá normas que determinen en qué medida es posible imponer multas administrativas a autoridades y organismos públicos establecidos en dicho Estado miembro.
9. En función del ordenamiento jurídico de los Estados miembros, las normas relativas a las multas administrativas podrán aplicarse de tal modo que las multas las impongan órganos jurisdiccionales nacionales competentes u otros organismos, según proceda en dichos Estados miembros. La aplicación de dichas normas en estos Estados miembros tendrá un efecto equivalente.
10. El ejercicio de poderes en virtud del presente artículo estará sujeto a garantías procesales adecuadas de conformidad

con el Derecho de la Unión y nacional, entre ellas la tutela judicial efectiva y el respeto de las garantías procesales.

11. Los Estados miembros informarán anualmente a la Comisión de las multas administrativas que hayan impuesto durante ese año de conformidad con el presente artículo y de cualquier litigio o proceso judicial relacionados.

ARTÍCULO 100
MULTAS ADMINISTRATIVAS A INSTITUCIONES, ÓRGANOS Y ORGANISMOS DE LA UNIÓN

1. El Supervisor Europeo de Protección de Datos podrá imponer multas administrativas a las instituciones, órganos y organismos de la Unión comprendidos en el ámbito de aplicación del presente Reglamento. Al decidir la imposición de una multa administrativa y su cuantía en cada caso concreto se tomarán en consideración todas las circunstancias pertinentes de la situación de que se trate y se tendrá debidamente en cuenta lo siguiente:
   a) la naturaleza, la gravedad y la duración de la infracción y de sus consecuencias, teniendo en cuenta la finalidad del sistema de IA de que se trate, así como, cuando proceda, el número de personas afectadas y el nivel de los daños que hayan sufrido;
   b) el grado de responsabilidad de la institución, órgano u organismo de la Unión, teniendo en cuenta las medidas técnicas y organizativas aplicadas;
   c) las acciones emprendidas por la institución, órgano u organismo de la Unión para mitigar los perjuicios sufridos por las personas afectadas;
   d) el grado de cooperación con el Supervisor Europeo de Protección de Datos con el fin de subsanar la infracción y mitigar sus posibles efectos adversos, incluido el cumplimiento de cualquiera de las medidas que el propio Supervisor Europeo de Protección de Datos haya ordenado previamente contra la institución, órgano u organismo de la Unión de que se trate en relación con el mismo asunto;
   e) toda infracción anterior similar cometida por la institución, órgano u organismo de la Unión;
   f) la forma en que el Supervisor Europeo de Protección de Datos tuvo conocimiento de la infracción, en particular si la institución, órgano u organismo de la Unión notificó la infracción y, en tal caso, en qué medida;
   g) el presupuesto anual de la institución, órgano u organismo de la Unión.
2. El no respeto de la prohibición de las prácticas de IA a que se refiere el artículo 5 estará sujeto a multas administrativas de hasta 1 500 000 EUR.
3. El incumplimiento por parte del sistema de IA de cualquiera de los requisitos u obligaciones establecidos en el presente Reglamento, distintos de los previstos en el artículo 5, estará sujeto a multas administrativas de hasta 750 000 EUR.
4. Antes de tomar ninguna decisión en virtud del presente artículo, el Supervisor Europeo de Protección de Datos ofrecerá a la institución, órgano u organismo de la Unión sometida al procedimiento instruido por el Supervisor Europeo de Protección de Datos la oportunidad de ser oída en lo que respecta a la posible infracción. El Supervisor Europeo de Protección de Datos basará sus decisiones únicamente en los elementos y las circunstancias sobre los que las partes afectadas hayan podido manifestarse. Los denunciantes, si los hay, participarán estrechamente en el procedimiento.
5. Los derechos de defensa de las partes estarán garantizados plenamente en el curso del procedimiento. Tendrán derecho a acceder al expediente del Supervisor Europeo de Protección de Datos, sin perjuicio del interés legítimo de las personas físicas y las empresas en la protección de sus datos personales o secretos comerciales.
6. La recaudación proveniente de la imposición de multas con arreglo al presente artículo contribuirá al presupuesto general de la Unión. Las multas no afectarán al funcionamiento efectivo de la institución, órgano u organismo de la Unión sancionado.
7. El Supervisor Europeo de Protección de Datos informará anualmente a la Comisión de las multas administrativas que haya impuesto en virtud del presente artículo y de cualquier litigio o proceso judicial que haya iniciado.

ARTÍCULO 101
MULTAS A PROVEEDORES DE MODELOS DE IA DE USO GENERAL

1. La Comisión podrá imponer multas a los proveedores de modelos de IA de uso general que no superen el 3 % de su volumen de negocios mundial total anual correspondiente al ejercicio financiero anterior o de 15 000 000 EUR, si esta cifra es superior, cuando la Comisión considere que, de forma deliberada o por negligencia:
   a) infringieron las disposiciones pertinentes del presente Reglamento;
   b) no atendieron una solicitud de información o documentos con arreglo al artículo 91, o han facilitado información inexacta, incompleta o engañosa;
   c) incumplieron una medida solicitada en virtud del artículo 93;
   d) no dieron acceso a la Comisión al modelo de IA de uso general o al modelo de IA de uso general con riesgo sistémico para que se lleve a cabo una evaluación con arreglo al artículo 92.

   Al fijar el importe de la multa o de la multa coercitiva, se tomarán en consideración la naturaleza, gravedad y duración de la infracción, teniendo debidamente en cuenta los principios de proporcionalidad y adecuación. La Comisión también tendrá en cuenta los compromisos contraídos de conformidad con el artículo 93, apartado 3, y en los códigos de buenas prácticas pertinentes previstos en el artículo 56.
2. Antes de adoptar una decisión con arreglo al apartado 1, la Comisión comunicará sus conclusiones preliminares al proveedor del modelo de IA de uso general o del modelo de IA y le dará la oportunidad de ser oído.
3. Las multas impuestas de conformidad con el presente artículo serán efectivas, proporcionadas y disuasorias.
4. La información sobre las multas impuestas en virtud del presente artículo también se comunicará al Consejo de IA, según proceda.
5. El Tribunal de Justicia de la Unión Europea tendrá plena competencia jurisdiccional para examinar las decisiones de imposición de una multa adoptadas por la Comisión en virtud del presente artículo. Podrá anular, reducir o incrementar la cuantía de la multa impuesta.

6. La Comisión adoptará actos de ejecución que contengan disposiciones detalladas y garantías procesales para los procedimientos con vistas a la posible adopción de decisiones con arreglo al apartado 1 del presente artículo. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 98, apartado 2.

Fuente: Reglamento (UE) 2024/1689, texto consolidado a 27 de julio de 2026. Transcripción del PDF aportado; se han omitido las marcas editoriales de consolidación y las cabeceras de página.

Resumen del Capítulo XII — Sanciones por incumplimiento de la normativa de IA

Reglamento (UE) 2024/1689 · Texto consolidado a 27/07/2026 · Páginas 115–120 · Artículos 99 a 101

Este es uno de los capítulos de mayor interés para empresarios, fabricantes de software y empresas que utilizan inteligencia artificial.

Establece **las sanciones económicas por incumplir el Reglamento Europeo de IA**, diferenciando entre las prácticas prohibidas, el incumplimiento de obligaciones legales, la información engañosa y las infracciones cometidas por proveedores de modelos de IA de uso general.

La idea fundamental es que las sanciones pueden ser muy elevadas, pero deben aplicarse de manera proporcionada, teniendo en cuenta la gravedad de la infracción, el tamaño de la empresa y las circunstancias concretas.

El capítulo contiene tres artículos.

1. Artículo 99. Sanciones a las empresas y demás operadores

El artículo 99 establece los principales niveles de sanciones.

Cuantías máximas generales

Infracción	Máximo general
Prácticas prohibidas	**35 M€ o 7 %** de facturación mundial
Obligaciones específicas	**15 M€ o 3 %** de facturación mundial
Información incorrecta	**7,5 M€ o 1 %** de facturación mundial
Proveedores de modelos de uso general (art. 101)	**15 M€ o 3 %** de facturación mundial

Con carácter general, para empresas se aplica el límite más elevado entre la cantidad fija y el porcentaje, con las reglas especiales establecidas para pymes y pequeñas empresas de mediana capitalización. Estas cifras son máximos legales, no multas automáticas.

A. Infracciones muy graves: hasta 35 millones de euros o el 7 %

Máximo sancionador más elevado

El artículo 99.3 contempla estas sanciones para el incumplimiento de las prohibiciones establecidas en el artículo 5.

Entre las prácticas prohibidas que pueden dar lugar a estas sanciones se encuentran, cuando concurren sus condiciones legales:

- Manipulación perjudicial del comportamiento de las personas.
- Explotación de vulnerabilidades de determinados colectivos.
- Determinados sistemas de puntuación social.
- Reconocimiento de emociones en entornos laborales o educativos fuera de las excepciones.
- Determinadas prácticas prohibidas de reconocimiento o clasificación biométrica.
- Otras prácticas prohibidas incorporadas al artículo 5.

Ejemplo empresarial: una compañía utiliza deliberadamente un sistema de IA que analiza biométricamente las emociones de sus empleados para evaluar su motivación y controlar su comportamiento, fuera de las excepciones legales.

Esta utilización puede constituir una infracción de las prohibiciones del artículo 5 y quedar comprendida en el régimen sancionador más elevado.

B. Incumplimiento de obligaciones específicas: hasta 15 millones o el 3 %

El artículo 99.4 establece este nivel para determinadas obligaciones de los operadores.

Artículo	Infracción que puede sancionarse
16	Incumplimiento de obligaciones del proveedor de sistemas de IA de alto riesgo.
22	Incumplimiento de obligaciones de representantes autorizados.
23	Incumplimiento de obligaciones de importadores.
24	Incumplimiento de obligaciones de distribuidores.
25.2 y 25.4	Incumplimiento de determinadas obligaciones de proveedores y otros operadores en la cadena de valor.
26	Incumplimiento de obligaciones de las empresas que utilizan sistemas de alto riesgo.
31, 33 y 34	Incumplimiento de determinados requisitos de organismos notificados.
50	Incumplimiento de obligaciones de transparencia.

¿Qué significa para una empresa que utiliza IA?

Supongamos que una empresa implanta un sistema de IA de alto riesgo para seleccionar trabajadores.

Si incumple las obligaciones aplicables del artículo 26, por ejemplo, las relativas a la supervisión humana o la información previa a trabajadores y representantes, puede quedar expuesta al régimen sancionador del artículo 99.4.

También es especialmente relevante el artículo 50: determinadas obligaciones de transparencia se aplican incluso a sistemas que no están clasificados como de alto riesgo.

Por tanto, utilizar una solución de IA adquirida a un tercero no elimina automáticamente las responsabilidades de la empresa usuaria.

C. Información falsa, incompleta o engañosa: hasta 7,5 millones o el 1 %

El artículo 99.5 sanciona la presentación de información incorrecta, incompleta o engañosa a organismos notificados o autoridades nacionales competentes como respuesta a una solicitud.

Ejemplo: una empresa presenta documentación engañosa en respuesta a un requerimiento de una autoridad sobre el cumplimiento de su sistema de IA.

No se trata de sancionar cualquier error administrativo sin atender a las circunstancias, sino de aplicar el régimen previsto cuando concurren los elementos de la infracción.

2. ¿Qué ocurre con las pymes y las empresas pequeñas?

Protección específica para pymes

El artículo 99.6 contempla un tratamiento especial para las pymes, incluidas las empresas emergentes.

En estos casos, la sanción puede determinarse tomando **la menor de las dos cuantías: el importe fijo o el porcentaje de facturación**, frente al criterio general de la mayor cuantía previsto para las empresas.

La modificación de 2026 también establece una regla especial para las pequeñas empresas de mediana capitalización en las infracciones de los apartados 4 y 5.

Ejemplo orientativo: una empresa con 2 millones de euros de facturación mundial anual

Infracción	Límite porcentual	Cuantía
Práctica prohibida	7 %	140.000 €
Obligaciones específicas	3 %	60.000 €
Información incorrecta	1 %	20.000 €

Estas cifras ilustran el cálculo porcentual y el límite reducido previsto para una empresa que reúna las condiciones de pyme. **No representan la multa que necesariamente recibiría**: la sanción concreta debe fijarse atendiendo a las circunstancias de la infracción.

¿Se puede imponer la sanción máxima automáticamente?

No.

El artículo 99.7 obliga a considerar las circunstancias pertinentes del caso.

Entre ellas figuran la gravedad, duración y consecuencias de la infracción, las personas afectadas, el tamaño de la empresa, el grado de responsabilidad, la intencionalidad o negligencia, la cooperación con las autoridades y las medidas adoptadas para reducir los perjuicios.

Además, el régimen sancionador debe ser efectivo, proporcionado y disuasorio.

3. Artículo 100. Sanciones a instituciones y organismos de la Unión Europea

Páginas 118–119

Este artículo establece un régimen específico para instituciones, órganos y organismos de la Unión Europea.

El organismo competente para imponer estas multas es el Supervisor Europeo de Protección de Datos.

Infracción	Multa máxima
Incumplimiento de las prácticas prohibidas del artículo 5	1.500.000 €
Incumplimiento de otros requisitos u obligaciones del Reglamento	750.000 €

El artículo también establece garantías de audiencia, defensa y acceso al expediente.

Importante: este régimen se refiere específicamente a instituciones, órganos y organismos de la Unión. No es un límite sancionador general aplicable a cualquier Administración pública española.

En el caso de autoridades y organismos públicos nacionales, el artículo 99.8 remite a las normas que establezca cada Estado miembro.

4. Artículo 101. Multas a proveedores de modelos de IA de uso general

Páginas 119–120

Este artículo establece el régimen sancionador específico aplicable a los proveedores de modelos de IA de uso general.

Se contempla una multa máxima de **15 millones de euros o el 3 % del volumen de negocios mundial anual del ejercicio anterior, si esta última cuantía es superior**.

¿Qué conductas pueden sancionarse?

La Comisión Europea puede imponer multas cuando, deliberadamente o por negligencia, los proveedores:

- Incumplen las disposiciones pertinentes del Reglamento.

- No responden a solicitudes de información o documentación del artículo 91, o facilitan información incorrecta, incompleta o engañosa.
- Incumplen las medidas solicitadas conforme al artículo 93.
- No facilitan el acceso al modelo para realizar evaluaciones conforme al artículo 92.

La Comisión debe respetar las garantías procedimentales y permitir que los proveedores sean oídos antes de adoptar una decisión sancionadora.

¿Afecta a cualquier empresa que utilice ChatGPT u otro LLM?

No por el mero hecho de utilizarlo.

El artículo 101 se dirige a los **proveedores de modelos de IA de uso general**.

Una empresa que utiliza un modelo de un tercero para consultar información o generar documentos no asume automáticamente las obligaciones sancionadas por este artículo.

Sin embargo, sí puede estar sujeta a otras obligaciones si desarrolla, proporciona o utiliza un sistema de IA comprendido en el Reglamento.

5. ¿Qué consecuencias puede tener para Sage 200 y sus integraciones?

Para una empresa que utiliza Sage 200 y decide incorporar inteligencia artificial, el riesgo sancionador depende fundamentalmente de la funcionalidad y del papel que desempeñe cada participante.

Situación	Riesgo normativo principal
OCR para contabilizar facturas	No supone por sí mismo una infracción del Reglamento. Debe cumplir las obligaciones aplicables.
Agente de IA que consulta información del ERP	La integración no es sancionable por sí misma; deben analizarse sus características y obligaciones.
Chatbot de atención al cliente	Incumplimiento de las obligaciones de transparencia, cuando procedan.
IA para evaluar candidatos o trabajadores	Incumplimiento de obligaciones aplicables a sistemas de alto riesgo, si se clasifica como tal.
IA para inferir emociones de empleados mediante biometría	Posible práctica prohibida del artículo 5.
Integrador que transforma sustancialmente un sistema de alto riesgo	Posible asunción de obligaciones como proveedor, conforme al artículo 25.

Ejemplo de reparto de responsabilidades

Imaginemos que se implanta una IA conectada a Sage 200 para analizar el rendimiento laboral de los empleados.

El fabricante o proveedor del sistema tendrá las obligaciones que correspondan a su posición jurídica.

La empresa cliente deberá cumplir las obligaciones aplicables al uso, incluida la supervisión humana y la información a trabajadores y representantes si el sistema se clasifica como de alto riesgo.

Y si el integrador modifica sustancialmente el sistema o cambia su finalidad en los supuestos del artículo 25, podría asumir obligaciones de proveedor.

La responsabilidad no se determina únicamente por quién ha comprado la licencia del software, sino por quién desarrolla, modifica, comercializa y utiliza el sistema y qué obligaciones le corresponden.

6. ¿Cuándo se aplican las sanciones?

El artículo 113 establece un calendario diferenciado.

02/08/2025 — Aplicable

Capítulo XII, salvo el artículo 101

Entrada en aplicación del régimen sancionador general, teniendo en cuenta la fecha de exigibilidad de cada obligación material.

02/08/2026 — Aplicable

Artículo 101

Aplicación del régimen de multas específico para proveedores de modelos de IA de uso general.

2027–2028 — Escalonado

Determinadas obligaciones sobre sistemas de alto riesgo

Su exigibilidad se determina conforme al calendario del capítulo III y las disposiciones transitorias correspondientes.

Es importante distinguir entre la aplicación del régimen sancionador y la fecha en que resulta exigible cada obligación.

No puede presumirse que todas las obligaciones sobre sistemas de alto riesgo sean sancionables desde agosto de 2025.

7. Conclusión del capítulo XII

Este capítulo establece un régimen de sanciones significativo, especialmente para las prácticas de IA prohibidas y los incumplimientos de obligaciones aplicables a los operadores.

Las principales conclusiones para las empresas son que las multas pueden alcanzar cantidades elevadas, que el sistema sancionador contempla reglas especiales para pymes y que las cuantías concretas deben determinarse de manera proporcionada.

También es importante comprender que **las sanciones no se dirigen exclusivamente a los grandes fabricantes de inteligencia artificial**: pueden afectar a proveedores, integradores y empresas usuarias cuando incumplan las obligaciones que les correspondan.

En un proyecto de IA conectado a un ERP, la mejor forma de reducir el riesgo normativo es identificar correctamente el tipo de sistema, definir las responsabilidades de cada participante y establecer controles adecuados para su utilización.

El mensaje más importante para los empresarios: no se sanciona por utilizar inteligencia artificial, sino por incumplir las obligaciones y prohibiciones que resulten aplicables a cada uso.

Resumen basado en los artículos 99, 100 y 101 del texto consolidado aportado, incluida la modificación de 2026.

TEXTO OFICIAL · CAPÍTULO XIII

CAPÍTULO XIII
DISPOSICIONES FINALES

ARTÍCULO 102
MODIFICACIÓN DEL REGLAMENTO (CE) N. O 300/2008

En el artículo 4, apartado 3, del Reglamento (CE) n. o 300/2008, se añade el párrafo siguiente:

«Al adoptar medidas detalladas relativas a las especificaciones técnicas y los procedimientos de aprobación y utilización del equipo de seguridad en relación con sistemas de inteligencia artificial en el sentido del Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo (*), se tendrán en cuenta los requisitos establecidos en el capítulo III, sección 2, de dicho Reglamento.

(*) 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 y por el que se modifican los Reglamentos (CE) n. o 300/2008, (UE) n. o 167/2013, (UE) n. o 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial) (DO L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).».

ARTÍCULO 103
MODIFICACIÓN DEL REGLAMENTO (UE) N. O 167/2013

En el artículo 17, apartado 5, del Reglamento (UE) n. o 167/2013, se añade el párrafo siguiente:

«Al adoptar actos delegados en virtud del párrafo primero relativos a sistemas de inteligencia artificial que sean componentes de seguridad en el sentido del Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo (*), se tendrán en cuenta los requisitos establecidos en el capítulo III, sección 2, de dicho Reglamento.

(*) 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 y por el que se modifican los Reglamentos (CE) n. o 300/2008, (UE) n. o 167/2013, (UE) n. o 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial) (DO L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).».

ARTÍCULO 104
MODIFICACIÓN DEL REGLAMENTO (UE) N. O 168/2013

En el artículo 22, apartado 5, del Reglamento (UE) n. o 168/2013, se añade el párrafo siguiente:

«Al adoptar actos delegados en virtud del párrafo primero relativos a sistemas de inteligencia artificial que sean componentes de seguridad en el sentido del Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo (*), se tendrán en cuenta los requisitos establecidos en el capítulo III, sección 2, de dicho Reglamento.

(*) 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 y por el que se modifican los Reglamentos (CE) n. o 300/2008, (UE) n. o 167/2013, (UE) n. o 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial) (DO L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).».

ARTÍCULO 105
MODIFICACIÓN DE LA DIRECTIVA 2014/90/UE

En el artículo 8 de la Directiva 2014/90/UE, se añade el apartado siguiente:

«5. En el caso de los sistemas de inteligencia artificial que sean componentes de seguridad en el sentido del Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo (*), la Comisión tendrá en cuenta los requisitos establecidos en el capítulo III, sección 2, de dicho Reglamento al desempeñar sus actividades con arreglo al apartado 1 y al adoptar especificaciones técnicas y normas de ensayo de conformidad con los apartados 2 y 3.

(*) 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 y por el que se modifican los Reglamentos (CE) n. o 300/2008, (UE) n. o 167/2013, (UE) n. o 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial) (DO L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).».

ARTÍCULO 106
MODIFICACIÓN DE LA DIRECTIVA (UE) 2016/797

En el artículo 5 de la Directiva (UE) 2016/797, se añade el apartado siguiente:

«12. Al adoptar actos delegados en virtud del apartado 1 y actos de ejecución en virtud del apartado 11 relativos a sistemas de inteligencia artificial que sean componentes de seguridad en el sentido del Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo (*), se tendrán en cuenta los requisitos establecidos en el capítulo III, sección 2, de dicho Reglamento.

(*) 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 y por el que se modifican los Reglamentos (CE) n. o 300/2008, (UE) n. o 167/2013, (UE) n. o 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial) (DO L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).».

ARTÍCULO 107
MODIFICACIÓN DEL REGLAMENTO (UE) 2018/858

En el artículo 5 del Reglamento (UE) 2018/858, se añade el apartado siguiente:

«4. Al adoptar actos delegados en virtud del apartado 3 relativos a sistemas de inteligencia artificial que sean componentes de seguridad en el sentido del Reglamento (UE) 2024/… del Parlamento Europeo y del Consejo (*), se tendrán en cuenta los requisitos establecidos en el capítulo III, sección 2, de dicho Reglamento.

(*) 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 y por el que se modifican los Reglamentos (CE) n. o 300/2008, (UE)

n. o 167/2013, (UE) n. o 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial) (DO L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).».

ARTÍCULO 108
MODIFICACIÓN DEL REGLAMENTO (UE) 2018/1139

El Reglamento (UE) 2018/1139 se modifica como sigue:

1) En el artículo 17, se añade el apartado siguiente:

«3. Sin perjuicio de lo dispuesto en el apartado 2, al adoptar actos de ejecución en virtud del apartado 1 relativos a sistemas de inteligencia artificial que sean componentes de seguridad en el sentido del Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo (*), se tendrán en cuenta los requisitos establecidos en el capítulo III, sección 2, de dicho Reglamento.

(*) 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 y por el que se modifican los Reglamentos (CE) n. o 300/2008, (UE) n. o 167/2013, (UE) n. o 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial) (DO L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).».

2) En el artículo 19, se añade el apartado siguiente:

«4. Al adoptar actos delegados en virtud de los apartados 1 y 2 relativos a sistemas de inteligencia artificial que sean componentes de seguridad en el sentido del Reglamento (UE) 2024/1689, se tendrán en cuenta los requisitos establecidos en el capítulo III, sección 2, de dicho Reglamento.».

3) En el artículo 43, se añade el apartado siguiente:

«4. Al adoptar actos de ejecución en virtud del apartado 1 relativos a sistemas de inteligencia artificial que sean componentes de seguridad en el sentido del Reglamento (UE) 2024/1689, se tendrán en cuenta los requisitos establecidos en el capítulo III, sección 2, de dicho Reglamento.».

4) En el artículo 47, se añade el apartado siguiente:

«3. Al adoptar actos delegados en virtud de los apartados 1 y 2 relativos a sistemas de inteligencia artificial que sean componentes de seguridad en el sentido del Reglamento (UE) 2024/1689, se tendrán en cuenta los requisitos establecidos en el capítulo III, sección 2, de dicho Reglamento.».

5) En el artículo 57, se añade el párrafo siguiente:

«Al adoptar dichos actos de ejecución relativos a sistemas de inteligencia artificial que sean componentes de seguridad en el sentido del Reglamento (UE) 2024/1689, se tendrán en cuenta los requisitos establecidos en el capítulo III, sección 2, de dicho Reglamento.».

6) En el artículo 58, se añade el apartado siguiente:

«3. Al adoptar actos delegados en virtud de los apartados 1 y 2 relativos a sistemas de inteligencia artificial que sean componentes de seguridad en el sentido del Reglamento (UE) 2024/1689, se tendrán en cuenta los requisitos establecidos en el capítulo III, sección 2, de dicho Reglamento.».

ARTÍCULO 109
MODIFICACIÓN DEL REGLAMENTO (UE) 2019/2144

En el artículo 11 del Reglamento (UE) 2019/2144, se añade el párrafo siguiente:

«3. Al adoptar actos de ejecución en virtud del apartado 2 relativos a sistemas de inteligencia artificial que sean componentes de seguridad en el sentido del Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo (*), se tendrán en cuenta los requisitos establecidos en el capítulo III, sección 2, de dicho Reglamento.

(*) 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 y por el que se modifican los Reglamentos (CE) n. o 300/2008, (UE) n. o 167/2013, (UE) n. o 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial) (DO L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).».

ARTÍCULO 110
MODIFICACIÓN DE LA DIRECTIVA (UE) 2020/1828

En el anexo I de la Directiva (UE) 2020/1828 del Parlamento Europeo y del Consejo (2) se añade el punto siguiente:

«68) Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 1689, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n. o 300/2008, (UE) n. o 167/2013, (UE) n. o 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial) (DO L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).».

ARTÍCULO 111
SISTEMAS DE IA YA INTRODUCIDOS EN EL MERCADO O PUESTOS EN SERVICIO Y MODELOS DE IA DE USO GENERAL YA INTRODUCIDOS EN EL MERCADO

1. Sin perjuicio de que se aplique el artículo 5 con arreglo a lo dispuesto en el artículo 113, párrafo tercero, letra a), los sistemas de IA que sean componentes de los sistemas informáticos de gran magnitud establecidos en virtud de los actos legislativos enumerados en el anexo X que se hayan introducido en el mercado o se hayan puesto en servicio antes del 2 de agosto de 2027 deberán estar en conformidad con el presente Reglamento a más tardar el 31 de diciembre de 2030.

Los requisitos establecidos en el presente Reglamento se tendrán en cuenta en la evaluación de cada sistema informático de gran magnitud establecido en virtud de los actos jurídicos enumerados en el anexo X que se efectúe de conformidad con lo dispuesto en dichos actos jurídicos y cuando dichos actos jurídicos hayan sido sustituidos o modificados.

2. Sin perjuicio de que se aplique el artículo 5 con arreglo a lo dispuesto en el artículo 113, párrafo tercero, letra a), el presente Reglamento se aplicará a los operadores de sistemas de IA de alto riesgo, distintos de los mencionados en el apartado 1 del presente artículo, que se hayan introducido en el mercado o puesto en servicio antes de la fecha de aplicación del capítulo III a que se refiere el artículo 113, únicamente si, a partir de esa fecha, dichos sistemas se ven sometidos a cambios significativos en sus diseños. En cualquier caso, los proveedores y los responsables del despliegue de los sistemas de IA de alto riesgo destinados a ser utilizados por las autoridades públicas adoptarán las medidas necesarias para cumplir los

requisitos y obligaciones establecidas en el presente Reglamento a más tardar el 2 de agosto de 2030.

3. Los proveedores de modelos de IA de uso general que se hayan introducido en el mercado antes del 2 de agosto de 2025 adoptarán las medidas necesarias para cumplir las obligaciones establecidas en el presente Reglamento a más tardar el 2 de agosto de 2027.

4. Los proveedores de sistemas de IA, incluidos los sistemas de IA de uso general, que generen contenido sintético de audio, imagen, vídeo o texto y se hayan introducido en el mercado antes del 2 de agosto de 2026 adoptarán las medidas necesarias para cumplir lo dispuesto en el artículo 50, apartado 2, a más tardar el 2 de diciembre de 2026.

(2) Directiva (UE) 2020/1828 del Parlamento Europeo y del Consejo, de 25 de noviembre de 2020, relativa a las acciones de representación para la protección de los intereses colectivos de los consumidores, y por la que se deroga la Directiva 2009/22/CE (DO L 409 de 4.12.2020, p. 1).

ARTÍCULO 112
EVALUACIÓN Y REVISIÓN

1. La Comisión evaluará la necesidad de modificar la lista del anexo III y la lista de prácticas de IA prohibidas previstas en el artículo 5 una vez al año a partir de la entrada en vigor del presente Reglamento y hasta el final del período de delegación de poderes previsto en el artículo 97. La Comisión presentará las conclusiones de dicha evaluación al Parlamento Europeo y al Consejo.

2. A más tardar el 2 de agosto de 2028, y posteriormente cada cuatro años, la Comisión evaluará los puntos siguientes e informará de ello al Parlamento Europeo y al Consejo:

   a) la necesidad de ampliar los ámbitos enumerados en el anexo III o de añadir nuevos ámbitos;

   b) la necesidad de modificar la lista de sistemas de IA que requieren medidas de transparencia adicionales con arreglo al artículo 50;

   c) la necesidad de mejorar la eficacia del sistema de supervisión y gobernanza.

3. A más tardar el 2 de agosto de 2029, y posteriormente cada cuatro años, la Comisión presentará al Parlamento Europeo y al Consejo un informe sobre la evaluación y revisión del presente Reglamento. El informe incluirá una evaluación de la estructura de control del cumplimiento y de la posible necesidad de que una agencia de la Unión resuelva las deficiencias detectadas. En función de sus conclusiones, dicho informe irá acompañado, en su caso, de una propuesta de modificación del presente Reglamento. Los informes se harán públicos.

4. En los informes mencionados en el apartado 2 se prestará una atención especial a lo siguiente:

   a) el estado de los recursos financieros, técnicos y humanos de las autoridades nacionales competentes para desempeñar de forma eficaz las funciones que les hayan sido asignadas en virtud del presente Reglamento;

   b) el estado de las sanciones, en particular, de las multas administrativas a que se refiere el artículo 99, apartado 1, aplicadas por los Estados miembros a las infracciones de las disposiciones del presente Reglamento;

   c) las normas armonizadas adoptadas y las especificaciones comunes desarrolladas en apoyo del presente Reglamento;

   d) el número de empresas que entran en el mercado después de que se empiece a aplicar el presente Reglamento y, de entre ellas, el número de pymes.

5. A más tardar el 2 de agosto de 2028, la Comisión evaluará el funcionamiento de la Oficina de IA, si se le han otorgado poderes y competencias suficientes para desempeñar sus funciones, y si sería pertinente y necesario para la correcta aplicación y ejecución del presente Reglamento mejorar la Oficina de IA y sus competencias de ejecución, así como aumentar sus recursos. La Comisión presentará un informe sobre su evaluación al Parlamento Europeo y al Consejo.

6. A más tardar el 2 de agosto de 2028 y posteriormente cada cuatro años, la Comisión presentará un informe sobre la revisión de los avances en la elaboración de documentos de normalización sobre el desarrollo eficiente desde el punto de vista energético de modelos de IA de uso general y evaluará la necesidad de medidas o acciones adicionales, incluidas medidas o acciones vinculantes. Este informe se remitirá al Parlamento Europeo y al Consejo y se hará público.

7. A más tardar el 2 de agosto de 2028 y posteriormente cada tres años, la Comisión evaluará la incidencia y la eficacia de los códigos de conducta voluntarios por lo que respecta a promover la aplicación de los requisitos establecidos en el capítulo III, sección 2, a sistemas de IA que no sean de alto riesgo y, en su caso, de otros requisitos adicionales aplicables a los sistemas de IA que no sean sistemas de IA de alto riesgo, como, por ejemplo, requisitos relativos a la sostenibilidad medioambiental.

8. A efectos de lo dispuesto en los apartados 1 a 7, el Consejo de IA, los Estados miembros y las autoridades nacionales competentes facilitarán información a la Comisión, cuando así lo solicite, y sin demora indebida.

9. Al llevar a cabo las evaluaciones y revisiones mencionadas en los apartados 1 a 7, la Comisión tendrá en cuenta las posiciones y conclusiones del Consejo de IA, el Parlamento Europeo, el Consejo y los demás organismos o fuentes pertinentes.

10. La Comisión presentará, en caso necesario, las propuestas oportunas de modificación del presente Reglamento, en particular teniendo en cuenta la evolución de la tecnología y el efecto de los sistemas de IA en la salud y la seguridad y en los derechos fundamentales, y a la vista de los avances en la sociedad de la información.

11. Para orientar las evaluaciones y revisiones a que se refieren los apartados 1 a 7 del presente artículo, la Oficina de IA se encargará de desarrollar una metodología objetiva y participativa para la evaluación de los niveles de riesgo a partir de los criterios expuestos en los artículos pertinentes y la inclusión de nuevos sistemas en:

   a) la lista establecida en el anexo III, incluida la ampliación de los ámbitos existentes o la inclusión de nuevos ámbitos en dicho anexo;

   b) la lista de prácticas prohibidas establecida en el artículo 5, y

   c) la lista de sistemas de IA que requieren medidas de transparencia adicionales con arreglo al artículo 50.

12. Las modificaciones del presente Reglamento con arreglo al apartado 10, o los actos delegados o de ejecución pertinentes, que afecten a los actos legislativos de armonización de la Unión sectoriales que se enumeran en el anexo I, sección B, tendrán en cuenta las

particularidades normativas de cada sector y los mecanismos de gobernanza, evaluación de la conformidad y ejecución vigentes, así como las autoridades establecidas en ellos.

13. A más tardar el 2 de agosto de 2031, la Comisión evaluará la ejecución del presente Reglamento e informará al respecto al Parlamento Europeo, al Consejo y al Comité Económico y Social Europeo, teniendo en cuenta los primeros años de aplicación del presente Reglamento. En función de sus conclusiones, dicho informe irá acompañado, en su caso, de una propuesta de modificación del presente Reglamento en lo que respecta a la estructura de ejecución y a la necesidad de que una agencia de la Unión resuelva las deficiencias detectadas.

ARTÍCULO 113
ENTRADA EN VIGOR Y APLICACIÓN

El presente Reglamento entrará en vigor a los veinte días de su publicación en el Diario Oficial de la Unión Europea.

Será aplicable a partir del 2 de agosto de 2026.

No obstante:

a) los capítulos I y II serán aplicables a partir del 2 de febrero de 2025, a excepción del artículo 5, apartado 1, párrafo primero, letras b bis) y b ter), y el artículo 5, apartado 1 bis, y apartado 1 ter, que serán aplicables a partir del 2 de diciembre de 2026;

b) el capítulo III, sección 4, el capítulo V, el capítulo VII y el capítulo XII y el artículo 78 serán aplicables a partir del 2 de agosto de 2025, a excepción del artículo 101;

c) el capítulo III, secciones 1, 2 y 3, con excepción de su artículo 6, apartado 5, será aplicable a partir del:

i) 2 de diciembre de 2027 en lo que respecta a los sistemas de IA clasificados como de alto riesgo en virtud del artículo 6, apartado 2, y el anexo III, y

ii) 2 de agosto de 2028 en lo que respecta a los sistemas de IA clasificados como de alto riesgo en virtud del artículo 6, apartado 1, y al anexo I;

d) los artículos 102 a 110 serán aplicables a partir del 27 de julio de 2026.

El presente Reglamento será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro.

Fuente: Reglamento (UE) 2024/1689, texto consolidado a 27 de julio de 2026. Transcripción del PDF aportado; se han omitido las marcas editoriales de consolidación y las cabeceras de página.

Resumen del Capítulo XIII — Disposiciones finales

Reglamento (UE) 2024/1689 · Texto consolidado a 27/07/2026 · Páginas 120–127 · Artículos 102 a 113

Este último capítulo es especialmente importante para las empresas porque establece **cuándo deben cumplir las obligaciones del Reglamento Europeo de Inteligencia Artificial, qué ocurre con los sistemas ya instalados y cómo se revisará la normativa en los próximos años**.

También modifica distintas normas europeas sectoriales para incorporar los requisitos de seguridad de la inteligencia artificial.

La idea fundamental: el Reglamento no exige que todos los sistemas de IA se adapten en una única fecha. Establece un calendario progresivo y un régimen transitorio para determinadas soluciones existentes.

1. Artículos 102 a 110. Modificaciones de otras normativas europeas

Páginas 120–124

Estos artículos adaptan diferentes reglamentos y directivas europeos para que sus disposiciones tengan en cuenta los requisitos de IA establecidos en el capítulo III, sección 2.

Artículo	Normativa modificada	Ámbito
102	Reglamento (CE) 300/2008	Seguridad de la aviación civil
103	Reglamento (UE) 167/2013	Vehículos agrícolas y forestales
104	Reglamento (UE) 168/2013	Vehículos de dos o tres ruedas y cuatriciclos
105	Directiva 2014/90/UE	Equipos marinos
106	Directiva (UE) 2016/797	Interoperabilidad ferroviaria
107	Reglamento (UE) 2018/858	Homologación de vehículos de motor
108	Reglamento (UE) 2018/1139	Seguridad de la aviación
109	Reglamento (UE) 2019/2144	Seguridad general de vehículos
110	Directiva (UE) 2020/1828	Acciones de representación para proteger intereses colectivos de consumidores

¿Qué persiguen estas modificaciones?

La finalidad principal es coordinar el Reglamento de IA con la legislación sectorial existente.

Cuando un sistema de IA se utiliza como componente de seguridad de determinados productos, las normas técnicas y los procedimientos sectoriales deben tener en cuenta los requisitos pertinentes sobre inteligencia artificial.

Por ejemplo, una máquina o equipo cuyo funcionamiento dependa de sistemas inteligentes relacionados con la seguridad puede estar sujeto tanto a su regulación sectorial como a los requisitos aplicables del Reglamento de IA.

El artículo 110 tiene una finalidad diferente: incorpora el Reglamento de IA a la normativa europea sobre acciones de representación para la protección de los intereses colectivos de los consumidores.

Repercusión empresarial

Estas modificaciones afectan especialmente a fabricantes de productos regulados, proveedores tecnológicos e integradores de IA en sistemas industriales, vehículos, infraestructuras o equipos sujetos a regulación específica.

Para un ERP como Sage 200, la conexión con maquinaria o sistemas industriales **no convierte automáticamente al ERP en un sistema de alto riesgo**. Lo relevante es la función concreta de la IA y su posible intervención en componentes de seguridad.

2. Artículo 111. Sistemas de IA existentes y períodos transitorios

Página 124

Uno de los artículos más importantes para las empresas

Este artículo determina qué sucede con los sistemas de IA que ya se habían comercializado o puesto en funcionamiento antes de determinadas fechas.

El Reglamento distingue diferentes situaciones.

A. Sistemas de IA de alto riesgo ya comercializados

La redacción consolidada de 2026 establece que, para los sistemas de alto riesgo ya introducidos en el mercado o puestos en servicio antes de la fecha aplicable del capítulo III, las obligaciones correspondientes se aplicarán, como regla general, **si a partir de esa fecha se producen cambios significativos en su diseño**.

Existen excepciones específicas, especialmente para sistemas destinados a autoridades públicas.

Ejemplo: una empresa utiliza un sistema de IA de alto riesgo implantado antes de la fecha de aplicación correspondiente. Si posteriormente introduce cambios significativos en su diseño, puede tener que cumplir los requisitos aplicables del Reglamento conforme al régimen transitorio.

Esto no constituye una exención general frente a las prohibiciones de prácticas de IA del artículo 5 ni frente a otras normas que puedan resultar exigibles.

B. Sistemas de alto riesgo utilizados por autoridades públicas

02/08/2030 — Fecha límite

Los proveedores y responsables del despliegue de sistemas de alto riesgo destinados a ser utilizados por autoridades públicas deben adoptar las medidas necesarias para cumplir las obligaciones aplicables, a más tardar en esta fecha.

C. Grandes sistemas informáticos europeos

Los sistemas de IA que sean componentes de determinados sistemas informáticos de gran magnitud regulados por los actos del anexo X, introducidos en el mercado o puestos en servicio antes del 2 de agosto de 2027, deberán estar adaptados a más tardar el **31 de diciembre de 2030**.

Esta disposición se refiere a los sistemas específicos del anexo X, no a cualquier ERP empresarial de gran tamaño.

D. Modelos de IA de uso general ya existentes

Los proveedores de modelos de IA de uso general comercializados antes del 2 de agosto de 2025 deben adoptar las medidas necesarias para cumplir las obligaciones del Reglamento a más tardar el **2 de agosto de 2027**.

Esto afecta a los proveedores de modelos, no automáticamente a todas las empresas que utilizan sus APIs o servicios.

E. Sistemas que generan contenido sintético

La modificación de 2026 introduce una disposición transitoria específica.

Los proveedores de sistemas de IA que generan audio, imágenes, vídeos o textos sintéticos y que se introdujeron en el mercado antes del 2 de agosto de 2026 tienen hasta el **2 de diciembre de 2026** para cumplir el artículo 50.2, relativo al marcado técnico de contenidos sintéticos.

Se trata de esa obligación concreta, no de una prórroga general para todas las obligaciones de transparencia.

3. Artículo 112. Evaluación y revisión del Reglamento

Páginas 125–127

Este artículo establece un mecanismo de revisión periódica para adaptar el Reglamento a los avances tecnológicos y a la experiencia acumulada.

La Comisión Europea debe evaluar distintas cuestiones, entre ellas la clasificación de los sistemas de alto riesgo, las prácticas prohibidas, la transparencia, los mecanismos de supervisión y la eficacia del régimen regulatorio.

Principales fechas de revisión

Fecha	Actuación prevista
Revisiones anuales	Evaluar la necesidad de modificar el anexo III y la lista de prácticas prohibidas del artículo 5, conforme a las condiciones del artículo 112.1.
02/08/2028	Evaluar posibles ampliaciones del anexo III, cambios en las obligaciones de transparencia y mejoras en la supervisión.
02/08/2028	Evaluar el funcionamiento y los recursos de la Oficina de IA.
02/08/2028	Revisar los avances en normalización sobre eficiencia energética de modelos de uso general.
02/08/2028	Primera evaluación de la eficacia de los códigos de conducta voluntarios.
02/08/2029	Primera evaluación general y revisión del Reglamento, con periodicidad posterior de cuatro años.
02/08/2031	Evaluación de la ejecución del Reglamento y de la estructura institucional de control.

El Reglamento contempla que, a partir de estas evaluaciones, la Comisión pueda proponer modificaciones cuando resulte necesario.

¿Por qué es relevante?

Una clasificación o interpretación regulatoria que hoy se aplique a una solución de IA puede verse afectada en el futuro por cambios normativos.

Para fabricantes de software e integradores resulta conveniente mantener un seguimiento periódico, especialmente cuando comercializan soluciones a múltiples clientes o sectores.

4. Artículo 113. Entrada en vigor y aplicación

Página 127

Calendario fundamental

El artículo 113 es el que establece las principales fechas de aplicación del Reglamento.

La versión consolidada de julio de 2026 modifica varios plazos respecto del calendario inicial.

Calendario de aplicación 2025–2028

02/02/2025 — Aplicable

Capítulos I y II

Disposiciones generales, alfabetización en IA y prácticas prohibidas.

Excepción: las nuevas prohibiciones y apartados incorporados al artículo 5 en 2026 se aplican desde el 02/12/2026.

02/08/2025 — Aplicable

Capítulos y disposiciones específicas

Capítulo III, sección 4; capítulos V, VII y XII; y artículo 78.

Excepto el artículo 101, relativo a multas a proveedores de modelos de uso general.

27/07/2026 — Aplicable

Artículos 102 a 110

Modificaciones de la legislación sectorial europea previstas en el capítulo XIII.

02/08/2026 — Aplicable

Aplicación general del Reglamento

Entrada en aplicación de las demás disposiciones no sujetas a plazos específicos, incluido el artículo 101.

02/12/2026 — Próxima

Nuevas prohibiciones incorporadas al artículo 5

Aplicación de las letras b bis y b ter y de los apartados 1 bis y 1 ter.

02/12/2027 — Pendiente

Sistemas de alto riesgo del anexo III

Aplicación de las secciones 1, 2 y 3 del capítulo III a los sistemas clasificados conforme al artículo 6.2 y al anexo III, con la excepción indicada en el artículo 113.

02/08/2028 — Pendiente

Sistemas de alto riesgo vinculados al anexo I

Aplicación de las secciones 1, 2 y 3 del capítulo III a los sistemas clasificados conforme al artículo 6.1.

Calendario transcrito e interpretado a partir del artículo 113 de la versión consolidada aportada. Debe leerse junto con las reglas transitorias del artículo 111.

5. ¿Cómo afecta a las empresas?

La repercusión depende del tipo de sistema de IA y de si ya se encuentra en funcionamiento.

Tipo de aplicación	Principal consideración temporal
Chatbot empresarial	Las obligaciones aplicables, como determinadas reglas de transparencia, están sujetas al calendario general y a sus excepciones.
IA que realiza prácticas prohibidas	Debe respetar el calendario del artículo 5, incluidas las prohibiciones que entran en aplicación en diciembre de 2026.
IA de alto riesgo para selección de personal	Las principales obligaciones del capítulo III aplican desde el 02/12/2027, conforme al texto consolidado.
IA de alto riesgo vinculada a productos del anexo I	Aplicación de las obligaciones correspondientes desde el 02/08/2028.
Sistema de alto riesgo ya comercializado	Debe analizarse el régimen transitorio del artículo 111.

Tipo de aplicación	Principal consideración temporal
Modelo de uso general comercializado antes de agosto de 2025	Período de adaptación hasta el 02/08/2027 para su proveedor.

Atención: estas fechas no suspenden otras normas, como el RGPD, la legislación laboral o los requisitos sectoriales que ya sean aplicables.

6. ¿Qué implica para Sage 200 y las integraciones con IA?

Consideremos tres escenarios empresariales.

Escenario A. Automatización contable y administrativa

Una empresa incorpora IA para contabilizar facturas, analizar saldos o generar informes.

Estas funciones no implican por sí mismas una clasificación de alto riesgo. Deben analizarse las obligaciones generales que correspondan y sus fechas de aplicación.

Escenario B. IA para recursos humanos

Una solución que evalúa candidatos o interviene en determinadas decisiones laborales puede clasificarse como de alto riesgo conforme al anexo III.

El calendario consolidado sitúa la aplicación de las principales obligaciones de las secciones 1–3 del capítulo III el 2 de diciembre de 2027, sin perjuicio de las demás obligaciones ya exigibles y las reglas transitorias.

Escenario C. IA integrada en maquinaria

Si una integración forma parte de un componente de seguridad de un producto incluido en el anexo I y reúne las condiciones del artículo 6.1, el calendario establece el 2 de agosto de 2028 para las obligaciones correspondientes del capítulo III.

Deben considerarse también las exigencias de la legislación sectorial del producto.

Precaución con los sistemas existentes

No debe suponerse que todo sistema de IA previamente instalado está obligado a adaptarse automáticamente en las mismas condiciones que uno nuevo.

El artículo 111 establece tratamientos diferenciados según la fecha de comercialización, el tipo de sistema, su finalidad y la existencia de cambios significativos.

Por eso resulta importante documentar la fecha de implantación y las modificaciones relevantes del sistema.

7. Conclusión del capítulo XIII

Este capítulo cierra el Reglamento estableciendo tres elementos fundamentales: **la coordinación con otras normas europeas, los períodos transitorios para sistemas existentes y el calendario progresivo de aplicación**.

Para las empresas, su importancia es especialmente práctica.

No basta con saber qué obligaciones establece el Reglamento. También hay que conocer cuándo son exigibles, si existen excepciones transitorias y si una modificación del sistema puede alterar su situación jurídica.

La conclusión más relevante para el sector ERP es que **la incorporación de inteligencia artificial requiere evaluar tanto la función de la herramienta como su clasificación, fecha de puesta en servicio y posibles modificaciones posteriores**.

El capítulo XIII demuestra además que la regulación europea seguirá sometida a evaluaciones y revisiones periódicas, por lo que el seguimiento normativo deberá mantenerse actualizado.

Resumen basado en los artículos 102 a 113 del texto consolidado de 27 de julio de 2026 que has facilitado.

ANEXO I

LISTA DE ACTOS LEGISLATIVOS DE ARMONIZACIÓN DE LA UNIÓN

SECCIÓN A — LISTA DE ACTOS LEGISLATIVOS DE ARMONIZACIÓN DE LA UNIÓN BASADOS EN EL NUEVO MARCO LEGISLATIVO

2. Directiva 2009/48/CE del Parlamento Europeo y del Consejo, de 18 de junio de 2009, sobre la seguridad de los juguetes (DO L 170 de 30.6.2009, p. 1)
3. Directiva 2013/53/UE del Parlamento Europeo y del Consejo, de 20 de noviembre de 2013, relativa a las embarcaciones de recreo y a las motos acuáticas, y por la que se deroga la Directiva 94/25/CE (DO L 354 de 28.12.2013, p. 90)
4. Directiva 2014/33/UE del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, sobre la armonización de las legislaciones de los Estados miembros en materia de ascensores y componentes de seguridad para ascensores (DO L 96 de 29.3.2014, p. 251)
5. Directiva 2014/34/UE del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, sobre la armonización de las legislaciones de los Estados miembros en materia de aparatos y sistemas de protección para uso en atmósferas potencialmente explosivas (DO L 96 de 29.3.2014, p. 309)
6. Directiva 2014/53/UE del Parlamento Europeo y del Consejo, de 16 de abril de 2014, relativa a la armonización de las legislaciones de los Estados miembros sobre la comercialización de equipos radioeléctricos, y por la que se deroga la Directiva 1999/5/CE (DO L 153 de 22.5.2014, p. 62)
7. Directiva 2014/68/UE del Parlamento Europeo y del Consejo, de 15 de mayo de 2014, relativa a la armonización de las legislaciones de los Estados miembros sobre la comercialización de equipos a presión (DO L 189 de 27.6.2014, p. 164)
8. Reglamento (UE) 2016/424 del Parlamento Europeo y del Consejo, de 9 de marzo de 2016, relativo a las instalaciones de transporte por cable y por el que se deroga la Directiva 2000/9/CE (DO L 81 de 31.3.2016, p. 1)
9. Reglamento (UE) 2016/425 del Parlamento Europeo y del Consejo, de 9 de marzo de 2016, relativo a los equipos de protección individual y por el que se deroga la Directiva 89/686/CEE del Consejo (DO L 81 de 31.3.2016, p. 51)
10. Reglamento (UE) 2016/426 del Parlamento Europeo y del Consejo, de 9 de marzo de 2016, sobre los aparatos que queman combustibles gaseosos y por el que se deroga la Directiva 2009/142/CE (DO L 81 de 31.3.2016, p. 99)
11. Reglamento (UE) 2017/745 del Parlamento Europeo y del Consejo, de 5 de abril de 2017, sobre los productos sanitarios, por el que se modifican la Directiva 2001/83/CE, el Reglamento (CE) n. o 178/2002 y el Reglamento (CE) n. o 1223/2009 y por el que se derogan las Directivas 90/385/CEE y 93/42/CEE del Consejo (DO L 117 de 5.5.2017, p. 1)
12. Reglamento (UE) 2017/746 del Parlamento Europeo y del Consejo, de 5 de abril de 2017, sobre los productos sanitarios para diagnóstico in vitro y por el que se derogan la Directiva 98/79/CE y la Decisión 2010/227/UE de la Comisión (DO L 117 de 5.5.2017, p. 176)

SECCIÓN B — LISTA DE OTROS ACTOS LEGISLATIVOS DE ARMONIZACIÓN DE LA UNIÓN

13. Reglamento (CE) n. o 300/2008 del Parlamento Europeo y del Consejo, de 11 de marzo de 2008, sobre normas comunes para la seguridad de la aviación civil y por el que se deroga el Reglamento (CE) n. o 2320/2002 (DO L 97 de 9.4.2008, p. 72)
14. Reglamento (UE) n. o 168/2013 del Parlamento Europeo y del Consejo, de 15 de enero de 2013, relativo a la homologación de los vehículos de dos o tres ruedas y los cuatriciclos, y a la vigilancia del mercado de dichos vehículos (DO L 60 de 2.3.2013, p. 52)
15. Reglamento (UE) n. o 167/2013 del Parlamento Europeo y del Consejo, de 5 de febrero de 2013, relativo a la homologación de los vehículos agrícolas o forestales, y a la vigilancia del mercado de dichos vehículos (DO L 60 de 2.3.2013, p. 1)
16. Directiva 2014/90/UE del Parlamento Europeo y del Consejo, de 23 de julio de 2014, sobre equipos marinos, y por la que se deroga la Directiva 96/98/CE del Consejo (DO L 257 de 28.8.2014, p. 146)
17. Directiva (UE) 2016/797 del Parlamento Europeo y del Consejo, de 11 de mayo de 2016, sobre la interoperabilidad del sistema ferroviario dentro de la Unión Europea (DO L 138 de 26.5.2016, p. 44)
18. Reglamento (UE) 2018/858 del Parlamento Europeo y del Consejo, de 30 de mayo de 2018, sobre la homologación y la vigilancia del mercado de los vehículos de motor y sus remolques y de los sistemas, los componentes y las unidades técnicas independientes destinados a dichos vehículos, por el que se modifican los Reglamentos (CE) n. o 715/2007 y (CE) n. o 595/2009 y por el que se deroga la Directiva 2007/46/CE (DO L 151 de 14.6.2018, p. 1)
19. Reglamento (UE) 2019/2144 del Parlamento Europeo y del Consejo, de 27 de noviembre de 2019, relativo a los requisitos de homologación de tipo de los vehículos de motor y de sus remolques, así como de los sistemas, componentes y unidades técnicas independientes destinados a esos vehículos, en lo que respecta a su seguridad general y a la protección de los ocupantes de los vehículos y de los usuarios vulnerables de la vía pública, por el que se modifica el Reglamento (UE) 2018/858 del Parlamento Europeo y del Consejo y se derogan los Reglamentos (CE) n. o 78/2009, (CE) n. o 79/2009 y (CE) n. o 661/2009 del Parlamento Europeo y del Consejo y los Reglamentos (CE) n. o 631/2009, (UE) n. o 406/2010, (UE) n. o 672/2010, (UE) n. o 1003/2010, (UE) n. o 1005/2010, (UE) n. o 1008/2010, (UE) n. o 1009/2010, (UE) n. o 19/2011, (UE) n. o 109/2011, (UE) n. o 458/2011, (UE) n. o 65/2012, (UE) n. o 130/2012, (UE) n. o 347/2012, (UE) n. o 351/2012, (UE) n. o 1230/2012 y (UE) 2015/166 de la Comisión (DO L 325 de 16.12.2019, p. 1)
20. Reglamento (UE) 2018/1139 del Parlamento Europeo y del Consejo, de 4 de julio de 2018, sobre normas comunes en el ámbito de la aviación civil y por el que se crea una Agencia de la Unión Europea para la Seguridad Aérea y por el que se modifican los Reglamentos (CE) n. o 2111/2005, (CE) n. o 1008/2008, (UE) n. o 996/2010 y (UE) n. o 376/2014 y las Directivas 2014/30/UE y 2014/53/UE del Parlamento Europeo y del Consejo y se derogan los Reglamentos (CE) n. o 552/2004 y (CE) n. o 216/2008 del Parlamento Europeo y del Consejo y el

Reglamento (CEE) n. o 3922/91 del Consejo (DO L 212 de 22.8.2018, p. 1), en la medida en que afecte al diseño, la producción y la introducción en el mercado de aeronaves a que se refiere el artículo 2, apartado 1, letras a) y b), por lo que respecta a las aeronaves no tripuladas y sus motores, hélices, componentes y equipos para controlarlas a distancia

21. Reglamento (UE) 2023/1230 del Parlamento Europeo y del Consejo, de 14 de junio de 2023, relativo a las máquinas, y por el que se derogan la Directiva 2006/42/CE del Parlamento Europeo y del Consejo y la Directiva 73/361/CEE del Consejo (DO L 165 de 29.6.2023, p. 1, ELI: http:// data.europa.eu/eli/reg/2023/1230/oj).

Fuente: Reglamento (UE) 2024/1689, texto consolidado a 27 de julio de 2026. Transcripción del PDF aportado; se han omitido las marcas editoriales de consolidación y las cabeceras de página.

Resumen del Anexo I — Legislación europea sobre productos y sistemas de IA

Reglamento (UE) 2024/1689 · Texto consolidado a 27/07/2026 · Páginas 128–129

Hemos terminado los 13 capítulos del Reglamento. A continuación vienen los **anexos**, que concretan aspectos importantes de su aplicación.

Empezamos por el **Anexo I: Lista de actos legislativos de armonización de la Unión**.

Este anexo es fundamental para las empresas industriales y los fabricantes de productos porque identifica las normativas sectoriales relacionadas con los sistemas de inteligencia artificial.

La idea principal: determinados productos que incorporan IA relacionada con la seguridad pueden quedar sujetos tanto a la normativa específica del producto como a los requisitos del Reglamento Europeo de IA.

1. ¿Qué regula el Anexo I?

El anexo contiene dos secciones:

Sección	Contenido	Importancia
A	Legislación de productos basada en el nuevo marco legislativo europeo	Está directamente vinculada al mecanismo de clasificación de alto riesgo del artículo 6.1.
B	Otros actos legislativos sectoriales de armonización	Permite coordinar los requisitos de IA con la regulación de sectores específicos.

La inclusión de una normativa en el anexo no significa que todos los productos de ese sector sean automáticamente sistemas de IA de alto riesgo.

2. Sección A — Productos sujetos al nuevo marco legislativo

La lista incluye:

Normativa	Productos regulados
Directiva 2009/48/CE	Seguridad de los juguetes
Directiva 2013/53/UE	Embarcaciones de recreo y motos acuáticas
Directiva 2014/33/UE	Ascensores y componentes de seguridad
Directiva 2014/34/UE	Equipos para atmósferas potencialmente explosivas
Directiva 2014/53/UE	Equipos radioeléctricos
Directiva 2014/68/UE	Equipos a presión
Reglamento (UE) 2016/424	Instalaciones de transporte por cable
Reglamento (UE) 2016/425	Equipos de protección individual
Reglamento (UE) 2016/426	Aparatos que queman combustibles gaseosos
Reglamento (UE) 2017/745	Productos sanitarios
Reglamento (UE) 2017/746	Productos sanitarios para diagnóstico in vitro

En la versión consolidada aportada, el punto 1 de esta sección aparece suprimido.

¿Cuándo una IA vinculada a estos productos es de alto riesgo?

El artículo 6.1 establece dos condiciones acumulativas:

1. Que la IA sea un componente de seguridad del producto regulado, o constituya por sí misma uno de esos productos.
2. Que el producto o sistema correspondiente requiera una evaluación de conformidad de terceros conforme a la legislación sectorial pertinente.

Además, deben considerarse las precisiones incorporadas al artículo 6 en 2026 sobre los componentes de seguridad.

Ejemplo: un dispositivo médico que utiliza IA para realizar una función crítica puede estar sujeto a los requisitos de alto riesgo si cumple las condiciones legales.

En cambio, una aplicación administrativa que utiliza IA para gestionar las compras de un hospital no se clasifica como de alto riesgo simplemente por pertenecer al sector sanitario.

3. Sección B — Otras normativas sectoriales

Esta sección recoge los siguientes ámbitos:

Normativa	Sector
Reglamento (CE) 300/2008	Seguridad de la aviación civil
Reglamento (UE) 168/2013	Vehículos de dos o tres ruedas y cuatriciclos
Reglamento (UE) 167/2013	Vehículos agrícolas y forestales
Directiva 2014/90/UE	Equipos marinos
Directiva (UE) 2016/797	Sistemas ferroviarios
Reglamento (UE) 2018/858	Homologación de vehículos de motor
Reglamento (UE) 2019/2144	Seguridad general de vehículos
Reglamento (UE) 2018/1139	Aviación y determinadas aeronaves no tripuladas
Reglamento (UE) 2023/1230	Máquinas y maquinaria

Novedad relevante de 2026: maquinaria

En el texto consolidado, el **Reglamento (UE) 2023/1230 sobre máquinas figura en la sección B**, como punto 21.

Esto es importante para los proyectos de integración de inteligencia artificial en entornos industriales.

No debe aplicarse automáticamente a un sistema incluido en esta sección el mismo mecanismo de clasificación del artículo 6.1 previsto para los productos de la sección A. Hay que considerar las disposiciones específicas de coordinación con la normativa sectorial correspondiente.

4. Aplicación práctica a la industria y a los ERP

Imaginemos una fábrica que utiliza Sage 200 como ERP y lo conecta con diferentes soluciones tecnológicas.

Funcionalidad	Consideración normativa
IA que realiza previsiones de producción	No es de alto riesgo por esta función por sí sola.
IA que optimiza compras y aprovisionamientos	No es de alto riesgo por su mera automatización.
IA que analiza datos de un sistema MES	Depende de la función que realice.
IA que interviene en la seguridad de una máquina	Requiere analizar la normativa sectorial y los requisitos de seguridad aplicables.
IA integrada en un producto sanitario	Puede estar sujeta a la clasificación de alto riesgo del artículo 6.1.
IA que controla funciones de seguridad de un producto regulado	Puede requerir medidas reforzadas según su clasificación y legislación sectorial.

La clave está en distinguir entre **la IA que gestiona información de un proceso industrial y la IA que interviene directamente en funciones de seguridad**.

Por ejemplo, Sage 200 puede recibir información de una máquina sobre consumos, tiempos de fabricación o incidencias.

Esa integración no convierte automáticamente al ERP en un sistema de alto riesgo.

Sin embargo, si una solución de IA participa en el control de funciones de seguridad de un producto regulado, debe analizarse con mayor profundidad su clasificación y sus obligaciones.

5. ¿Cuándo son aplicables estos requisitos?

El artículo 113 del texto consolidado establece el **2 de agosto de 2028** como fecha de aplicación de las secciones 1, 2 y 3 del capítulo III para los sistemas clasificados como de alto riesgo conforme al artículo 6.1 y el anexo I.

Esta fecha está sujeta a las disposiciones transitorias y no sustituye los plazos de cumplimiento de otras normas sectoriales que ya sean aplicables.

6. Conclusión del Anexo I

El Anexo I sirve para identificar las normas europeas sobre productos que deben coordinarse con el Reglamento de Inteligencia Artificial.

Para las empresas industriales, su mayor importancia está en la utilización de IA en maquinaria, dispositivos, vehículos, equipos e instalaciones sometidos a regulación específica.

Conclusión para el entorno Sage 200: conectar un ERP con maquinaria, equipos industriales o aplicaciones de fabricación no implica automáticamente que toda la solución sea de alto riesgo. Lo decisivo es identificar si la inteligencia artificial desarrolla funciones de seguridad reguladas y qué normativa sectorial resulta aplicable.

El siguiente es el **Anexo II**, que contiene la lista de delitos relacionados con determinadas excepciones a la prohibición de identificación biométrica remota en tiempo real prevista en el artículo 5.

Resumen elaborado a partir del Anexo I del documento consolidado aportado.

Resumen de los anexos II al XIV del Reglamento Europeo de Inteligencia Artificial

Reglamento (UE) 2024/1689 · Texto consolidado a 27/07/2026 · Páginas 130–151

Los anexos son una parte fundamental del Reglamento porque concretan **qué sistemas se consideran de alto riesgo, qué documentación deben preparar los proveedores, cómo se demuestra el cumplimiento y qué información deben facilitar los fabricantes de modelos de IA**.

He revisado los trece anexos restantes del documento que estamos estudiando. Me centraré especialmente en los que tienen consecuencias prácticas para las empresas y para la integración de IA con software empresarial.

1. Visión general: qué anexos son realmente importantes

Anexo	Contenido	Importancia empresarial
II	Delitos relacionados con excepciones al reconocimiento biométrico	Baja, salvo sectores policiales
III	**Sistemas de IA de alto riesgo**	**Muy alta**
IV	**Documentación técnica de sistemas de alto riesgo**	**Muy alta**
V	Declaración UE de conformidad	Alta para proveedores afectados
VI	**Evaluación de conformidad mediante control interno**	**Alta**
VII	Evaluación con organismo notificado	Alta cuando corresponda
VIII	Registro europeo de sistemas de IA	Alta para sistemas registrables
IX	Registro de pruebas en condiciones reales	Media
X	Grandes sistemas informáticos europeos	Baja para empresas ordinarias
XI	**Documentación técnica de modelos de uso general**	**Alta para fabricantes de modelos**
XII	**Información técnica para empresas integradoras**	**Muy alta para desarrolladores**
XIII	Clasificación de modelos con riesgo sistémico	Alta para fabricantes de grandes modelos
XIV	**Categorías y códigos tecnológicos de IA, incluida IA agente**	**Relevante para el sector tecnológico**

TEXTO OFICIAL · ANEXO II

ANEXO II

LISTA DE LOS DELITOS A QUE SE REFIERE EL ARTÍCULO 5, APARTADO 1, PÁRRAFO PRIMERO, LETRA H), INCISO III)

Delitos a que se refiere el artículo 5, apartado 1, párrafo primero, letra h), inciso iii):

— terrorismo,

— trata de seres humanos,

— explotación sexual de menores y pornografía infantil,

— tráfico ilícito de estupefacientes o sustancias psicotrópicas,

— tráfico ilícito de armas, municiones y explosivos,

— homicidio voluntario, agresión con lesiones graves,

— tráfico ilícito de órganos o tejidos humanos,

— tráfico ilícito de materiales nucleares o radiactivos,

— secuestro, detención ilegal o toma de rehenes,

— delitos que son competencia de la Corte Penal Internacional,

— secuestro de aeronaves o buques,

— violación,

— delitos contra el medio ambiente,

— robo organizado o a mano armada,

— sabotaje,

— participación en una organización delictiva implicada en uno o varios de los delitos enumerados en esta lista.

Fuente: Reglamento (UE) 2024/1689, texto consolidado a 27 de julio de 2026. Transcripción del PDF aportado; se han omitido las marcas editoriales de consolidación y las cabeceras de página.

2. Anexo II — Delitos relacionados con determinadas excepciones biométricas

Página 130

Este anexo contiene la lista de delitos a los que se refiere el artículo 5.1.h.iii.

Está relacionado con las condiciones excepcionales en las que podría autorizarse la utilización de sistemas de identificación biométrica remota en tiempo real en espacios de acceso público con fines policiales.

La lista comprende, entre otros, terrorismo, trata de seres humanos, explotación sexual de menores, tráfico de armas o drogas, homicidio, secuestro, violación, delitos contra el medio ambiente y participación en determinadas organizaciones delictivas.

¿Qué es importante?

El anexo no autoriza por sí mismo a utilizar reconocimiento facial indiscriminadamente.

La utilización debe cumplir las condiciones restrictivas y garantías del artículo 5, incluidas las autorizaciones exigibles.

Repercusión para empresas: generalmente limitada, salvo proveedores de tecnología biométrica destinada a las autoridades competentes.

TEXTO OFICIAL · ANEXO III

ANEXO III

SISTEMAS DE IA DE ALTO RIESGO A QUE SE REFIERE EL ARTÍCULO 6, APARTADO 2

Los sistemas de IA de alto riesgo con arreglo al artículo 6, apartado 2, son los sistemas de IA que formen parte de cualquiera de los ámbitos siguientes:

1. Biometría, en la medida en que su uso esté permitido por el Derecho de la Unión o nacional aplicable:
   a) Sistemas de identificación biométrica remota

   Quedan excluidos los sistemas de IA destinados a ser utilizados con fines de verificación biométrica cuya única finalidad sea confirmar que una persona física concreta es la persona que afirma ser
   b) Sistemas de IA destinados a ser utilizados para la categorización biométrica en función de atributos o características sensibles o protegidos basada en la inferencia de dichos atributos o características
   c) Sistemas de IA destinados a ser utilizados para el reconocimiento de emociones
2. Infraestructuras críticas: Sistemas de IA destinados a ser utilizados como componentes de seguridad en la gestión y el funcionamiento de las infraestructuras digitales críticas, del tráfico rodado o del suministro de agua, gas, calefacción o electricidad
3. Educación y formación profesional:
   a) Sistemas de IA destinados a ser utilizados para determinar el acceso o la admisión de personas físicas a centros educativos y de formación profesional a todos los niveles o para distribuir a las personas físicas entre dichos centros
   b) Sistemas de IA destinados a ser utilizados para evaluar los resultados del aprendizaje, también cuando dichos resultados se utilicen para orientar el proceso de aprendizaje de las personas físicas en centros educativos y de formación profesional a todos los niveles
   c) Sistemas de IA destinados a ser utilizados para evaluar el nivel de educación adecuado que recibirá una persona o al que podrá acceder, en el contexto de los centros educativos y de formación profesional o dentro de estos a todos los niveles
   d) Sistemas de IA destinados a ser utilizados para el seguimiento y la detección de comportamientos prohibidos por parte de los estudiantes durante los exámenes en el contexto de los centros educativos y de formación profesional o dentro de estos a todos los niveles
4. Empleo, gestión de los trabajadores y acceso al autoempleo:
   a) Sistemas de IA destinados a ser utilizados para la contratación o la selección de personas físicas, en particular para publicar anuncios de empleo específicos, analizar y filtrar las solicitudes de empleo y evaluar a los candidatos
   b) Sistemas de IA destinados a ser utilizados para tomar decisiones que afecten a las condiciones de las relaciones de índole laboral o a la promoción o rescisión de relaciones contractuales de índole laboral, para la asignación de tareas a partir de comportamientos individuales o rasgos o características personales o para supervisar y evaluar el rendimiento y el comportamiento de las personas en el marco de dichas relaciones
5. Acceso a servicios privados esenciales y a servicios y prestaciones públicos esenciales y disfrute de estos servicios y prestaciones:
   a) Sistemas de IA destinados a ser utilizados por las autoridades públicas o en su nombre para evaluar la admisibilidad de las personas físicas para beneficiarse de servicios y prestaciones esenciales de asistencia pública, incluidos los servicios de asistencia sanitaria, así como para conceder, reducir o retirar dichos servicios y prestaciones o reclamar su devolución
   b) Sistemas de IA destinados a ser utilizados para evaluar la solvencia de personas físicas o establecer su calificación crediticia, salvo los sistemas de IA utilizados al objeto de detectar fraudes financieros
   c) Sistemas de IA destinados a ser utilizados para la evaluación de riesgos y la fijación de precios en relación con las personas físicas en el caso de los seguros de vida y de salud
   d) Sistemas de IA destinados a ser utilizados para la evaluación y la clasificación de las llamadas de emergencia realizadas por personas físicas o para el envío o el establecimiento de prioridades en el envío de servicios de primera intervención en situaciones de emergencia, por ejemplo, policía, bomberos y servicios de asistencia médica, y en sistemas de triaje de pacientes en el contexto de la asistencia sanitaria de urgencia
6. Garantía del cumplimiento del Derecho, en la medida en que su uso esté permitido por el Derecho de la Unión o nacional aplicable:
   a) Sistemas de IA destinados a ser utilizados por las autoridades garantes del cumplimiento del Derecho, o en su nombre, o por las instituciones, órganos y organismos de la Unión en apoyo de las autoridades garantes del cumplimiento del Derecho, o en su nombre, para evaluar el riesgo de que una persona física sea víctima de delitos
   b) Sistemas de IA destinados a ser utilizados por las autoridades garantes del cumplimiento del Derecho, o en su nombre, o por las instituciones, órganos y organismos de la Unión en apoyo de las autoridades garantes del cumplimiento del Derecho como polígrafos o herramientas similares
   c) Sistemas de IA destinados a ser utilizados por las autoridades garantes del cumplimiento del Derecho, o en su nombre, o por las instituciones, órganos y organismos de la Unión en apoyo de las autoridades garantes del cumplimiento del Derecho para evaluar la fiabilidad de las pruebas durante la investigación o el enjuiciamiento de delitos
   d) Sistemas de IA destinados a ser utilizados por las autoridades garantes del cumplimiento del Derecho, o en su nombre, o por las instituciones, órganos y organismos de la Unión en apoyo de las autoridades garantes del cumplimiento del Derecho para evaluar el riesgo de que una persona física cometa un delito o reincida en la comisión de un delito atendiendo no solo a la elaboración de perfiles de personas físicas mencionada en el artículo 3, punto 4, de la Directiva (UE) 2016/680 o para evaluar rasgos y características de la personalidad o comportamientos delictivos pasados de personas físicas o colectivos

e) Sistemas de IA destinados a ser utilizados por las autoridades garantes del cumplimiento del Derecho, o en su nombre, o por las instituciones, órganos y organismos de la Unión en apoyo de las autoridades garantes del cumplimiento del Derecho para elaborar perfiles de personas físicas, como se menciona en el artículo 3, punto 4, de la Directiva (UE) 2016/680, durante la detección, la investigación o el enjuiciamiento de delitos

7. Migración, asilo y gestión del control fronterizo, en la medida en que su uso esté permitido por el Derecho de la Unión o nacional aplicable:

a) Sistemas de IA destinados a ser utilizados por las autoridades públicas competentes, o en su nombre, o por las instituciones, órganos y organismos de la Unión, como polígrafos o herramientas similares

b) Sistemas de IA destinados a ser utilizados por las autoridades públicas competentes, o en su nombre, o por las instituciones, órganos y organismos de la Unión para evaluar un riesgo, por ejemplo, un riesgo para la seguridad, la salud o de migración irregular, que plantee una persona física que tenga la intención de entrar en el territorio de un Estado miembro o haya entrado en él

c) Sistemas de IA destinados a ser utilizados por las autoridades públicas competentes, o en su nombre, o por las instituciones, órganos y organismos de la Unión para ayudar a las autoridades públicas competentes a examinar las solicitudes de asilo, visado o permiso de residencia y las reclamaciones conexas con el fin de determinar si las personas físicas solicitantes reúnen los requisitos necesarios para que se conceda su solicitud, con inclusión de la evaluación conexa de la fiabilidad de las pruebas

d) Sistemas de IA destinados a ser utilizados por las autoridades públicas competentes, o en su nombre, o por las instituciones, órganos y organismos de la Unión, en el contexto de la migración, el asilo o la gestión del control fronterizo, con el fin de detectar, reconocer o identificar a personas físicas, con excepción de la verificación de documentos de viaje

8. Administración de justicia y procesos democráticos:

a) Sistemas de IA destinados a ser utilizados por una autoridad judicial, o en su nombre, para ayudar a una autoridad judicial en la investigación e interpretación de hechos y de la ley, así como en la garantía del cumplimiento del Derecho a un conjunto concreto de hechos, o a ser utilizados de forma similar en una resolución alternativa de litigios;

b) Sistemas de IA destinados a ser utilizados para influir en el resultado de una elección o referéndum o en el comportamiento electoral de personas físicas que ejerzan su derecho de voto en elecciones o referendos. Quedan excluidos los sistemas de IA a cuyos resultados de salida no estén directamente expuestos las personas físicas, como las herramientas utilizadas para organizar, optimizar o estructurar campañas políticas desde un punto de vista administrativo o logístico.

Fuente: Reglamento (UE) 2024/1689, texto consolidado a 27 de julio de 2026. Transcripción del PDF aportado; se han omitido las marcas editoriales de consolidación y las cabeceras de página.

3. Anexo III — Sistemas de IA considerados de alto riesgo

Uno de los anexos más importantes de todo el Reglamento

Páginas 131–133 · Relacionado con el artículo 6.2

Este anexo identifica **ocho grandes ámbitos de utilización de IA especialmente sensibles**.

Su importancia radica en que determinados sistemas destinados a estos usos están sujetos al régimen de alto riesgo y a sus obligaciones específicas.

Las ocho categorías

Nº	Categoría	Aplicaciones incluidas
1	Biometría	Identificación biométrica remota, determinada categorización biométrica y reconocimiento de emociones.
2	Infraestructuras críticas	Componentes de seguridad en infraestructuras digitales críticas, tráfico rodado y suministros de agua, gas, calefacción o electricidad.
3	Educación	Admisión, evaluación del aprendizaje, asignación de niveles educativos y detección de conductas prohibidas en exámenes.
4	**Empleo y recursos humanos**	**Selección, contratación, promoción, despido, asignación de tareas y evaluación de trabajadores.**
5	**Servicios esenciales**	**Prestaciones públicas, evaluación crediticia de personas físicas, determinados seguros y servicios de emergencia.**
6	Actividades policiales	Determinados sistemas de evaluación de riesgos, pruebas, perfiles y apoyo a investigaciones.
7	Migración y fronteras	Evaluaciones de riesgos, tramitación de solicitudes y determinados sistemas de identificación de personas.
8	Justicia y procesos democráticos	Apoyo a determinadas decisiones judiciales e IA destinada a influir en elecciones o referendos.

Especial atención: recursos humanos

El punto 4 es particularmente importante para el software empresarial.

Incluye sistemas de IA destinados a:

- Analizar y filtrar currículums.
- Evaluar candidatos en procesos de contratación.
- Adoptar o apoyar decisiones sobre condiciones laborales, promociones o finalización de relaciones contractuales.
- Asignar tareas basándose en comportamientos individuales o características personales.
- Supervisar y evaluar el rendimiento o comportamiento de trabajadores.

Ejemplo: un módulo de recursos humanos conectado a Sage 200 que evalúa candidatos y propone automáticamente a quién contratar puede entrar en el ámbito de alto riesgo.

En cambio, una aplicación que simplemente calcula nóminas o registra vacaciones no se considera de alto riesgo por esas funciones administrativas.

Especial atención: evaluación crediticia

El punto 5 incluye sistemas destinados a evaluar la solvencia o establecer calificaciones crediticias de personas físicas, salvo los sistemas utilizados para detectar fraudes financieros.

Esto es relevante para soluciones financieras, aseguradoras y determinadas herramientas de análisis crediticio.

Importante: no equivale a considerar de alto riesgo cualquier previsión de tesorería o análisis de riesgo comercial entre empresas.

¿Todo sistema incluido en el anexo III es automáticamente de alto riesgo?

No necesariamente.

El artículo 6.3 establece una excepción para determinados sistemas que no presentan un riesgo importante para la salud, la seguridad o los derechos fundamentales y que cumplen alguna de las condiciones previstas, como realizar una tarea de procedimiento limitada o una tarea preparatoria.

Sin embargo, hay una regla esencial:

Los sistemas del anexo III que realizan elaboración de perfiles de personas físicas siempre se consideran de alto riesgo conforme al artículo 6.3.

Cuando un proveedor utiliza la excepción para considerar que su sistema no es de alto riesgo, debe documentar esa evaluación y cumplir la obligación de registro correspondiente.

Fecha de aplicación

El texto consolidado establece el **2 de diciembre de 2027** para la aplicación de las principales obligaciones de las secciones 1, 2 y 3 del capítulo III a los sistemas clasificados conforme al artículo 6.2 y el anexo III, con las excepciones y reglas transitorias correspondientes.

TEXTO OFICIAL · ANEXO IV

ANEXO IV
DOCUMENTACIÓN TÉCNICA A QUE SE REFIERE EL ARTÍCULO 11, APARTADO 1

La documentación técnica a que se refiere el artículo 11, apartado 1, incluirá como mínimo la siguiente información, aplicable al sistema de IA pertinente:

1. Una descripción general del sistema de IA que incluya:
   a) su finalidad prevista, el nombre del proveedor y la versión del sistema de tal manera que se refleje su relación con versiones anteriores;
   b) la manera en que el sistema de IA interactúa o puede utilizarse para interactuar con hardware o software, también con otros sistemas de IA, que no formen parte del propio sistema de IA, cuando proceda;
   c) las versiones de software o firmware pertinentes y todo requisito relacionado con la actualización de versiones;
   d) la descripción de todas las formas en que el sistema de IA se introduce en el mercado o se pone en servicio, como paquetes de software integrados en el hardware, descargas o API;
   e) la descripción del hardware en el que está previsto que se ejecute el sistema de IA;
   f) en el caso de que el sistema de IA sea un componente de un producto, fotografías o ilustraciones de las características exteriores, el marcado y la configuración interna de dicho producto;
   g) una descripción básica de la interfaz de usuario facilitada al responsable del despliegue;
   h) instrucciones de uso para el responsable del despliegue y una descripción básica de la interfaz de usuario facilitada al responsable del despliegue, cuando proceda.
2. Una descripción detallada de los elementos del sistema de IA y de su proceso de desarrollo, incluidos:
   a) los métodos y las medidas adoptados para el desarrollo del sistema de IA, incluido, en su caso, el recurso a sistemas o herramientas previamente entrenados facilitados por terceros y la manera en que han sido utilizados, integrados o modificados por el proveedor;
   b) las especificaciones de diseño del sistema, a saber, la lógica general del sistema de IA y de los algoritmos; las decisiones clave de diseño, incluidos la lógica y los supuestos de los que se ha partido, también con respecto a las personas o colectivos de personas en relación con los que está previsto que se utilice el sistema; las principales decisiones de clasificación; aquello que el sistema está diseñado para optimizar y la pertinencia de los diversos parámetros; la descripción de los resultados de salida esperados del sistema y la calidad de dichos resultados; las decisiones adoptadas acerca de cualquier posible concesión con respecto a las soluciones técnicas adoptadas para dar cumplimiento a los requisitos establecidos en el capítulo III, sección 2;
   c) la arquitectura del sistema, con una explicación de la manera en que los componentes del software se utilizan o enriquecen mutuamente y de la manera en que se integran en el procesamiento general; los recursos informáticos utilizados para desarrollar, entrenar, probar y validar el sistema de IA;
   d) cuando proceda, los requisitos en materia de datos, en forma de fichas técnicas que describan las metodologías y técnicas de entrenamiento, así como los conjuntos de datos de entrenamiento utilizados, e incluyan una descripción general de dichos conjuntos de datos e información acerca de su procedencia, su alcance y sus características principales; la manera en que se obtuvieron y seleccionaron los datos; los procedimientos de etiquetado (p. ej., para el aprendizaje supervisado) y las metodologías de depuración de datos (p. ej., la detección de anomalías);
   e) una evaluación de las medidas de supervisión humana necesarias de conformidad con el artículo 14, incluida una evaluación de las medidas técnicas necesarias para facilitar la interpretación de los resultados de salida de los sistemas de IA por parte de los responsables del despliegue, con arreglo al artículo 13, apartado 3, letra d);
   f) en su caso, una descripción detallada de los cambios predeterminados en el sistema de IA y su funcionamiento, junto con toda la información pertinente relativa a las soluciones técnicas adoptadas con el objetivo de garantizar la conformidad permanente del sistema de IA con los requisitos pertinentes establecidos en el capítulo III, sección 2;
   g) los procedimientos de validación y prueba utilizados, incluida la información acerca de los datos de validación y prueba empleados y sus características principales; los parámetros utilizados para medir la precisión, la solidez y el cumplimiento de otros requisitos pertinentes establecidos en el capítulo III, sección 2, así como los efectos potencialmente discriminatorios; los archivos de registro de las pruebas y todos los informes de las pruebas fechados y firmados por las personas responsables, también en lo que respecta a los cambios predeterminados a que se refiere la letra f);
   h) las medidas de ciberseguridad adoptadas.
3. Información detallada acerca de la supervisión, el funcionamiento y el control del sistema de IA, en particular con respecto a sus capacidades y limitaciones de funcionamiento, incluidos los niveles de precisión para las personas o colectivos de personas específicos en relación con los que está previsto que se utilice el sistema y el nivel general de precisión esperado en relación con su finalidad prevista; los resultados no deseados previsibles y las fuentes de riesgo para la salud y la seguridad, los derechos fundamentales y la discriminación, en vista de la finalidad prevista del sistema de IA; las medidas de supervisión humana necesarias de conformidad con el artículo 14, incluidas las medidas técnicas establecidas para facilitar la interpretación de los resultados de salida de los sistemas de IA por parte de los responsables del despliegue; las especificaciones de los datos de entrada, según proceda.
4. Una descripción de la idoneidad de los parámetros de rendimiento para el sistema de IA concreto.
5. Una descripción detallada del sistema de gestión de riesgos con arreglo al artículo 9.
6. Una descripción de los cambios pertinentes realizados por el proveedor en el sistema a lo largo de su ciclo de vida.
7. Una lista de las normas armonizadas, aplicadas total o parcialmente, cuyas referencias se hayan publicado en el Diario Oficial de la Unión Europea; cuando no se hayan aplicado normas armonizadas, una descripción detallada

de las soluciones adoptadas para cumplir los requisitos establecidos en el capítulo III, sección 2, incluida una lista de otras normas y especificaciones técnicas pertinentes que se hayan aplicado.

8. Una copia de la declaración UE de conformidad de conformidad con el artículo 47.
9. Una descripción detallada del sistema establecido para evaluar el funcionamiento del sistema de IA en la fase posterior a la comercialización, de conformidad con el artículo 72, incluido el plan de vigilancia poscomercialización a que se refiere el artículo 72, apartado 3.

Fuente: Reglamento (UE) 2024/1689, texto consolidado a 27 de julio de 2026. Transcripción del PDF aportado; se han omitido las marcas editoriales de consolidación y las cabeceras de página.

4. Anexo IV — Documentación técnica de sistemas de alto riesgo

Páginas 134–135 · Artículo 11

Este anexo establece qué documentación debe preparar el proveedor para demostrar que un sistema de IA de alto riesgo cumple los requisitos aplicables.

Es el equivalente a un **expediente técnico del sistema de IA**.

Información mínima exigida

Apartado	Qué debe documentarse
Identificación	Nombre, proveedor, finalidad y versión del sistema.
Arquitectura	Componentes, software, hardware e integraciones.
Desarrollo	Métodos, tecnologías, herramientas y decisiones de diseño.
Datos	Datos de entrenamiento, validación y prueba, cuando proceda.
Supervisión humana	Cómo pueden intervenir las personas y cómo interpretar los resultados.
Pruebas	Validaciones realizadas, precisión, solidez y posibles sesgos.
Seguridad	Medidas de ciberseguridad implantadas.
Gestión de riesgos	Riesgos identificados y medidas adoptadas.
Cambios	Registro de modificaciones relevantes durante la vida del sistema.
Conformidad	Normas utilizadas y declaración UE de conformidad.
Seguimiento	Plan de vigilancia posterior a la comercialización.

Un punto particularmente importante para las integraciones

El anexo exige documentar cómo interactúa el sistema con otros programas o componentes, así como los recursos y herramientas de terceros utilizados para desarrollarlo.

También menciona expresamente la comercialización o puesta en servicio mediante **API**.

Esto resulta relevante para sistemas que combinan un ERP, un modelo de IA, conexiones con herramientas externas y otros componentes.

Ejemplo orientativo: expediente técnico de un sistema de alto riesgo conectado a Sage 200

Sage 200 — Origen de información empresarial

API / Conector — Integración y control de permisos

Modelo y sistema de IA — Procesamiento y evaluación

Controles — Supervisión, registros, validación y seguridad

En un sistema sujeto al anexo IV, deben documentarse los elementos aplicables de la arquitectura, su integración, las decisiones técnicas, los riesgos y los controles.

La documentación debe reflejar también las modificaciones relevantes y las condiciones bajo las cuales el sistema se mantiene conforme.

Importante: este expediente técnico no se exige automáticamente, con todo este alcance, a cualquier chatbot o agente ordinario conectado a un ERP. Está vinculado al régimen regulatorio correspondiente.

TEXTO OFICIAL · ANEXO V

ANEXO V
DECLARACIÓN UE DE CONFORMIDAD

La declaración UE de conformidad a que se hace referencia en el artículo 47 contendrá toda la información siguiente:

1. El nombre y tipo del sistema de IA, y toda referencia inequívoca adicional que permita la identificación y trazabilidad del sistema de IA.
2. El nombre y la dirección del proveedor o, en su caso, de su representante autorizado.
3. La afirmación de que la declaración UE de conformidad con el artículo 47 se expide bajo la exclusiva responsabilidad del proveedor.
4. La declaración de que el sistema de IA es conforme con el presente Reglamento y, en su caso, con cualquier otra disposición de Derecho de la Unión pertinente que disponga la expedición de la declaración UE de conformidad con el artículo 47.
5. Cuando un sistema de IA implique el tratamiento de datos personales, la declaración de que el sistema de IA se ajusta al Reglamento (UE) 2016/679, al Reglamento (UE) 2018/1725 y a la Directiva (UE) 2016/680.
6. Referencias a todas las normas armonizadas pertinentes que se hayan aplicado o a cualquier otra especificación común respecto de la que se declara la conformidad.
7. En su caso, el nombre y el número de identificación del organismo notificado, una descripción del procedimiento de evaluación de la conformidad que se haya seguido y la identificación del certificado expedido.
8. El lugar y la fecha de expedición de la declaración, el nombre y el cargo de la persona que la firme, la indicación de la persona en cuyo nombre o por cuya cuenta firma la declaración y la firma.

Fuente: Reglamento (UE) 2024/1689, texto consolidado a 27 de julio de 2026. Transcripción del PDF aportado; se han omitido las marcas editoriales de consolidación y las cabeceras de página.

5. Anexo V — Declaración UE de conformidad

Página 136 · Artículo 47

Establece la información que debe incluir la declaración UE de conformidad de un sistema de IA de alto riesgo.

Se trata del documento mediante el cual el proveedor declara, bajo su responsabilidad, que el sistema cumple los requisitos aplicables.

Debe incluir la identificación del sistema y del proveedor, la declaración de conformidad, las referencias normativas pertinentes, la información del organismo notificado cuando corresponda y la identificación y firma de la persona responsable.

Cuando el sistema trata datos personales, el anexo contempla una declaración sobre su ajuste a las normas de protección de datos indicadas.

Aspecto importante: la declaración no es lo mismo que una certificación independiente. El proveedor asume la responsabilidad de su contenido, y el procedimiento de evaluación que corresponda se determina conforme al artículo 43.

TEXTO OFICIAL · ANEXO VI

ANEXO VI

PROCEDIMIENTO DE EVALUACIÓN DE LA CONFORMIDAD FUNDAMENTADO EN UN CONTROL INTERNO

1. El procedimiento de evaluación de la conformidad fundamentado en un control interno es el procedimiento de evaluación de la conformidad basado en los puntos 2, 3 y 4.
2. El proveedor comprueba que el sistema de gestión de la calidad establecido cumple los requisitos establecidos en el artículo 17.
3. El proveedor examina la información de la documentación técnica para evaluar la conformidad del sistema de IA con los requisitos esenciales pertinentes establecidos en el capítulo III, sección 2.
4. Asimismo, el proveedor comprueba que el proceso de diseño y desarrollo del sistema de IA y la vigilancia poscomercialización del mismo a que se refiere el artículo 72 son coherentes con la documentación técnica.

Fuente: Reglamento (UE) 2024/1689, texto consolidado a 27 de julio de 2026. Transcripción del PDF aportado; se han omitido las marcas editoriales de consolidación y las cabeceras de página.

TEXTO OFICIAL · ANEXO VII

ANEXO VII

CONFORMIDAD FUNDAMENTADA EN LA EVALUACIÓN DEL SISTEMA DE GESTIÓN DE LA CALIDAD Y LA EVALUACIÓN DE LA DOCUMENTACIÓN TÉCNICA

1. INTRODUCCIÓN

La conformidad fundamentada en la evaluación del sistema de gestión de la calidad y la evaluación de la documentación técnica es el procedimiento de evaluación de la conformidad basado en los puntos 2 a 5.

2. PRESENTACIÓN GENERAL

El sistema de gestión de la calidad aprobado en relación con el diseño, el desarrollo y las pruebas de los sistemas de IA con arreglo al artículo 17 se examinará de conformidad con el punto 3 y será objeto de vigilancia con arreglo a lo establecido en el punto 5. La documentación técnica del sistema de IA se examinará de conformidad con el punto 4.

3. SISTEMA DE GESTIÓN DE LA CALIDAD

3.1. La solicitud del proveedor incluirá:

a) el nombre y la dirección del proveedor y, si es el representante autorizado quien presenta la solicitud, también su nombre y dirección;

b) la lista de los sistemas de IA a los que se aplica el mismo sistema de gestión de la calidad;

c) la documentación técnica de cada sistema de IA al que se aplica el mismo sistema de gestión de la calidad;

d) la documentación relativa al sistema de gestión de la calidad, que cubrirá todos los aspectos enumerados en el artículo 17;

e) una descripción de los procedimientos establecidos para garantizar que el sistema de gestión de la calidad sigue siendo adecuado y eficaz;

f) una declaración por escrito de que no se ha presentado la misma solicitud ante ningún otro organismo notificado.

3.2. El sistema de gestión de la calidad será evaluado por el organismo notificado, que determinará si cumple los requisitos especificados en el artículo 17.

La decisión se notificará al proveedor o a su representante autorizado.

La notificación incluirá las conclusiones de la evaluación del sistema de gestión de la calidad y una decisión motivada sobre la evaluación.

3.3. El proveedor continuará aplicando y manteniendo el sistema de gestión de la calidad aprobado de forma que siga siendo adecuado y eficaz.

3.4. El proveedor comunicará al organismo notificado toda modificación prevista del sistema de gestión de la calidad aprobado o de la lista de sistemas de IA a los que este se aplica.

El organismo notificado examinará los cambios propuestos y decidirá si el sistema de gestión de la calidad modificado sigue cumpliendo los requisitos mencionados en el punto 3.2 o si es necesario realizar una nueva evaluación.

El organismo notificado notificará su decisión al proveedor. La notificación incluirá las conclusiones del examen de los cambios y una decisión motivada sobre la evaluación.

4. CONTROL DE LA DOCUMENTACIÓN TÉCNICA

4.1. Además de la solicitud a que se refiere el punto 3, el proveedor presentará una solicitud ante el organismo notificado de su elección para la evaluación de la documentación técnica relativa al sistema de IA que el proveedor pretenda introducir en el mercado o poner en servicio y al que se aplique el sistema de gestión de la calidad mencionado en el punto 3.

4.2. La solicitud incluirá:

a) el nombre y la dirección del proveedor;

b) una declaración por escrito de que no se ha presentado la misma solicitud ante ningún otro organismo notificado;

c) la documentación técnica prevista en el anexo IV.

4.3. El organismo notificado examinará la documentación técnica. Cuando proceda, y en la medida en que sea necesario para el desempeño de sus tareas, se concederá al organismo notificado pleno acceso a los conjuntos de datos de entrenamiento, validación y prueba utilizados, también, cuando proceda y con sujeción a garantías de seguridad, a través de API u otras herramientas y medios técnicos pertinentes que permitan el acceso a distancia.

4.4. Al examinar la documentación técnica, el organismo notificado podrá exigir que el proveedor facilite más pruebas justificativas o que lleve a cabo pruebas adicionales para que pueda evaluarse adecuadamente la conformidad del sistema de IA con los requisitos establecidos en el capítulo III, sección 2. Cuando el organismo notificado no quede satisfecho con las pruebas realizadas por el proveedor, efectuará él mismo directamente las pruebas adecuadas, según proceda.

4.5. Asimismo, se concederá al organismo notificado acceso al modelo de entrenamiento y al modelo entrenado del sistema de IA, con sus correspondientes parámetros, para, en caso necesario, una vez se hayan agotado y hayan demostrado ser insuficientes todas las demás vías razonables para verificar la conformidad, y previa solicitud motivada, evaluar la conformidad del sistema de IA de alto riesgo con los requisitos establecidos en el capítulo III, sección 2. Dicho acceso estará sujeto al Derecho de la Unión vigente relativo a la protección de la propiedad intelectual e industrial y los secretos comerciales.

4.6. Se notificará la decisión del organismo notificado al proveedor o a su representante autorizado. La notificación incluirá las conclusiones de la evaluación de la documentación técnica y una decisión motivada sobre la evaluación.

Cuando el sistema de IA cumpla los requisitos establecidos en el capítulo III, sección 2, el organismo notificado expedirá un certificado de la Unión de evaluación de la documentación técnica. Dicho certificado indicará el nombre y la dirección del proveedor, las conclusiones del examen, las condiciones de validez (en su caso) y los datos necesarios para identificar el sistema de IA.

El certificado y sus anexos contendrán toda la información pertinente para poder evaluar la conformidad del sistema de IA y permitir el control del sistema de IA mientras esté en uso, cuando proceda.

Cuando el sistema de IA no cumpla los requisitos establecidos en el capítulo III, sección 2, el organismo notificado denegará la expedición del certificado de la Unión de evaluación de la documentación técnica e informará de ello al solicitante, motivando detalladamente su decisión.

Cuando el sistema de IA no cumpla los requisitos relativos a los datos utilizados para su entrenamiento, será necesario llevar a cabo un nuevo entrenamiento del sistema antes de solicitar una nueva evaluación de la conformidad. En este caso, la decisión motivada sobre la evaluación del organismo notificado que deniegue la expedición del certificado de la Unión de evaluación de la documentación técnica contendrá consideraciones específicas relativas a la calidad de los datos utilizados para entrenar el sistema de IA, en particular acerca de los motivos del incumplimiento.

4.7. Todo cambio del sistema de IA que pueda afectar a su cumplimiento de los requisitos o su finalidad prevista será evaluado por el organismo notificado que haya expedido el certificado de la Unión de evaluación de la documentación técnica. El proveedor informará a dicho organismo notificado de su intención de introducir cualquiera de los cambios previamente mencionados o de si tiene constancia de que se hayan producido tales cambios. El organismo notificado evaluará los cambios previstos y decidirá si estos requieren una nueva evaluación de la conformidad con arreglo al artículo 43, apartado 4, o si pueden ser objeto de un suplemento al certificado de la Unión de evaluación de la documentación técnica. En este último caso, el organismo notificado evaluará los cambios, notificará su decisión al proveedor y, si aprueba los cambios, expedirá un suplemento al certificado de la Unión de evaluación de la documentación técnica.

5. VIGILANCIA DEL SISTEMA DE GESTIÓN DE LA CALIDAD APROBADO

5.1. La finalidad de la vigilancia por parte del organismo notificado a que se refiere el punto 3 es asegurarse de que el proveedor cumple debidamente las condiciones del sistema de gestión de la calidad aprobado.

5.2. A efectos de la evaluación, el proveedor dará acceso al organismo notificado a las instalaciones donde se estén diseñando, desarrollando o probando los sistemas de IA. Además, el proveedor facilitará al organismo notificado toda la información necesaria.

5.3. El organismo notificado realizará auditorías periódicas para asegurarse de que el proveedor mantiene y aplica el sistema de gestión de la calidad, y le entregará un informe de la auditoría. En el marco de dichas auditorías, el organismo notificado podrá efectuar más pruebas de los sistemas de IA para los que se hayan expedido certificados de la Unión de evaluación de la documentación técnica.

Fuente: Reglamento (UE) 2024/1689, texto consolidado a 27 de julio de 2026. Transcripción del PDF aportado; se han omitido las marcas editoriales de consolidación y las cabeceras de página.

6. Anexos VI y VII — Evaluación de conformidad

Páginas 137–140 · Artículo 43

Ambos anexos regulan procedimientos para comprobar que determinados sistemas de alto riesgo cumplen el Reglamento.

La diferencia esencial es **si la evaluación se basa en el control interno del proveedor o implica la intervención de un organismo notificado**.

Característica	Anexo VI	Anexo VII
Procedimiento	Control interno	Evaluación con organismo notificado
Quién verifica	El proveedor	Organismo notificado
Sistema de gestión de calidad	Se comprueba internamente	Se evalúa externamente
Documentación técnica	Revisión interna	Examen externo
Pruebas adicionales	Las necesarias para acreditar la conformidad	El organismo puede exigir o realizar pruebas adicionales
Vigilancia posterior	Responsabilidad del proveedor	Incluye vigilancia del sistema de gestión de calidad aprobado

Anexo VI. Control interno

El proveedor verifica que su sistema de gestión de calidad cumple el artículo 17, examina la documentación técnica y comprueba la coherencia del diseño, desarrollo y seguimiento posterior.

Anexo VII. Intervención de organismo notificado

El organismo examina el sistema de gestión de calidad y la documentación técnica, puede solicitar datos de entrenamiento y pruebas, realizar verificaciones y efectuar auditorías periódicas.

Cuando resulte estrictamente necesario y se cumplan las condiciones previstas, también puede solicitar acceso al modelo y a sus parámetros, respetando las garantías sobre propiedad intelectual y secretos comerciales.

¿Cuándo se utiliza cada procedimiento?

Este es un punto que merece especial atención.

El artículo 43 establece, con carácter general:

- Para los sistemas de alto riesgo del anexo III, puntos 2 a 8, se utiliza el procedimiento de control interno del anexo VI, sin participación de un organismo notificado.
- Para determinados sistemas biométricos del punto 1 del anexo III, pueden corresponder procedimientos distintos según las normas aplicadas y las condiciones legales.
- Para sistemas sujetos a la legislación del anexo I, sección A, se aplican las reglas de conformidad sectoriales y las disposiciones de coordinación previstas en el artículo 43.

No todos los sistemas de IA de alto riesgo necesitan necesariamente una certificación externa.

TEXTO OFICIAL · ANEXO VIII

ANEXO VIII

INFORMACIÓN QUE DEBE PRESENTARSE PARA LA INSCRIPCIÓN EN EL REGISTRO DE SISTEMAS DE IA DE ALTO RIESGO DE CONFORMIDAD CON EL ARTÍCULO 49

SECCIÓN A — INFORMACIÓN QUE DEBEN PRESENTAR LOS PROVEEDORES DE SISTEMAS DE IA DE ALTO RIESGO DE CONFORMIDAD CON EL ARTÍCULO 49, APARTADO 1

CON RESPECTO A LOS SISTEMAS DE IA DE ALTO RIESGO QUE VAYAN A INSCRIBIRSE EN EL REGISTRO DE CONFORMIDAD CON EL ARTÍCULO 49, APARTADO 1, SE FACILITARÁ Y SE ACTUALIZARÁ DEBIDAMENTE LA INFORMACIÓN SIGUIENTE:

1. El nombre, la dirección y los datos de contacto del proveedor.
2. Cuando sea otra persona la que presente la información en nombre del proveedor, el nombre, dirección y datos de contacto de dicha persona.
3. El nombre, la dirección y los datos de contacto del representante autorizado, en su caso.
4. El nombre comercial del sistema de IA y toda referencia inequívoca adicional que permita su identificación y trazabilidad.
5. La descripción de la finalidad prevista del sistema de IA y de los componentes y funciones que se apoyan a través del mismo.
6. Una descripción sencilla y concisa de la información que utiliza el sistema (datos, entradas) y su lógica de funcionamiento.
7. La situación del sistema de IA (comercializado o puesto en servicio, ha dejado de comercializarse o de estar en servicio, recuperado).
8. El tipo, el número y la fecha de caducidad del certificado expedido por el organismo notificado y el nombre o número de identificación de dicho organismo notificado, cuando proceda.
9. Una copia escaneada del certificado a que se refiere el punto 8, cuando proceda.
10. Todo Estado miembro en el que el sistema de IA se haya introducido en el mercado, puesto en servicio o comercializado en la Unión.
11. Una copia de la declaración UE de conformidad a que se refiere el artículo 47.
12. Las instrucciones de uso electrónicas. No se facilitará esta información en el caso de los sistemas de IA de alto riesgo en los ámbitos de la garantía del cumplimiento del Derecho o la migración, el asilo y la gestión del control fronterizo a que se refiere el anexo III, puntos 1, 6 y 7.
13. Una URL para obtener información adicional (opcional).

SECCIÓN B — INFORMACIÓN QUE DEBEN PRESENTAR LOS PROVEEDORES DE SISTEMAS DE IA DE ALTO RIESGO DE CONFORMIDAD CON EL ARTÍCULO 49, APARTADO 2

CON RESPECTO A LOS SISTEMAS DE IA QUE VAYAN A INSCRIBIRSE EN EL REGISTRO DE CONFORMIDAD CON EL ARTÍCULO 49, APARTADO 2, SE FACILITARÁ Y SE ACTUALIZARÁ DEBIDAMENTE LA INFORMACIÓN SIGUIENTE:

1. El nombre, la dirección y los datos de contacto del proveedor.
2. Cuando sea otra persona la que presente la información en nombre del proveedor, el nombre, dirección y datos de contacto de dicha persona.
3. El nombre, la dirección y los datos de contacto del representante autorizado, en su caso.
4. El nombre comercial del sistema de IA y toda referencia inequívoca adicional que permita su identificación y trazabilidad.
5. La descripción de la finalidad prevista del sistema de IA.
6. La condición o condiciones previstas en el artículo 6, apartado 3, con arreglo a las cuales se considera que el sistema de IA no es de alto riesgo.
8. La situación del sistema de IA (comercializado o puesto en servicio, ha dejado de comercializarse o de estar en servicio, recuperado).

SECCIÓN C — INFORMACIÓN QUE DEBEN PRESENTAR LOS RESPONSABLES DEL DESPLIEGUE DE SISTEMAS DE IA DE ALTO RIESGO DE CONFORMIDAD CON EL ARTÍCULO 49, APARTADO 3

CON RESPECTO A LOS SISTEMAS DE IA DE ALTO RIESGO QUE VAYAN A INSCRIBIRSE EN EL REGISTRO DE CONFORMIDAD CON EL ARTÍCULO 49, APARTADO 3, SE FACILITARÁ Y SE ACTUALIZARÁ DEBIDAMENTE LA INFORMACIÓN SIGUIENTE:

1. El nombre, la dirección y los datos de contacto del responsable del despliegue.
2. El nombre, la dirección y los datos de contacto de la persona que presente la información en nombre del responsable del despliegue.
3. La URL de entrada del sistema de IA en la base de datos de la UE por parte de su proveedor.
4. Un resumen de las conclusiones de la evaluación de impacto relativa a los derechos fundamentales realizada de conformidad con el artículo 27.
5. Un resumen de la evaluación de impacto relativa a la protección de datos realizada de conformidad con el artículo 35 del Reglamento (UE) 2016/679 o el artículo 27 de la Directiva (UE) 2016/680, tal como se especifica en el artículo 26, apartado 8, del presente Reglamento, cuando proceda.

Fuente: Reglamento (UE) 2024/1689, texto consolidado a 27 de julio de 2026. Transcripción del PDF aportado; se han omitido las marcas editoriales de consolidación y las cabeceras de página.

7. Anexo VIII — Información para el registro europeo

Páginas 141–142 · Artículos 49 y 71

Concreta qué información debe presentarse para registrar determinados sistemas de IA en la base de datos europea.

Se divide en tres secciones.

Sección	Quién facilita información	Qué se registra
A	Proveedores de sistemas de alto riesgo	Identificación del proveedor, sistema, finalidad, estado, conformidad y otra información exigida.
B	Proveedores que consideran que un sistema del anexo III no es de alto riesgo conforme al artículo 6.3	Identificación y justificación de esa clasificación.
C	Determinados responsables públicos del despliegue	Identificación del responsable, sistema utilizado y resúmenes de evaluaciones de impacto, cuando correspondan.

Punto especialmente importante

Un proveedor que decide clasificar como no de alto riesgo un sistema situado en el ámbito del anexo III puede seguir estando obligado a registrarlo.

Esto impide que la excepción de clasificación quede completamente fuera de los mecanismos de control.

Para los ERP: no todos los módulos inteligentes deben registrarse. Es necesario comprobar si la funcionalidad concreta está dentro de los supuestos del artículo 49.

TEXTO OFICIAL · ANEXO IX

ANEXO IX

INFORMACIÓN QUE DEBE PRESENTARSE PARA LA INSCRIPCIÓN EN EL REGISTRO DE LOS SISTEMAS DE IA DE ALTO RIESGO ENUMERADOS EN EL ANEXO III EN RELACIÓN CON LAS PRUEBAS EN CONDICIONES REALES DE CONFORMIDAD CON EL ARTÍCULO 60

Con respecto a las pruebas en condiciones reales que vayan a inscribirse en el registro de conformidad con el artículo 60, se facilitará y se actualizará debidamente la información siguiente:

1. El número de identificación único para toda la Unión de la prueba en condiciones reales.
2. El nombre y los datos de contacto del proveedor o proveedor potencial y de los responsables del despliegue que participen en la prueba en condiciones reales.
3. Una breve descripción del sistema de IA, su finalidad prevista y demás información necesaria para la identificación del sistema.
4. Un resumen de las principales características del plan de la prueba en condiciones reales.
5. Información sobre la suspensión o la conclusión de la prueba en condiciones reales.

Fuente: Reglamento (UE) 2024/1689, texto consolidado a 27 de julio de 2026. Transcripción del PDF aportado; se han omitido las marcas editoriales de consolidación y las cabeceras de página.

8. Anexo IX — Registro de pruebas en condiciones reales

Página 143 · Artículo 60

Establece los datos que deben registrarse cuando se realizan determinadas pruebas de sistemas de IA de alto riesgo en condiciones reales.

La información incluye:

- Número de identificación único de la prueba.
- Datos del proveedor y de los responsables del despliegue participantes.
- Descripción y finalidad del sistema.
- Características principales del plan de pruebas.
- Información sobre su suspensión o finalización.

Aspecto relevante: el registro permite que las autoridades identifiquen y supervisen las pruebas. No constituye una autorización genérica para experimentar libremente con sistemas de alto riesgo.

TEXTO OFICIAL · ANEXO X

ANEXO X
ACTOS LEGISLATIVOS DE LA UNIÓN RELATIVOS A SISTEMAS INFORMÁTICOS DE GRAN MAGNITUD EN EL ESPACIO DE LIBERTAD, SEGURIDAD Y JUSTICIA

1. SISTEMA DE INFORMACIÓN DE SCHENGEN

a) Reglamento (UE) 2018/1860 del Parlamento Europeo y del Consejo, de 28 de noviembre de 2018, sobre la utilización del Sistema de Información de Schengen para el retorno de nacionales de terceros países en situación irregular (DO L 312 de 7.12.2018, p. 1).

b) Reglamento (UE) 2018/1861 del Parlamento Europeo y del Consejo, de 28 de noviembre de 2018, relativo al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen (SIS) en el ámbito de las inspecciones fronterizas, por el que se modifica el Convenio de aplicación del Acuerdo de Schengen y se modifica y deroga el Reglamento (CE) n. o 1987/2006 (DO L 312 de 7.12.2018, p. 14).

c) Reglamento (UE) 2018/1862 del Parlamento Europeo y del Consejo, de 28 de noviembre de 2018, relativo al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen (SIS) en el ámbito de la cooperación policial y de la cooperación judicial en materia penal, por el que se modifica y deroga la Decisión 2007/533/JAI del Consejo, y se derogan el Reglamento (CE) n. o 1986/2006 del Parlamento Europeo y del Consejo y la Decisión 2010/261/UE de la Comisión (DO L 312 de 7.12.2018, p. 56).

2. SISTEMA DE INFORMACIÓN DE VISADOS

a) Reglamento (UE) 2021/1133 del Parlamento Europeo y del Consejo, de 7 de julio de 2021, por el que se modifican los Reglamentos (UE) n. o 603/2013, (UE) 2016/794, (UE) 2018/1862, (UE) 2019/816 y (UE) 2019/818 en lo que respecta al establecimiento de las condiciones para acceder a otros sistemas de información de la UE a efectos del Sistema de Información de Visados (DO L 248 de 13.7.2021, p. 1).

b) Reglamento (UE) 2021/1134 del Parlamento Europeo y del Consejo, de 7 de julio de 2021, por el que se modifican los Reglamentos (CE) n. o

767/2008, (CE) n. o 810/2009, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1860, (UE) 2018/1861, (UE) 2019/817 y (UE) 2019/1896 del Parlamento Europeo y del Consejo y por el que se derogan las Decisiones 2004/512/CE y 2008/633/JAI del Consejo, a fin de reformar el Sistema de Información de Visados (DO L 248 de 13.7.2021, p. 11).

3. EURODAC

Reglamento (UE) 2024/1358 del Parlamento Europeo y del Consejo, de 14 de mayo de 2024, sobre la creación del sistema «Eurodac» para la comparación de datos biométricos a efectos de la aplicación efectiva de los Reglamentos (UE) 2024/1315 y (UE) 2024/1350 del Parlamento Europeo y del Consejo y de la Directiva 2001/55/CE del Consejo y de la identificación de nacionales de terceros países y apátridas en situación irregular, y sobre las solicitudes de comparación con los datos de Eurodac presentadas por los servicios de seguridad de los Estados miembros y Europol a efectos de garantía de cumplimiento del Derecho, por el que se modifican los Reglamentos (UE) 2018/1240 y (UE) 2019/818 del Parlamento Europeo y del Consejo y se deroga el Reglamento (UE) n. o 603/2013 del Parlamento Europeo y del Consejo (DO L, 2024/1358, 22.5.2024, ELI: http://data.europa.eu/eli/reg/2024/1358/oj).

4. SISTEMA DE ENTRADAS Y SALIDAS

Reglamento (UE) 2017/2226 del Parlamento Europeo y del Consejo, de 30 de noviembre de 2017, por el que se establece un Sistema de Entradas y Salidas (SES) para registrar los datos de entrada y salida y de denegación de entrada relativos a nacionales de terceros países que crucen las fronteras exteriores de los Estados miembros, se determinan las condiciones de acceso al SES con fines policiales y se modifican el Convenio de aplicación del Acuerdo de Schengen y los Reglamentos (CE) n. o 767/2008 y (UE) n. o 1077/2011 (DO L 327 de 9.12.2017, p. 20).

5. SISTEMA EUROPEO DE INFORMACIÓN Y AUTORIZACIÓN DE VIAJES

a) Reglamento (UE) 2018/1240 del Parlamento Europeo y del Consejo, de 12 de septiembre de 2018, por el que se establece un Sistema Europeo de Información y Autorización de Viajes (SEIAV) y por el que se modifican los Reglamentos (UE) n. o 1077/2011, (UE) n. o 515/2014, (UE) 2016/399, (UE) 2016/1624 y (UE) 2017/2226 (DO L 236 de 19.9.2018, p. 1).

b) Reglamento (UE) 2018/1241 del Parlamento Europeo y del Consejo, de 12 de septiembre de 2018, por el que se modifica el Reglamento (UE) 2016/794 con objeto de establecer el Sistema Europeo de Información y Autorización de Viajes (SEIAV) (DO L 236 de 19.9.2018, p. 72).

6. Sistema Europeo de Información de Antecedentes Penales en relación con los nacionales de terceros países y apátridas

Reglamento (UE) 2019/816 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, por el que se establece un sistema centralizado para la identificación de los Estados miembros que poseen información sobre condenas de nacionales de terceros países y apátridas (ECRIS-TCN) a fin de complementar el Sistema Europeo de Información de Antecedentes Penales, y por el que se modifica el Reglamento (UE) 2018/1726 (DO L 135 de 22.5.2019, p. 1).

7. INTEROPERABILIDAD

a) Reglamento (UE) 2019/817 del Parlamento Europeo y del Consejo, de 20 de mayo de 2019, relativo al establecimiento de un marco para la interoperabilidad de los sistemas de información de la UE en el ámbito de las fronteras y los visados y por el que se modifican los Reglamentos (CE) n. o 767/2008,(UE)2016/399,(UE)2017/2226,(UE)2018/1240,(UE)2018/1726 y (UE) 2018/1861 del Parlamento Europeo y del Consejo, y las Decisiones 2004/512/CE y 2008/633/JAI del Consejo (DO L 135 de 22.5.2019, p. 27).

b) Reglamento (UE) 2019/818 del Parlamento Europeo y del Consejo, de 20 de mayo de 2019, relativo al establecimiento de un marco para la interoperabilidad entre los sistemas de información de la UE en el ámbito de la cooperación policial y judicial, el asilo y la migración y por el que se modifican los Reglamentos

(UE) 2018/1726, (UE) 2018/1862 y (UE) 2019/816 (DO L 135 de 22.5.2019, p. 85).

Fuente: Reglamento (UE) 2024/1689, texto consolidado a 27 de julio de 2026. Transcripción del PDF aportado; se han omitido las marcas editoriales de consolidación y las cabeceras de página.

9. Anexo X — Grandes sistemas informáticos europeos

Páginas 144–145 · Artículo 111

Este anexo identifica sistemas informáticos de gran magnitud utilizados en ámbitos europeos de seguridad, fronteras, migración y justicia.

Entre ellos están:

Sistema	Finalidad general
SIS	Sistema de Información de Schengen
VIS	Sistema de Información de Visados
Eurodac	Sistema europeo de datos biométricos vinculado a migración y asilo
SES	Sistema de Entradas y Salidas
SEIAV / ETIAS	Información y autorización de viajes
ECRIS-TCN	Información sobre antecedentes penales de nacionales de terceros países
Sistemas de interoperabilidad	Interconexión de determinados sistemas europeos

Su relevancia principal está relacionada con el régimen transitorio del artículo 111.

Fecha importante: 31 de diciembre de 2030. Es el plazo de adaptación previsto para los sistemas comprendidos en el supuesto específico del artículo 111.1.

Para una empresa privada que utiliza un ERP convencional, este anexo tiene una repercusión normalmente reducida.

TEXTO OFICIAL · ANEXO XI

ANEXO XI

DOCUMENTACIÓN TÉCNICA A QUE SE REFIERE EL ARTÍCULO 53, APARTADO 1, LETRA A) — DOCUMENTACIÓN TÉCNICA PARA PROVEEDORES DE MODELOS DE IA DE USO GENERAL

SECCIÓN 1

INFORMACIÓN QUE DEBEN PRESENTAR LOS PROVEEDORES DE MODELOS DE IA DE USO GENERAL

La documentación técnica a que se refiere el artículo 53, apartado 1, letra a), incluirá como mínimo la siguiente información en función del tamaño y perfil de riesgo del modelo:

1. Una descripción general del modelo de IA de uso general que incluya:
   a) las tareas que el modelo vaya a realizar y el tipo y la naturaleza de los sistemas de IA en los que puede integrarse;
   b) las políticas de usos aceptables aplicables;
   c) la fecha de lanzamiento y los métodos de distribución;
   d) la arquitectura y el número de parámetros;
   e) la modalidad (por ejemplo, texto, imagen) y el formato de las entradas y salidas;
   f) la licencia.
2. Una descripción detallada de los elementos del modelo a que se refiere el punto 1 e información pertinente sobre el proceso de desarrollo que incluya los siguientes elementos:
   a) los medios técnicos (por ejemplo, instrucciones de uso, infraestructura, herramientas) necesarios para integrar el modelo de IA de uso general en los sistemas de IA;
   b) las especificaciones de diseño del modelo y el proceso de entrenamiento, incluidos los métodos y las técnicas de entrenamiento, las decisiones clave de diseño, incluidas la justificación lógica y los supuestos de los que se ha partido; aquello que el modelo está diseñado para optimizar y la pertinencia de los diversos parámetros, según proceda;
   c) información sobre los datos utilizados para el entrenamiento, las pruebas y la validación, cuando proceda, incluidos el tipo y la procedencia de los datos y los métodos de gestión (por ejemplo, limpieza, filtrado, etc.), el número de puntos de datos, su alcance y sus principales características; cómo se obtuvieron y seleccionaron los datos, así como cualquier otra medida que permita detectar que las fuentes de datos no son idóneas y los métodos para detectar sesgos identificables, cuando proceda;
   d) los recursos computacionales utilizados para entrenar el modelo (por ejemplo, número de operaciones de coma flotante, el tiempo de entrenamiento y otros detalles pertinentes relacionados con el mismo;
   e) el consumo de energía conocido o estimado del modelo.

A propósito de la letra e), cuando se desconozca el consumo de energía del modelo, podrá hacerse una estimación del consumo de energía a partir de la información relativa a los recursos computacionales utilizados.

SECCIÓN 2

INFORMACIÓN ADICIONAL QUE DEBEN PRESENTAR LOS PROVEEDORES DE MODELOS DE IA DE USO GENERAL CON RIESGO SISTÉMICO

1. Una descripción detallada de las estrategias de evaluación, con los resultados de la misma, sobre la base de los protocolos y herramientas de evaluación públicos disponibles o de otros métodos de evaluación. Las estrategias de evaluación incluirán los criterios de evaluación, los parámetros y el método de detección de limitaciones.
2. Cuando proceda, una descripción detallada de las medidas adoptadas para realizar pruebas adversarias internas o externas (por ejemplo, utilización de «equipos rojos») y adaptaciones de los modelos, incluida su alineación y puesta a punto.
3. Cuando proceda, una descripción detallada de la arquitectura del sistema, con una explicación de la manera en que se incorporan o enriquecen mutuamente los componentes del software y de la manera en que se integran en el procesamiento general.

Fuente: Reglamento (UE) 2024/1689, texto consolidado a 27 de julio de 2026. Transcripción del PDF aportado; se han omitido las marcas editoriales de consolidación y las cabeceras de página.

10. Anexo XI — Documentación técnica de modelos de IA de uso general

Páginas 146–147 · Artículo 53.1.a

Este anexo se dirige a los **proveedores de modelos de inteligencia artificial de uso general**.

Es distinto del anexo IV, que se refiere a la documentación técnica de sistemas de alto riesgo.

¿Qué información debe documentar el proveedor del modelo?

Bloque	Contenido
Capacidades	Tareas que realiza el modelo y sistemas en los que puede integrarse.
Arquitectura	Diseño, parámetros y características técnicas.
Modalidades	Tipos de entrada y salida: texto, imagen y otras.
Distribución	Fecha de lanzamiento, métodos de distribución y licencia.
Entrenamiento	Métodos, técnicas y decisiones de diseño.
Datos	Procedencia, características y tratamiento de los datos utilizados.
Capacidad de cálculo	Recursos computacionales utilizados para entrenar el modelo.
Energía	Consumo conocido o estimado del modelo.
Evaluaciones	Resultados y documentación de las pruebas correspondientes.

Para los modelos de uso general con riesgo sistémico se exige información adicional, incluidas evaluaciones más detalladas y, cuando proceda, pruebas adversarias (*red teaming*).

Diferencia importante

Esta documentación se prepara para las obligaciones del proveedor del modelo y su posible supervisión por las autoridades.

No equivale a exigir que el fabricante revele públicamente todos los parámetros, datos o secretos comerciales del modelo.

TEXTO OFICIAL · ANEXO XII

ANEXO XII

INFORMACIÓN SOBRE TRANSPARENCIA A QUE SE REFIERE EL ARTÍCULO 53, APARTADO 1, LETRA B) — DOCUMENTACIÓN TÉCNICA DE LOS PROVEEDORES DE MODELOS DE IA DE USO GENERAL PARA LOS PROVEEDORES POSTERIORES QUE INTEGREN EL MODELO EN SU SISTEMA DE IA

La información a que se refiere el artículo 53, apartado 1, letra b), incluirá como mínimo la siguiente información:

1. Una descripción general del modelo de IA de uso general que incluya:
   a) las tareas que el modelo vaya a realizar y el tipo y la naturaleza de los sistemas de IA en los que puede integrarse;
   b) las políticas de usos aceptables aplicables;
   c) la fecha de lanzamiento y los métodos de distribución;
   d) la manera en que el modelo interactúa o puede utilizarse para interactuar con el hardware o el software que no formen parte del propio modelo, cuando proceda;
   e) las versiones del software pertinente relacionadas con el uso del modelo de IA de uso general, cuando proceda;
   f) la arquitectura y el número de parámetros;
   g) la modalidad (por ejemplo, texto, imagen) y el formato de las entradas y salidas;
   h) la licencia del modelo.
2. Una descripción de los elementos del modelo y de su proceso de desarrollo, incluidos:
   a) los medios técnicos (por ejemplo, instrucciones de uso, infraestructura, herramientas) necesarios para integrar el modelo de IA de uso general en los sistemas de IA;
   b) la modalidad (por ejemplo, texto, imagen, etc.) y el formato de las entradas y salidas y su tamaño máximo (por ejemplo, longitud de la ventana de contexto, etc.);
   c) información sobre los datos utilizados para el entrenamiento, las pruebas y la validación, cuando proceda, incluidos el tipo y la procedencia de los datos y los métodos de gestión.

Fuente: Reglamento (UE) 2024/1689, texto consolidado a 27 de julio de 2026. Transcripción del PDF aportado; se han omitido las marcas editoriales de consolidación y las cabeceras de página.

11. Anexo XII — Información técnica para los integradores de modelos

Especialmente relevante para integraciones de IA con ERP

Página 148 · Artículo 53.1.b

Este anexo establece la documentación que el proveedor de un modelo de IA de uso general debe facilitar a los proveedores posteriores que pretendan integrarlo en sus propios sistemas.

Su objetivo es que puedan comprender las capacidades, limitaciones y condiciones técnicas del modelo.

¿Qué información debe facilitarse?

Información	Importancia práctica
Tareas admitidas	Identificar para qué puede utilizarse el modelo.
Usos aceptables	Conocer las restricciones y condiciones de utilización.
Versiones	Controlar la evolución de las versiones utilizadas.
Arquitectura y parámetros	Comprender las características generales del modelo.
Formatos de entrada y salida	Facilitar el desarrollo de integraciones.
Tamaños máximos de entrada y salida	Conocer límites técnicos, como la ventana de contexto.
Requisitos de integración	Identificar herramientas, infraestructura e instrucciones necesarias.
Información sobre datos de entrenamiento	Conocer los elementos exigidos sobre tipos, procedencia y gestión de datos.
Licencia	Comprender las condiciones bajo las que se distribuye y utiliza el modelo.

Ejemplo práctico: Sage 200 + LLM

Una empresa desarrolla un agente que permite consultar información del ERP mediante una API y un modelo de lenguaje.

El integrador necesita conocer las capacidades y limitaciones del modelo para determinar si resulta adecuado para las tareas previstas.

Proveedor del modelo de IA

Documentación del anexo XII

Capacidades, limitaciones, integración, formatos, licencia y datos exigidos

Integrador / proveedor del sistema de IA

Aplicación empresarial conectada al ERP

La relevancia es clara: **el proveedor del modelo tiene obligaciones de información respecto de las empresas que desarrollan sistemas utilizando ese modelo**.

Ello facilita que los integradores puedan cumplir sus propias obligaciones cuando les correspondan.

El alcance de estas exigencias debe interpretarse junto con las excepciones previstas en el artículo 53, especialmente para determinados modelos de código abierto.

TEXTO OFICIAL · ANEXO XIII

ANEXO XIII

CRITERIOS PARA LA CLASIFICACIÓN DE LOS MODELOS DE IA DE USO GENERAL CON RIESGO SISTÉMICO A QUE SE REFIERE EL ARTÍCULO 51

Con el fin de determinar si un modelo de IA de uso general tiene unas capacidades o unos efectos equivalentes a los contemplados en el artículo 51, apartado 1, letra a), la Comisión tendrá en cuenta los siguientes criterios:

a) el número de parámetros del modelo;

b) la calidad o el tamaño del conjunto de datos, por ejemplo medidos a través de criptofichas;

c) la cantidad de cálculo utilizada para entrenar el modelo, medida en operaciones de coma flotante o indicada con una combinación de otras variables, como el coste estimado del entrenamiento, el tiempo estimado necesario o el consumo de energía estimado para el mismo;

d) las modalidades de entrada y salida del modelo, como la conversión de texto a texto (grandes modelos de lenguaje), la conversión de texto a imagen, la multimodalidad y los umbrales punteros para determinar las capacidades de gran impacto de cada modalidad, y el tipo concreto de entradas y salidas (por ejemplo, secuencias biológicas);

e) los parámetros de referencia y las evaluaciones de las capacidades del modelo, también teniendo en cuenta el número de tareas sin entrenamiento adicional, la adaptabilidad para aprender tareas nuevas distintas, su nivel de autonomía y capacidad de ampliación y las herramientas a las que tiene acceso;

f) si sus repercusiones para el mercado interior son importantes debido a su alcance, lo que se dará por supuesto cuando se haya puesto a disposición de al menos 10 000 usuarios profesionales registrados establecidos en la Unión;

g) el número de usuarios finales registrados.

Fuente: Reglamento (UE) 2024/1689, texto consolidado a 27 de julio de 2026. Transcripción del PDF aportado; se han omitido las marcas editoriales de consolidación y las cabeceras de página.

12. Anexo XIII — Criterios para clasificar modelos de IA con riesgo sistémico

Página 149 · Artículo 51

Este anexo establece los factores que la Comisión debe considerar para determinar si un modelo de IA de uso general presenta capacidades o impactos equivalentes a los que permiten clasificarlo como modelo de riesgo sistémico.

Criterios principales

Criterio	Qué se analiza
Número de parámetros	Tamaño y características del modelo.
Datos utilizados	Calidad y volumen de los conjuntos de datos.
Cálculo de entrenamiento	Recursos computacionales y esfuerzo de entrenamiento.
Modalidades	Capacidades para procesar texto, imágenes y otros formatos.
Evaluaciones	Resultados de pruebas y parámetros de referencia.
Autonomía	Capacidad para realizar tareas y utilizar herramientas.
Adaptabilidad	Capacidad para aprender o abordar nuevas tareas.
Alcance de mercado	Impacto potencial por su distribución y utilización.
Usuarios	Número de usuarios profesionales y finales registrados.

Umbral relevante

El artículo 51 establece una presunción de capacidades de gran impacto cuando el cálculo acumulado de entrenamiento supera los (10^{25}) FLOP.

Pero este no es el único elemento posible de clasificación.

El anexo XIII también establece que se presume un impacto importante en el mercado interior, a los efectos del criterio correspondiente, cuando el modelo se ha puesto a disposición de al menos **10.000 usuarios profesionales registrados establecidos en la Unión Europea**.

Esto no constituye por sí solo una prohibición ni una clasificación automática de todas las herramientas construidas con ese modelo.

Para las empresas que utilizan modelos comerciales: las obligaciones de riesgo sistémico recaen principalmente sobre los proveedores de esos modelos, sin perjuicio de las responsabilidades que puedan corresponder por los sistemas desarrollados.

TEXTO OFICIAL · ANEXO XIV

ANEXO XIV

LISTA DE CÓDIGOS, CATEGORÍAS Y TIPOS CORRESPONDIENTES DE SISTEMAS DE IA A EFECTOS DEL PROCEDIMIENTO DE NOTIFICACIÓN PREVISTO EN EL ARTÍCULO 30 A FIN DE ESPECIFICAR EL ÁMBITO DE APLICACIÓN DE LA DESIGNACIÓN COMO ORGANISMOS NOTIFICADOS

1. INTRODUCCIÓN

La evaluación de la conformidad de los sistemas de IA de alto riesgo en virtud del presente Reglamento podrá requerir la participación de organismos de evaluación de la conformidad. Solo podrán llevar a cabo evaluaciones de la conformidad los organismos de evaluación de la conformidad designados con arreglo al presente Reglamento, y únicamente podrán hacerlo con respecto a las actividades relacionadas con los tipos de sistemas de IA de que se trate. La lista de códigos, categorías y tipos correspondientes de sistemas de IA regula la designación de los organismos de evaluación de la conformidad notificados con arreglo al artículo 30.

2. LISTA DE CÓDIGOS, CATEGORÍAS Y SISTEMAS DE IA CORRESPONDIENTES

A) SISTEMAS DE IA SUJETOS AL ANEXO I

CÓDIGO EN EL MARCO DEL REGLAMENTO DE IA

AIP 0102 Sistemas de IA sujetos a la sección A, punto 2, del anexo I.

AIP 0103 Sistemas de IA sujetos a la sección A, punto 3, del anexo I.

AIP 0104 Sistemas de IA sujetos a la sección A, punto 4, del anexo I.

AIP 0105 Sistemas de IA sujetos a la sección A, punto 5, del anexo I.

AIP 0106 Sistemas de IA sujetos a la sección A, punto 6, del anexo I.

AIP 0107 Sistemas de IA sujetos a la sección A, punto 7, del anexo I.

AIP 0108 Sistemas de IA sujetos a la sección A, punto 8, del anexo I.

AIP 0109 Sistemas de IA sujetos a la sección A, punto 9, del anexo I.

AIP 0110 Sistemas de IA sujetos a la sección A, punto 10, del anexo I.

AIP 0111 Sistemas de IA sujetos a la sección A, punto 11, del anexo I.

AIP 0112 Sistemas de IA sujetos a la sección A, punto 12, del anexo I.

B) SISTEMAS DE IA SUJETOS AL PUNTO 1 DEL ANEXO III

CÓDIGO EN EL MARCO DEL REGLAMENTO DE IA

AIB 0201 Sistemas de identificación biométrica remota

AIB 0202 Sistemas de IA de categorización biométrica

AIB 0203 Sistemas de IA para el reconocimiento de emociones

3. CÓDIGOS ESPECÍFICOS DE TECNOLOGÍA DE IA

A) IA SIMBÓLICA Y SISTEMAS EXPERTOS

CÓDIGO EN EL MARCO DEL REGLAMENTO DE IA

AIH 0101 Sistemas de IA basados en la IA simbólica, en sistemas expertos y en sistemas basados en el conocimiento, y sistemas de IA basados en búsqueda y optimización

B) APRENDIZAJE AUTOMÁTICO, EXCLUIDOS LOS SISTEMAS DE IA GENERATIVA Y DE IA DE USO GENERAL

CÓDIGO EN EL MARCO DEL REGLAMENTO DE IA

AIH 0201 Sistemas de IA que procesan datos estructurados

AIH 0202 Sistemas de IA que procesan datos de señales y de audio

AIH 0203 Sistemas de IA que procesan datos de texto

AIH 0204 Sistemas de IA que procesan imágenes y vídeos

AIH 0205 Sistemas de IA que aprenden de su entorno, excluidos los sistemas de IA contemplados en el código AIH 0401

C) SISTEMAS DE IA BASADOS EN MODELOS DE IA DE USO GENERAL O DE IA GENERATIVA

CÓDIGO EN EL MARCO DEL REGLAMENTO DE IA

AIH 0301 Sistemas de IA generativa, incluidos los sistemas de IA basados en modelos de IA de uso general

D) TECNOLOGÍAS DE IA EMERGENTES

CÓDIGO EN EL MARCO DEL REGLAMENTO DE IA

AIH 0401 Sistemas de IA basados en otras tecnologías emergentes de IA no cubiertas por otros códigos, incluida la IA agente

4. SOLICITUD DE DESIGNACIÓN

Los organismos de evaluación de la conformidad utilizarán las listas de códigos, categorías y tipos correspondientes de sistemas de IA que figuran en el presente anexo al especificar los tipos de sistemas de IA en la solicitud de designación a que se refiere el artículo 29.

Fuente: Reglamento (UE) 2024/1689, texto consolidado a 27 de julio de 2026. Transcripción del PDF aportado; se han omitido las marcas editoriales de consolidación y las cabeceras de página.

13. Anexo XIV — Categorías y códigos de sistemas de IA

Nuevo anexo incorporado en la versión consolidada de 2026

Páginas 150–151 · Artículos 29 y 30

Este anexo es especialmente interesante porque incorpora una clasificación técnica de tecnologías de IA y **menciona expresamente la IA agente**.

Su finalidad es establecer códigos para que los organismos de evaluación de conformidad delimiten los tipos de sistemas de IA para los que solicitan ser designados como organismos notificados.

Clasificación por ámbito regulatorio

Código	Tipo de sistema
AIP 0102–0112	Sistemas relacionados con las categorías enumeradas en el anexo I, sección A.
AIB 0201	Identificación biométrica remota.
AIB 0202	Categorización biométrica.
AIB 0203	Reconocimiento de emociones.

Clasificación por tecnología

Código	Tecnología
AIH 0101	IA simbólica, sistemas expertos, sistemas basados en conocimiento, búsqueda y optimización.
AIH 0201	Aprendizaje automático sobre datos estructurados.
AIH 0202	Aprendizaje automático sobre señales y audio.
AIH 0203	Aprendizaje automático sobre texto.
AIH 0204	Aprendizaje automático sobre imágenes y vídeo.
AIH 0205	Sistemas que aprenden de su entorno, con la excepción indicada.
AIH 0301	IA generativa, incluidos sistemas basados en modelos de uso general.
AIH 0401	**Otras tecnologías emergentes, incluida la IA agente.**

¿Por qué es interesante la aparición de la IA agente?

Porque el anexo reconoce expresamente esta tecnología dentro del sistema de clasificación utilizado para la designación de organismos notificados.

Es relevante para las empresas que desarrollan soluciones capaces de utilizar herramientas, conectarse a aplicaciones y ejecutar secuencias de tareas.

No obstante, hay que evitar una interpretación incorrecta:

La inclusión de la IA agente en el código AIH 0401 no convierte automáticamente a todos los agentes de IA en sistemas de alto riesgo.

Este anexo regula las categorías técnicas empleadas para delimitar las competencias de los organismos notificados, no establece una nueva clasificación general de riesgo para todos los agentes.

Por ejemplo, un agente conectado a Sage 200 que consulta existencias y prepara presupuestos no pasa a ser de alto riesgo por utilizar tecnología de IA agente.

Su clasificación dependerá de la finalidad y de las funciones del sistema, conforme a los artículos y anexos correspondientes.

14. Resumen final: qué deben retener las empresas de todos los anexos

Para una empresa que quiere incorporar inteligencia artificial a sus procesos o para una consultora que desarrolla integraciones con un ERP, los anexos pueden agruparse en cuatro cuestiones prácticas.

1. Identificar si la IA es de alto riesgo

El anexo III es la principal referencia para aplicaciones empresariales que afectan a personas, especialmente recursos humanos, evaluación crediticia y servicios esenciales.

2. Preparar la documentación y verificar el cumplimiento

Los anexos IV, V, VI, VII y VIII detallan documentación, declaración de conformidad, evaluaciones y registros cuando el sistema está sujeto a esas obligaciones.

3. Distinguir al fabricante del modelo del integrador

Los anexos XI, XII y XIII concretan obligaciones relacionadas con modelos de IA de uso general, con especial atención a la documentación y a los riesgos sistémicos.

4. Comprender la tecnología y su utilización

El anexo XIV establece categorías técnicas, incluida la IA generativa y la IA agente, para los fines específicos de designación de organismos de evaluación.

15. Conclusión general del Reglamento y sus anexos

Después de estudiar los 13 capítulos y los 14 anexos del texto consolidado, la conclusión más importante para el entorno empresarial es que **la regulación europea de IA se basa principalmente en las características, la finalidad, el riesgo y las responsabilidades asociadas a cada sistema**.

No existe una obligación uniforme para cualquier empresa que incorpore un modelo de lenguaje, un OCR inteligente, un sistema predictivo o un agente conectado a su ERP.

Sin embargo, cuando la IA interviene en decisiones sensibles sobre personas o en determinadas funciones de seguridad, las obligaciones pueden ser considerablemente mayores.

Para el desarrollo e integración de soluciones como Sage 200, el criterio fundamental consiste en distinguir tres responsabilidades: la del proveedor del modelo, la del proveedor del sistema desarrollado y la de la empresa que lo utiliza.

Si tuviera que destacar únicamente cuatro anexos para preparar una explicación dirigida a empresarios y fabricantes de software, elegiría el III, el IV, el XII y el XIV. Son los que mejor permiten explicar qué aplicaciones requieren especial atención, cómo debe documentarse un sistema de alto riesgo, qué información debe recibir un integrador y cómo se identifican las diferentes tecnologías de IA.

Resumen basado exclusivamente en los anexos II a XIV del documento consolidado aportado, con referencias complementarias a sus artículos relacionados.



TECNOLOGÍA CON CRITERIO.
INNOVACIÓN CON CONFIANZA.

Marco normativo europeo de inteligencia artificial.

Una lectura jurídica y empresarial para tomar mejores decisiones.

GRUPO solitium

SOLUCIONES ERP · SOFTWARE EMPRESARIAL · TRANSFORMACIÓN DIGITAL

www.solitium.es